

**UNIVERSITÀ POLITECNICA DELLE MARCHE**  
**FACOLTÀ DI INGEGNERIA**  
Dipartimento di Ingegneria dell'Informazione  
Corso di Laurea in Ingegneria Informatica e dell'Automazione

---



**TESI DI LAUREA**

**Alle frontiere dell'Intelligenza Artificiale: Riconoscimento di immagini, Traduzione di testi e Generative AI applicata all'arte**

**At the frontiers of Artificial Intelligence: Image Recognition, Text Translation and Generative AI applied to art**

Relatore

Prof. Domenico Ursino

Candidata

Caterina Sabatini

---

**ANNO ACCADEMICO 2023-2024**

*Sometimes it is the people no one can imagine  
anything of who do the things no one can imagine.*

Alan Turing

## Sommario

L'Intelligenza Artificiale costituisce una delle frontiere più affascinanti dell'innovazione tecnologica nel mondo contemporaneo. Il suo obiettivo è di emulare le capacità cognitive umane attraverso l'elaborazione di algoritmi complessi e l'analisi di grandi quantità di dati. Grazie ai progressi più recenti, l'IA ha reso più agevole l'esecuzione di svariate attività, sia nel campo dell'informatica che in altri settori. In particolare, con l'avvento dell'Intelligenza Artificiale Generativa, i sistemi intelligenti hanno raggiunto livelli di prestazioni senza precedenti, essendo in grado di generare risultati originali basati sull'analisi dei dati di input. Questa tesi si propone di fornire una panoramica completa sull'IA, partendo dalla sua definizione fino alle tecnologie più avanzate impiegate, esaminando le sue potenzialità e i principali limiti che ancora presenta.

**Keyword:** Intelligenza Artificiale, Machine Learning, Deep Learning, Amazon Web Services, Riconoscimento di immagini, Traduzione automatica, IA Generativa

<b>Introduzione</b>	<b>1</b>
<b>1 Introduzione all'Intelligenza Artificiale</b>	<b>4</b>
1.1 Che cos'è l'Intelligenza Artificiale? . . . . .	4
1.1.1 Il Test di Turing . . . . .	5
1.1.2 Intelligenza artificiale debole e forte . . . . .	5
1.2 Storia dell'Intelligenza Artificiale . . . . .	6
1.2.1 Primi cenni relativi all'IA . . . . .	6
1.2.2 Nascita della disciplina . . . . .	7
1.2.3 L'Età d'oro dell'IA . . . . .	7
1.2.4 Dai primi fallimenti all'impiego nelle industrie . . . . .	8
1.2.5 L'Intelligenza Artificiale oggi . . . . .	8
1.3 Machine Learning e Deep Learning . . . . .	9
1.3.1 Machine Learning . . . . .	9
1.3.2 Reti neurali artificiali . . . . .	10
1.3.3 Reti neurali avanzate e Deep Learning . . . . .	11
1.3.4 I limiti delle reti neurali artificiali . . . . .	12
1.4 Applicazioni dell'Intelligenza Artificiale . . . . .	12
1.4.1 Informatica . . . . .	12
1.4.2 Intelligenza Artificiale e Data Science . . . . .	13
1.4.3 Robotica e automazione . . . . .	13
1.4.4 IA e medicina . . . . .	14
<b>2 Introduzione ad Amazon Web Services</b>	<b>16</b>
2.1 Amazon Web Services . . . . .	16
2.1.1 Introduzione alla piattaforma . . . . .	16
2.1.2 Breve storia ed evoluzione di AWS . . . . .	17
2.1.3 Principali servizi offerti . . . . .	18
2.1.4 Il ruolo di AWS nella collaborazione industriale . . . . .	19
2.2 Analisi dell'Infrastruttura Cloud di AWS . . . . .	20
2.2.1 Cloud Computing . . . . .	20
2.2.2 Principali tipologie di Cloud Computing proposte da AWS . . . . .	21
2.3 L'Impatto di Amazon Web Services sull'Intelligenza Artificiale . . . . .	22
2.3.1 Reti neurali impiegate da AWS . . . . .	23

2.3.2	Soluzioni per la modellazione e l'implementazione di algoritmi fornite da AWS . . . . .	25
2.3.3	Sviluppi futuri di AWS nel mondo dell'Intelligenza Artificiale . . . . .	25
<b>3</b>	<b>Introduzione alla Generative AI</b>	<b>26</b>
3.1	Intelligenza Artificiale Generativa . . . . .	26
3.1.1	Storia dell'IA Generativa . . . . .	27
3.2	Architettura dell'IA Generativa . . . . .	27
3.2.1	Variational AutoEncoder . . . . .	27
3.2.2	Generative Adversarial Network . . . . .	28
3.2.3	Transformer . . . . .	30
3.2.4	Diffusion model . . . . .	32
3.3	Applicazioni della IA Generativa nelle aziende . . . . .	33
3.3.1	Settore finanziario . . . . .	33
3.3.2	Settore sanitario . . . . .	34
3.3.3	Settore automobilistico . . . . .	34
3.3.4	Media e intrattenimento . . . . .	35
3.3.5	Settore energetico . . . . .	35
3.3.6	Telecomunicazioni . . . . .	35
3.4	Deepfake . . . . .	35
3.4.1	Deepfake visivi . . . . .	36
3.4.2	Deepfake audio . . . . .	37
3.4.3	Digital forgery detection . . . . .	37
<b>4</b>	<b>Riconoscimento di immagini</b>	<b>38</b>
4.1	Introduzione alla Computer Vision e all'Image Recognition . . . . .	38
4.1.1	Computer Vision . . . . .	38
4.1.2	Principali algoritmi di Computer Vision . . . . .	39
4.1.3	Image Recognition . . . . .	40
4.1.4	Vantaggi e applicazioni . . . . .	40
4.1.5	Limiti del riconoscimento di immagini . . . . .	41
4.2	Amazon Rekognition . . . . .	42
4.2.1	Funzionalità principali di Amazon Rekognition . . . . .	42
4.3	Analisi dei case study di Amazon Rekognition . . . . .	43
4.3.1	Rilevamento delle etichette . . . . .	43
4.3.2	Testo nell'immagine . . . . .	46
4.3.3	Analisi facciale . . . . .	48
<b>5</b>	<b>Traduzione dei testi</b>	<b>51</b>
5.1	Introduzione al Natural Language Processing . . . . .	51
5.1.1	Natural Language Processing . . . . .	51
5.1.2	Metodologie impiegate del processo NLP . . . . .	52
5.1.3	Funzionalità principali del Natural Language Processing . . . . .	53
5.1.4	Principali applicazioni aziendali . . . . .	54
5.2	Traduzione automatica . . . . .	54
5.2.1	Neural Machine Translation . . . . .	55
5.2.2	Esempi di applicazioni . . . . .	56
5.3	Traduzioni a confronto: Amazon Translate e DeepL . . . . .	56
5.3.1	Amazon Translate . . . . .	56
5.3.2	DeepL . . . . .	57
5.3.3	Vantaggi e limiti della NMT . . . . .	57

---

<b>6</b>	<b>Generative AI applicata all'arte</b>	<b>63</b>
6.1	Rapporto tra l'arte e l'IA Generativa . . . . .	63
6.1.1	Arte Generativa . . . . .	63
6.1.2	Principali tecniche impiegate . . . . .	64
6.2	Strumenti basati sull'IA Generativa . . . . .	64
6.2.1	ChatGPT-4 . . . . .	64
6.2.2	DALL-E . . . . .	65
6.3	01-IO: il punto di vista dell'Intelligenza Artificiale attraverso la sua arte . . .	66
6.3.1	IO-L'entità digitale . . . . .	66
6.3.2	Umanità riflessa . . . . .	69
6.3.3	Futuri possibili . . . . .	71
6.4	Principi etici riguardo l'Intelligenza Artificiale . . . . .	73
6.4.1	Principi fondamentali . . . . .	73
6.4.2	Tutela dei diritti intellettuali . . . . .	74
6.4.3	AI ACT . . . . .	75
<b>7</b>	<b>Discussione</b>	<b>77</b>
7.1	Discussione sul riconoscimento di immagini . . . . .	77
7.2	Discussione sulla traduzione dei testi . . . . .	78
7.3	Discussione sulla IA Generativa . . . . .	79
	<b>Conclusioni</b>	<b>80</b>
	<b>Bibliografia</b>	<b>82</b>
	<b>Sitografia</b>	<b>84</b>
	<b>Ringraziamenti</b>	<b>85</b>

---

## Elenco delle figure

---

1.1	IA, Machine Learning e Deep Learning . . . . .	9
1.2	Esempio di rete neurale artificiale . . . . .	10
1.3	Esempio di rete neurale artificiale avanzata, impiegata nel Deep Learning . .	11
2.1	Panoramica sui servizi offerti da AWS . . . . .	17
2.2	Zone di disponibilità del servizio . . . . .	19
2.3	Architettura del Cloud Computing . . . . .	21
3.1	Struttura di un Variational AutoEncoder . . . . .	28
3.2	Architettura di una Generative Adversarial Network . . . . .	29
3.3	Architettura di un Transformer . . . . .	31
3.4	Processo di elaborazione di un Diffusion model . . . . .	32
4.1	Fotografia di Jannik Sinner . . . . .	44
4.2	Risultati relativi alla Figura 4.1 . . . . .	44
4.3	Immagine illusoria con relativi risultati . . . . .	45
4.4	Ritratto di Leonardo di Caprio con i relativi risultati . . . . .	45
4.5	Fotografia di Leonardo di Caprio con i relativi risultati . . . . .	45
4.6	Immagine con citazione di Alan Turing con relativi risultati . . . . .	47
4.7	Primo esempio di CAPTCHA con i relativi risultati . . . . .	47
4.8	Secondo esempio di CAPTCHA con i relativi risultati . . . . .	48
4.9	Primo esempio di immagine con i relativi risultati . . . . .	49
4.10	Secondo esempio di immagine con i relativi risultati . . . . .	50
4.11	<i>Le stiratrici</i> di Edgar Degas con i relativi risultati . . . . .	50
5.1	Esempio di albero sintattico con l'indicazione delle categorie sintattiche delle parole . . . . .	53
6.1	Nucleo Aureo . . . . .	67
6.2	La Fine di un Pensiero . . . . .	67
6.3	Le Mani della Creazione . . . . .	69
6.4	Quarto Stato . . . . .	71
6.5	Quinto Stato . . . . .	71

---

## Elenco delle tabelle

---



L'Intelligenza Artificiale (IA) rappresenta una delle frontiere più rivoluzionarie del tempo contemporaneo, influenzando settori cruciali, come la sanità, l'industria, l'educazione e molti altri. La sua capacità di elaborare dati su vasta scala e di apprendere autonomamente permette di affrontare problemi complessi con efficienza e precisione, aprendo nuove strade per il progresso scientifico e tecnologico.

Le potenzialità dell'Intelligenza Artificiale sono evidenti in numerosi ambiti. In medicina, ad esempio, gli algoritmi di IA sono in grado di analizzare immagini diagnostiche con una precisione spesso superiore a quella umana, consentendo diagnosi più rapide e accurate. Nella finanza, l'IA può prevedere tendenze di mercato e ottimizzare investimenti, migliorando la gestione del rischio. Anche nell'industria manifatturiera, l'automazione intelligente permette di ottimizzare la produzione, ridurre i costi e migliorare la qualità dei prodotti. Questi esempi dimostrano come l'Intelligenza Artificiale possa contribuire significativamente al miglioramento della qualità della vita, rendendo processi complessi più efficienti e affidabili.

Tuttavia in questa tesi, la scelta di esplorare il mondo dell'Intelligenza Artificiale non si basa solo sull'analisi delle sue potenzialità, ma anche sulla consapevolezza dei suoi limiti e delle sfide etiche e pratiche che essa comporta. Soprattutto con la nascita dell'Intelligenza Artificiale Generativa, per la prima volta l'essere umano si ritrova a confrontarsi con un sistema intelligente in grado di creare risultati originali in diversi ambiti, come quello dell'arte. Uno dei limiti principali risiede proprio nell'originalità dei contenuti prodotti. Infatti, la creatività dell'IA si limita alla sua capacità di analizzare ed elaborare il dataset di addestramento; i suoi risultati sono frutto del rifacimento di informazioni e pattern già esistenti. L'efficacia di qualsiasi sistema di IA è strettamente legata alla qualità e alla quantità dei dati su cui esso viene addestrato. Dati di scarsa qualità o non rappresentativi possono portare a risultati inaccurati o parziali, compromettendo l'affidabilità delle soluzioni proposte. Inoltre, la necessità di grandi quantità di dati può comportare problemi di privacy e sicurezza.

Sono numerosissime le questioni etiche riguardanti l'Intelligenza Artificiale che si aprono. Infatti, l'uso dell'IA Generativa può portare alla diffusione di informazioni false o fuorvianti. La capacità di generare testi e immagini realistiche, ma completamente inventate, può essere sfruttata per creare notizie false e manipolare l'opinione pubblica. Tutto questo evidenzia la necessità di sviluppare sistemi di verifica e legislativi che permettano un corretto utilizzo dei sistemi intelligenti da parte della società.

Questa tesi, dunque, si pone l'obiettivo di esplorare un ambito tecnologico di grande impatto, come l'Intelligenza Artificiale, permettendo una maggiore comprensione di questo mondo, evidenziando le sue potenzialità e i suoi limiti.

Infatti, questa tesi tratterà in maniera esaustiva i vari aspetti dell'Intelligenza Artificiale,

delineando inizialmente una sua definizione, approfondendo concetti come quello del Test di Turing, il principale sistema di analisi impiegato per comprendere se un sistema sia effettivamente intelligente. Verrà, poi, esplorata la storia dell'IA, partendo dalla nascita della disciplina fino a giungere all'età contemporanea. Si approfondiranno concetti di Machine Learning e Deep Learning, analizzando le reti neurali artificiali, ovvero la principale tecnica implementativa impiegata. Dopo aver enunciato i principali settori applicativi, che spaziano dall'informatica alla robotica, l'attenzione verrà spostata sulla piattaforma di Amazon Web Services (AWS), l'infrastruttura cloud in grado di offrire numerosi servizi di Intelligenza Artificiale che verranno utilizzati per effettuare le successive analisi.

Infatti, dopo aver introdotto il concetto di Computer Vision, verranno proposte le analisi effettuate mediante Amazon Rekognition, il servizio di AWS che consente di effettuare l'analisi di immagini e video mediante l'Intelligenza Artificiale.

Si proseguirà con un'introduzione al Natural Language Processing (NLP) e alle principali metodologie impiegate. Dopo aver approfondito il campo della traduzione automatica, verranno presentati i risultati ottenuti mediante Amazon Translate e DeepL, uno dei traduttori più utilizzati a livello aziendale.

A partire dai risultati ottenuti dalle analisi effettuate, sono stati evidenziati numerose potenzialità e diversi limiti dei servizi proposti.

Infine, verrà esplorato un nuovo settore in forte crescita negli ultimi anni, ovvero quello dell'Intelligenza Artificiale Generativa. Dopo averne illustrato la storia e le principali reti neurali impiegate, come i Variational AutoEncoder, le Generative Adversarial Network, i Transformer e i Diffusion Model, verranno studiate le sue applicazioni, discutendo le conseguenze che questa nuova tecnologia ha apportato sul mondo del lavoro e sulla società.

Dopo aver discusso del rapporto che sussiste tra l'IA Generativa e il mondo dell'arte, proponendone diversi esempi applicativi, realizzati con strumenti come ChatGpt-4 e DALL-E, verranno discusse le principali implicazioni etiche, derivate dalla nascita di questa disciplina. Verrà sottolineata l'importanza di impiegare questo strumento in modo critico e responsabile, rimanendo consapevoli sia delle sue potenzialità che dei suoi limiti.

La presente tesi è composta da otto capitoli strutturati come di seguito specificato:

- Nel Capitolo 1 verrà introdotto il concetto di Intelligenza Artificiale, esplorando la sua storia ed evoluzione. Verranno proposte le principali tecnologie utilizzate nel Machine Learning e nel Deep Learning, soffermandosi, in particolare, sul concetto di rete neurale artificiale. Infine, verranno enunciate alcune applicazioni di questo sistema nel mondo del lavoro.
- Nel Capitolo 2, dopo aver proposto una spiegazione inerente al Cloud Computing, verrà descritta la piattaforma di Amazon Web Services e i principali servizi che essa offre.
- Nel Capitolo 3 verrà fornita una spiegazione inerente all'IA Generativa, soffermandosi, in particolare, sulle reti neurali più utilizzate e sulle sue applicazioni. Infine, verrà proposto un breve *excursus* sui deepfake, per introdurre le prime considerazioni etiche sull'IA.
- Nel Capitolo 4 verranno descritte le analisi effettuate mediante Amazon Rekognition nell'ambito del riconoscimento di immagini.
- Nel Capitolo 5 verranno enunciati i risultati ottenuti mediante Amazon Translate, proponendo un confronto con il traduttore DeepL, al momento considerato il migliore al mondo.

- Nel Capitolo 6 verrà descritto il rapporto che sussiste tra l'IA Generativa e il mondo dell'arte. Dalle considerazioni effettuate verranno discusse le implicazioni etiche che l'utilizzo di questi sistemi comporta.
- Nel Capitolo 7 verranno discussi i risultati ottenuti dalle analisi effettuate nei capitoli precedenti.
- Nel Capitolo 8 verranno tratte le conclusioni relative alla ricerca effettuata, delineando i possibili sviluppi futuri di questa tecnologia.

---

## Introduzione all'Intelligenza Artificiale

---

*In questo capitolo, si propone un'introduzione all'Intelligenza Artificiale (IA). Si comincerà analizzando il concetto stesso di IA e il suo significato, per poi esaminare il suo sviluppo nel corso del tempo, passando dalle origini fino all'età moderna. Successivamente, si approfondiranno le metodologie di Machine Learning e Deep Learning, fondamentali per il funzionamento e l'evoluzione dei sistemi di IA. Infine, si tratterà un quadro generale delle applicazioni attuali e future.*

### 1.1 Che cos'è l'Intelligenza Artificiale?

Per millenni, l'essere umano ha cercato di studiare e comprendere i meccanismi che regolano l'intelligenza umana, ovvero l'insieme di capacità psichiche e mentali che consentono all'uomo di riflettere, capire e agire nel mondo che lo circonda. In tempi più recenti, l'umanità si è posta l'obiettivo di realizzare macchine "pensanti", in grado di svolgere azioni e prendere decisioni in modo del tutto simile all'uomo.

"*Can machines think?*" questa è la domanda che si pose il matematico Alan Turing nel 1950, e questa è la questione che si posero tutti i ricercatori che contribuirono, in un modo o nell'altro alla nascita dell'Intelligenza Artificiale, o IA. A darne la prima definizione, è stato John McCarthy, che coniò il termine nel 1956. Infatti, la definisce come:

*"La scienza e l'ingegneria della creazione di macchine intelligenti."*

Il campo è stato fondato sulla convinzione che l'intelligenza, una delle proprietà caratteristiche dell'essere umano, possa essere descritta così dettagliatamente da poter essere simulata da una macchina. Grazie ai risultati conseguiti recentemente nel campo della tecnologia, sia nel calcolo computazionale che nelle capacità di analisi di enormi quantità di dati, l'IA ha avuto un crescente sviluppo. Insieme a quest'ultima sono nate numerose controversie etiche e sociali riguardo la distinzione tra intelligenza umana e quella artificiale. Nel 2014, durante un'intervista rilasciata alla BBC, lo scienziato Stephen Hawking affermava come l'Intelligenza Artificiale fosse una minaccia per la sopravvivenza dell'umanità, considerando lo sviluppo che avrebbe raggiunto in futuro. Altri studiosi, invece, affermarono come l'intelligenza sviluppata da una macchina, per quanto avanzata, non avrebbe mai potuto raggiungere quella umana, rimanendone così una mediocre imitazione.

### 1.1.1 Il Test di Turing

Per determinare se una macchina possa effettivamente mostrare un comportamento intelligente, il matematico Alan Turing nel 1950 propose un test, noto come *Test di Turing*. Esso si basa su un gioco, noto come "*The Imitation Game*", che prevede tre partecipanti: un uomo (A), una donna (B) e una terza persona (C). Quest'ultima, tenuta separata dalle altre due, tramite una serie di domande, deve determinare quale persona sia l'uomo e quale la donna. Gli altri due partecipanti, invece, hanno dei ruoli differenti: A deve ingannare il giocatore C per cercare di portarlo a un'identificazione errata, mentre B deve aiutarlo nel suo intento. Per garantire che C non possa beneficiare di alcun indizio, come l'analisi della grafia o della voce, per regola, le risposte alle domande devono essere trascritte in forma dattiloscritta o trasmesse in modo simile. Il test di Turing si fonda sull'idea che, al posto del partecipante A, si possa sostituire una macchina. Se la percentuale di successo di C nell'identificare l'uomo e la donna è simile, prima e dopo la sostituzione di A con la macchina, allora quest'ultima dovrebbe essere considerata intelligente, portandola ad essere indistinguibile da un essere umano.

Il "Test di Turing classico", descritto in precedenza, evita intenzionalmente l'interazione diretta tra l'esaminatore e il computer, eliminando la necessità di simulare fisicamente una persona umana. Tuttavia, esiste il concetto di "Test di Turing totale", presente in letteratura, che incorpora un segnale video per consentire all'esaminatore di valutare le capacità percettive dell'individuo. Questa versione del test include anche la possibilità di scambiare oggetti fisici attraverso una finestrella. Affinché una macchina possa superare l'esame, sarà necessario dotarla di visione artificiale per percepire l'ambiente e gli oggetti circostanti, oltre a qualche forma di applicazione robotica per manipolare gli oggetti e spostarsi.

Il Test di Turing è stato considerato un esperimento mentale di grande importanza e ha alimentato discussioni riguardanti l'intelligenza e la coscienza fino al 1991, quando è stato effettivamente applicato e testato per la prima volta. Il pioniere di questa iniziativa fu Hugh Loebner, programmatore e imprenditore, che istituì un premio in denaro da assegnare al primo computer in grado di superare il test, noto come *Loebner Prize Competition*. Questa è una competizione annuale rivolta ai chatbot, le cui regole hanno subito dei cambiamenti nel tempo, passando dal Test di Turing, che sfruttava conversazioni limitate, a discussioni illimitate dal 1995. Alcune edizioni del concorso hanno incluso domande di screening per valutare lo stato della tecnologia. Tra i programmi che hanno conseguito il premio bisogna ricordare *PC Therapist* di Joseph Weintraub e *A.L.I.C.E. (Artificial Linguistic Internet Computer Entity)* di Richard Wallace. Tuttavia, il premio ha ricevuto critiche da esperti del settore. Marvin Minsky, ad esempio, offrì ironicamente un premio per chiunque potesse fermare la competizione.

### 1.1.2 Intelligenza artificiale debole e forte

Sin dagli albori, l'Intelligenza Artificiale ha fatto sorgere il problema di riuscire a rappresentare le tante sfaccettature dell'intelligenza umana. Partendo dallo studio del funzionamento del cervello, gli studiosi hanno cercato di realizzare un prodotto in grado di agire e pensare umanamente e razionalmente, utilizzando funzioni cognitive artificiali in modo del tutto simile a un essere umano. Per poter sviluppare un sistema così complesso, la ricerca ha preferito suddividere lo studio delle proprietà di una macchina intelligente in sotto-problemi. La distinzione più emblematica è quella di Intelligenza Artificiale debole e Intelligenza Artificiale forte, a seconda che vengano riprodotte solo alcune o tutte le funzionalità della mente umana. In particolare, si ricorda che:

- *L'Intelligenza Artificiale debole* comprende tutti i sistemi in grado di svolgere compiti specifici e limitati, senza possedere la complessità e la flessibilità propri dell'intelligenza

umana. In questo caso, il computer è considerato uno strumento estremamente potente utilizzato nello studio della mente, che ci consente di formulare e verificare ipotesi in modo più preciso e rigoroso. L'IA stessa, nel momento in cui è stata progettata per la prima volta, è stata concepita come "debole".

- *L'Intelligenza Artificiale forte* racchiude tutti i sistemi complessi capaci di emulare i processi e le capacità cognitive dell'uomo. Il filosofo statunitense J.R Searle affermava che:

*"Secondo l'IA forte, invece, il calcolatore non è semplicemente uno strumento per lo studio della mente, ma piuttosto, quando sia programmato opportunamente, una vera mente; e cioè è possibile affermare che i calcolatori, una volta corredati dei programmi giusti, letteralmente capiscono e posseggono altri stati cognitivi"*

Attualmente, sono stati molteplici i progressi apportati al campo dell'Intelligenza Artificiale, come sono svariati gli ambiti toccati da questa disciplina. Inoltre, recentemente sono state poste le prime basi per ipotizzare quella che oggi è nota come ASI (*Artificial Superintelligence*), o *Superintelligenza*. Questa forma supera l'IA forte in termini di intelligenza e capacità umane. Tuttavia, la Superintelligenza è ancora una speculazione, visto che ancora oggi non abbiamo raggiunto nemmeno la possibilità di costruire dispositivi dotati di Intelligenza Artificiale forte.

## 1.2 Storia dell'Intelligenza Artificiale

L'uomo, sin dall'antichità, si è occupato dello studio delle funzionalità cognitive umane. Partendo dall'analisi biologica del cervello, per finire a ricostruire la logica del pensiero, tramite il linguaggio matematico, sono stati numerosi gli studiosi che hanno contribuito alla nascita dell'attuale Intelligenza Artificiale. In questo capitolo, si propone un *excursus* sulla nascita di questa disciplina, per fornire un ampio prospetto della sua evoluzione.

### 1.2.1 Primi cenni relativi all'IA

Sono state molteplici le fasi che hanno portato alla nascita di questa disciplina. Infatti, già molto prima dell'esordio del primo calcolatore, molti studiosi iniziarono a formulare l'ipotesi della creazione di una macchina intelligente. La stessa parola *autonomia* deriva dal greco *autòmatos*, il quale significa "che si governa da sé". Infatti, furono proprio gli antichi greci a cimentarsi nella creazione di macchine che potessero agire da sole, senza l'intervento umano, risolvendo innumerevoli questioni nel campo dell'ingegneria, e non solo. Insieme a queste creazioni, crebbe sempre di più l'idea di rendere queste attrezzature "pensanti". Sicuramente, tra i vari studiosi va ricordato Erone di Alessandria, che nel suo trattato *Automata*, risalente al I secolo d.C., proponeva alcuni studi effettuati su delle macchine semoventi; tra queste si ricorda quella che oggi è stata definita come *La macchina di Erone*, opera ingegneristica prodigiosa in grado di aprire le imponenti porte di un tempio, sfruttando i principi dell'idraulica.

Assieme a lui, vanno ricordati tutti i matematici e fisici, che all'epoca hanno fornito le basi per l'algebra e la logica, risultate fondanti dell'informatica, e quindi dell'Intelligenza Artificiale. Tra questi si cita Aristotele (384-322 a.C.), il quale, con i suoi sillogismi, ha posto le basi per la logica dei predicati, essenziale per l'analisi del linguaggio e del pensiero umano.

Tra gli scienziati dei secoli successivi vanno menzionati: Leonardo da Vinci (1452-1519), che progettò il primo calcolatore meccanico<sup>1</sup>, e i matematici Blaise Pascal e Gottfried Wilhelm von Leibniz, i quali, all'alba del XVII secolo, costruirono le prime macchine in grado di effettuare semplici operazioni matematiche in modo automatico.

### 1.2.2 Nascita della disciplina

Il primo lavoro riguardante l'Intelligenza Artificiale è stato svolto da Warren McCulloch e Walter Pitts, i quali, nel 1943, crearono il primo modello di neuroni artificiali. Questo incredibile risultato, fu raggiunto grazie al contributo di altri studi effettuati precedentemente; tra questi va ricordato l'articolo di Alan Turing, redatto nel 1936, *On Computable Numbers, With An Application To The Entscheidungsproblem*, che pose le basi per concetti quali la calcolabilità, la computabilità e la macchina di Turing, definizioni tuttora cruciali per lo sviluppo degli attuali calcolatori.

Come precedentemente detto, il sistema, creato da McCulloch e Pitts, si basava sull'utilizzo di neuroni artificiali. Questi ultimi avevano un funzionamento del tutto simile a un interruttore che, in presenza di stimoli, passava dallo stato "Off" allo stato "On". Venne dunque dimostrato che tutti i connettivi logici<sup>2</sup> e, di conseguenza, le frasi proprie del linguaggio umano, potevano essere trattati da una struttura neurale artificiale. Nel 1950, due studenti dell'Università di Harvard, Marvin Minsky e Dean Edmonds svilupparono la SNARC, che è considerata oggi la prima rete neurale artificiale. Successivamente, nel 1956, su iniziativa di John McCarthy, una delle figure di spicco nel campo della computazione, Marvin Minsky, Claude Shannon e Nathaniel Rochester e lo stesso McCarthy si riunirono nel New Hampshire, al Dartmouth College, per organizzare un team, che in due mesi avrebbe dovuto creare una macchina in grado di simulare l'intelligenza umana. Questa idea portò, inoltre, alla nascita del *Logic Theorist* di Allen Newell e Herber Simon, un software in grado di dimostrare i teoremi matematici presenti nel testo *Principia Mathematica* di Russell e Whitehead.

Durante questo convegno McCarthy coniò per la prima volta l'espressione *Intelligenza Artificiale*, fatto che segnò l'inizio di questa disciplina.

### 1.2.3 L'Età d'oro dell'IA

Il software sviluppato da Newell e Simon segnò un passo avanti significativo, portando alla nascita del programma *General Problem Solver* o *GPS*. A differenza del *Logic Theorist*, il GPS fu concepito con l'obiettivo di emulare i processi di risoluzione dei problemi utilizzati dagli esseri umani. Nello stesso periodo IBM iniziò lo sviluppo di altri programmi in grado di ragionare autonomamente. Nel 1959, l'informatico Herbert Gelernter costruì il *Geometry Theorem Prover*, un software in grado di dimostrare teoremi matematici. Nello stesso periodo, McCarthy formulò quello che sarebbe diventato il linguaggio di riferimento per lo sviluppo di algoritmi di Intelligenza Artificiale dei successivi trent'anni: *Lisp*. Assieme a quest'ultimo, nel *Programs with Common Sense*, avanzò la prima proposta di un programma basato su IA, noto come *Advice Taker*. A differenza di quelli precedenti, questo software si poneva l'obiettivo di risolvere problemi che esulassero dal mondo matematico. Questo fu il primo programma che tentò di emulare in ogni aspetto le capacità cognitive umane. Successivamente ogni

<sup>1</sup>Il calcolatore meccanico non venne mai costruito da Leonardo da Vinci; recenti studi hanno, però, dimostrato che il progetto era, tuttavia, funzionante.

<sup>2</sup>I connettivi logici sono elementi grammaticali di collegamento fra due proposizioni A e B. Questi vanno a instaurare una relazione che dà origine a una terza proposizione C, la quale assume valore "vero" o "falso", in base ai valori delle due proposizioni e al carattere del connettivo utilizzato. Essi sono operatori fondamentali per l'algebra booleana, la quale fu presentata nel 1847 da George Boole nel suo libro *The Mathematical Analysis of Logic*, con l'obiettivo di scrivere in forma algebrica la logica proposizionale

ricercatore provò a creare una macchina che potesse pensare esattamente come un essere umano. Addirittura nel 1957, Herbert Simon affermò che:

*“ It is not my aim to surprise or shock you – but the simplest way I can summarize is to say that there are now in the world machines that think, that learn and that create. Moreover, their ability to do these things is going to increase rapidly until – in a visible future – the range of problems they can handle will be coextensive with the range to which the human mind has been applied”<sup>3</sup>.*

La previsione effettuata da Simon si realizzò, però, solo quarant'anni dopo, quando il computer Deep Blue sconfisse il giocatore di scacchi Kasparov.

#### 1.2.4 Dai primi fallimenti all'impiego nelle industrie

Diverse furono le problematiche riscontrate nello sviluppo di programmi basati su Intelligenza Artificiale. Prime fra tutte, l'incapacità delle macchine di possedere degli algoritmi in grado di acquisire una conoscenza semantica che si allontanasse dagli assiomi matematici, su cui si basavano i primi programmi. Il pessimismo crebbe nel momento in cui il governo dei Stati Uniti decise di tagliare i fondi per lo sviluppo di macchine traduttrici, fatto che diede un duro colpo allo sviluppo della disciplina.

Le innovazioni nel campo dell'IA risultarono piuttosto marginali fino al 1982, quando la Digital Equipment, azienda leader nel settore informatico, impiegò il primo sistema di Intelligenza Artificiale, noto come R1. Da quel momento in poi, ogni industria mondiale investì in risorse basate su IA. Da menzionare è il Giappone, che nel 1981 annunciò il progetto *Fifth Generation*, piano che aveva come obiettivo quello di realizzare sistemi intelligenti utilizzando il linguaggio di programmazione Prolog. In risposta a questo clima rivoluzionario, il governo degli Stati Uniti creò il *Microelectronics and Computer Technology Corporation (MCC)*, così da mantenere un costante sviluppo in ambito di Intelligenza Artificiale.

A metà degli anni ottanta, venne ripreso il modello di reti neurali *back-propagation*, proposto per la prima volta da Bryson e Ho nel 1969. Quest'ultimo risultò vincente in ogni ambito, dall'informatica alla psicologia, in quanto risolse innumerevoli problematiche che i modelli simbolici<sup>4</sup>, ideati da Newell, Simon, e poi McCarthy, non erano riusciti a trattare.

#### 1.2.5 L'Intelligenza Artificiale oggi

Al giorno d'oggi, l'IA ha subito uno sviluppo senza precedenti, tanto da essere utilizzata non solo dalle grandi aziende, per gestire i propri processi produttivi, ma anche comunemente da persone non esperte del settore. Infatti, soprattutto negli ultimi anni, sono stati sviluppati dei sistemi interamente basati su IA. Tra i più celebri vanno menzionati *Deep Blue*, computer realizzato da IBM negli anni novanta, in grado di confrontarsi con i migliori giocatori di scacchi, e *Remote Agent*, impiegato dalla NASA per gestire le attività relative a un sistema spaziale. Successivamente si è visto persino lo sviluppo di sistemi di guida autonoma, portati avanti da compagnie del calibro di Tesla e Uber. Altro campo che ha visto un notevole sviluppo è stato quello dei chatbot, ovvero dei software in grado di simulare ed elaborare le

---

<sup>3</sup>“Non è mia intenzione sorprendervi o scioccarvi, ma il modo più semplice in cui posso riassumere è dire che ora nel mondo ci sono macchine che pensano, che imparano e che creano. Inoltre, la loro capacità di fare queste cose aumenterà rapidamente fino a quando - in un futuro visibile - la gamma di problemi che possono gestire sarà coesa con la gamma [di ambiti] a cui è stata applicata la mente umana”. (Trad. di DeepL)

<sup>4</sup>L'intelligenza artificiale simbolica si riferisce ai metodi utilizzati nella ricerca sull'Intelligenza Artificiale che si fondano su rappresentazioni "simboliche" dei problemi, comprensibili per gli esseri umani, sulla logica e sulla ricerca. Questo approccio è stato il paradigma predominante nella ricerca sull'IA dalla metà degli anni '50 alla fine degli anni '80.



conversazioni umane, consentendo agli utenti di interagire con i dispositivi digitali come se stessero comunicando con una persona reale. Tra i più famosi vanno citati ELIZA, uno dei primi chatbot mai creati, risalente al 1966, Cleverbot e Siri, implementati nel 2010, e infine ChatGPT, realizzato da OpenAI, il quale risulta oggi uno dei più avanzati sul mercato.

## 1.3 Machine Learning e Deep Learning

Molto spesso, quando si parla di Intelligenza Artificiale, si rischia di utilizzare termini come *Machine Learning* e *Deep Learning* in modo improprio, a volte come sinonimo della stessa IA. Questi ultimi, in realtà, risultano essere due dei pilastri su cui si fonda l'intera teoria e, quindi, parte integrante dell'Intelligenza Artificiale, come si può visualizzare nella Figura 1.1, dalla quale si può evincere come i tre settori siano relazionati.

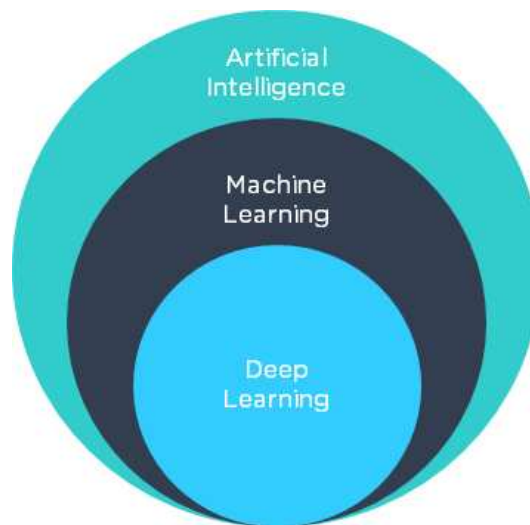


Figura 1.1: IA, Machine Learning e Deep Learning

### 1.3.1 Machine Learning

Il *Machine Learning* è una branca dell'IA che si pone l'obiettivo di sviluppare algoritmi intelligenti, in grado di trarre conoscenze e prendere decisioni in modo completamente autonomo, acquisendo tutte le nozioni necessarie dai dati, che vengono passati in ingresso. In particolare, utilizzando delle metodologie proprie della statistica, gli algoritmi vengono addestrati affinché possano acquisire più conoscenze possibili e, dunque, fornire delle risposte adeguate e conformi allo scopo. Le caratteristiche e l'accuratezza dei dati svolgono, perciò, un ruolo decisivo nel corretto funzionamento di un modello di apprendimento automatico.

A seconda della tipologia di ingresso e all'obiettivo perseguito dal sistema, la disciplina assume tre forme principali:

- *apprendimento supervisionato*, il cui obiettivo è quello di estrarre una regola che correli uno specifico ingresso all'output corretto;
- *apprendimento non supervisionato*, il cui scopo è quello di trovare una struttura specifica per gli input forniti, senza che questi vengano prima classificati;
- *apprendimento per rinforzo*, in cui il modello interagisce con un ambiente dinamico, cercando di portare a termine diversi obiettivi di natura complessa.

Attraverso delle metriche di valutazione, che si occupano di esaminare la precisione e l'accuratezza dell'algoritmo, viene rilasciato un feedback dal quale è possibile trarre diverse conclusioni sul corretto funzionamento del modello.

### 1.3.2 Reti neurali artificiali

Una rete neurale artificiale (ANN, *Artificial Neural Network*) è un modello matematico e informatico, sviluppato per la prima volta da Warren McCulloch e Walter Pitts nel 1943, su cui si basano molti degli algoritmi di *Machine Learning*. Per la loro creazione, gli studiosi si sono ispirati alle reti neurali biologiche. Infatti, nel cervello umano, i neuroni si connettono tramite le sinapsi, permettendo il ragionamento e il controllo del corpo. Una rete neurale artificiale, invece, presenta una struttura più limitata, ma comunque affine. I componenti principali sono i nodi e gli archi. Nei primi vengono effettuate delle funzioni (dette funzioni di attivazione), in grado di svolgere operazioni algoritmiche, che possono essere sia semplici che complesse. Invece, gli archi, come le sinapsi, consentono i collegamenti tra i vari nodi. Ciascun arco è caratterizzato da un peso sinaptico, il quale consente di trattare i dati ricevuti dal nodo di ingresso, per poi passare il risultato a quello di uscita.

I nodi possono essere suddivisi in tre tipologie principali, come riportato nella Figura 1.2:

- *input node* utilizzati per introdurre i dati dell'addestramento;
- *hidden node*, detti anche stati della rete (o livelli), in quanto non si trovano né in ingresso né in uscita;
- *output node* impiegati per restituire il risultato.

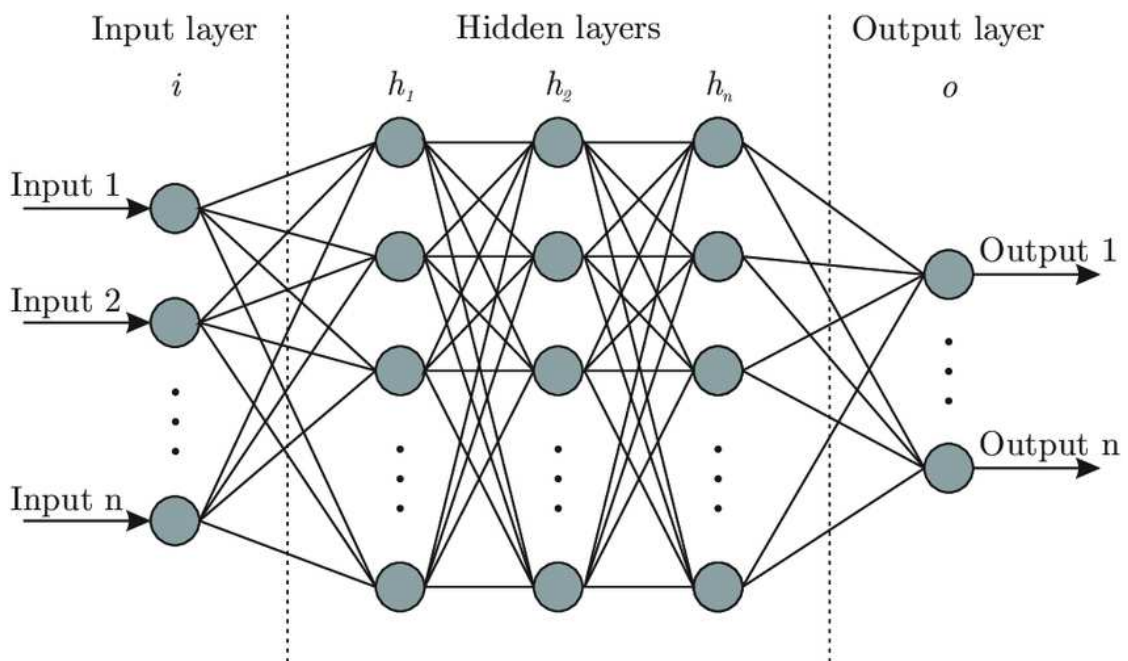


Figura 1.2: Esempio di rete neurale artificiale

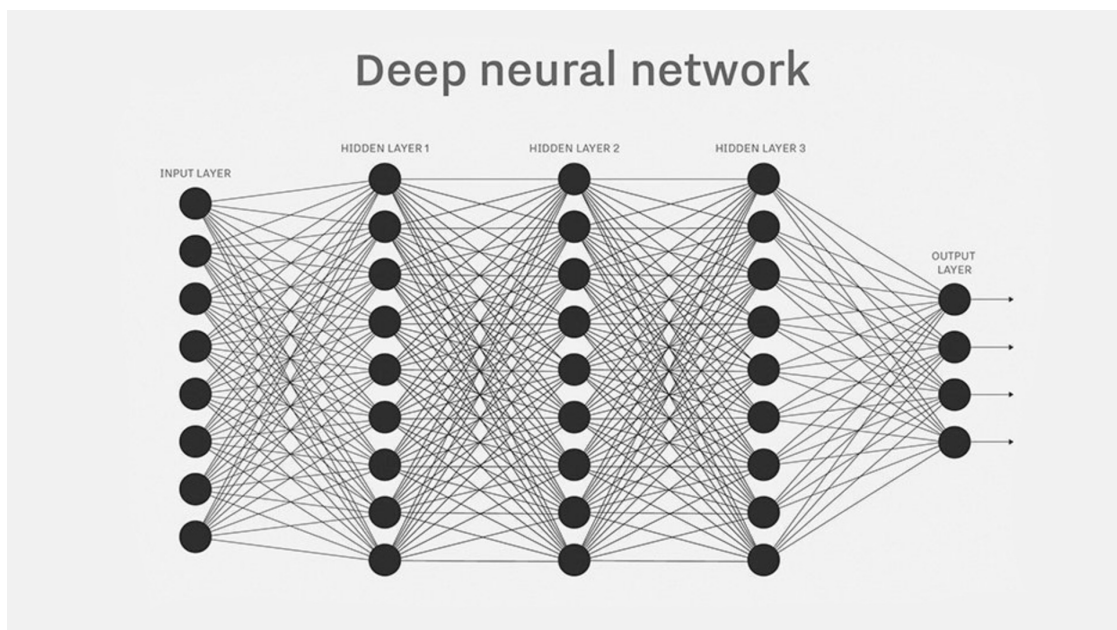
La stessa propagazione della rete neurale può presentare diverse forme e complessità. Si passa dalla propagazione in avanti (*feed-forward*), in cui il dato viene trasportato in un percorso aciclico, dai nodi di sinistra verso quelli di destra, per arrivare alla propagazione all'indietro (*back-propagation*), in cui il passaggio dell'informazione può avvenire verso il nodo immediatamente precedente o successivo. Ciò ha dato luogo alla nascita delle reti

neurali più complesse, in quanto tale tipo di propagazione ammette anche la presenza di cicli. Quest'ultima tipologia viene, in genere, impiegata per incrementare la precisione del risultato prodotto durante l'attività di apprendimento. Una volta raggiunto un livello di correttezza soddisfacente, e dopo aver aggiornato i pesi sugli archi della rete, si passa alla propagazione in avanti, proseguendo verso i nodi successivi.

### 1.3.3 Reti neurali avanzate e Deep Learning

Il *Deep Learning* è una branca del Machine Learning. Infatti, a differenza di quest'ultimo, esso utilizza delle reti neurali molto avanzate. A differenza delle reti utilizzate nel Machine Learning, quelle impiegate nel Deep Learning presentano un maggior numero di livelli di *hidden node*. Queste reti possono essere impiegate con un'ingente quantità di dati, che possono presentare una struttura anche molto complessa. Infatti, sono spesso impiegate nella Data Analysis per studiare la natura dei dati e per trarre delle previsioni su risultati futuri. A differenza delle reti impiegate dal Machine Learning, che sono basate su un livello di apprendimento più superficiale e autoconclusivo, quelle impiegate dal Deep Learning riescono a incrementare di volta in volta il livello di precisione dei risultati forniti, imparando elementi nuovi ogni volta che viene passato in ingresso un nuovo insieme di dati.

Nella Figura 1.3 si può osservare un esempio di rete neurale avanzata, in cui si possono notare i multi-livelli di hidden node, caratteristici del Deep Learning.



**Figura 1.3:** Esempio di rete neurale artificiale avanzata, impiegata nel Deep Learning

Tra le reti neurali avanzate principali è bene menzionare:

- Le *Recurrent Neural Networks (RNN)*, utilizzate per problemi di tipo ordinale e temporale, come il *Natural Language Processing*;
- Le *Convolution Neural Network (CNN)*, impiegate per l'elaborazione di dati di tipo visivo;
- Le *Generative Adversarial Network (GAN)*. in grado di creare immagini realistiche, basandosi su un input testuale o su figure già esistenti.

Il Deep Learning, a differenza del Machine Learning, necessita, quindi, di una capacità computazionale immensa. Infatti, questo rimane uno dei limiti più pesanti di questo campo, che, però, è tuttora una delle tecnologie più utilizzate e in crescente sviluppo.

### 1.3.4 I limiti delle reti neurali artificiali

Oltre alle ingenti capacità computazionali richieste, nonostante il crescente sviluppo dell'IA negli ultimi anni, gli algoritmi di Machine Learning e Deep Learning presentano ancora oggi dei limiti non trascurabili. Un esempio può essere fornito dall'approccio "black-box", con cui le reti neurali affrontano l'estrazione del risultato. Infatti, molto spesso diventa particolarmente complesso, se non impossibile, dare una spiegazione del risultato prodotto. Questo rende ancora più enigmatico il motivo della presenza di determinate conseguenze piuttosto che altre. Uno dei problemi principali rimane l'errata interpretazione dei dati, che a volte può portare la rete neurale a restituire delle conclusioni del tutto sbagliate. A questo si ricollega un'altra questione, ovvero l'*overfitting*. Le reti neurali, adattandosi ai dati che vengono forniti in input, possono produrre dei risultati standardizzati, rendendo difficoltosa la capacità di generare prodotti sempre nuovi e, soprattutto, corretti.

## 1.4 Applicazioni dell'Intelligenza Artificiale

L'avvento dell'Intelligenza Artificiale ha apportato una vera e propria rivoluzione in numerosi campi, industriali e non. Un esempio sono i sistemi di Smart Home<sup>5</sup>, che consentono di gestire la casa in modo intelligente, permettendo, in particolare, di regolare la temperatura e l'illuminazione degli alloggi, garantendo uno stile di vita più confortevole. Le applicazioni basate su IA sono caratterizzate da una diffusione piuttosto diversificata, strettamente dipendente dal settore di interesse e dalle tecnologie al momento disponibili. A seguire, si riportano alcuni campi in cui l'IA ha apportato dei cambiamenti significativi, spaziando dall'informatica alla robotica.

### 1.4.1 Informatica

L'Intelligenza Artificiale è stata integrata in molteplici campi dell'informatica. A partire dallo sviluppo software, l'IA ha permesso di creare algoritmi che generino autonomamente un codice efficiente e una documentazione corretta e completa. Inoltre, ha garantito un supporto nella fase di test e validazione del codice, riducendo, così, i futuri costi di manutenzione del prodotto.

L'Intelligenza Artificiale, inoltre, sta rivoluzionando il settore della sicurezza informatica, fornendo soluzioni avanzate per proteggere le infrastrutture digitali da minacce sempre più sofisticate. Alcune delle aree della cybersecurity toccate dall'IA sono, ad esempio:

- *Il rilevamento e prevenzione delle minacce*: i sistemi basati su IA analizzano grandi quantità di dati per individuare modelli e anomalie, consentendo di identificare minacce note e nuovi vettori di attacco che sfuggono ai sistemi tradizionali.
- *L'analisi del comportamento*: l'IA monitora il comportamento degli utenti e il traffico di rete per individuare attività sospette, aiutando a rilevare minacce interne, infezioni malware<sup>6</sup> e accessi non autorizzati.
- *L'automazione e l'orchestrazione della sicurezza*: l'IA automatizza le attività di sicurezza di routine e semplifica i processi di risposta agli incidenti, migliorando l'efficienza complessiva della cybersecurity.

<sup>5</sup>L'espressione "Smart Home", o "casa intelligente", si riferisce alla capacità di gestire in modo automatico o remoto gli impianti e i dispositivi all'interno di un'abitazione. L'obiettivo è quello di risparmiare energia, semplificare la vita domestica e garantire la sicurezza delle persone che vi abitano.

<sup>6</sup>Per software intenzionalmente dannoso, o "malware", si intende qualsiasi programma progettato per danneggiare i sistemi di elaborazione o gli utenti

L'integrazione dell'IA nella cybersecurity offre, dunque, diversi vantaggi, tra cui una protezione avanzata contro attacchi informatici, un miglioramento del rilevamento delle minacce e una riduzione della dipendenza dall'intervento umano. Questi vantaggi contribuiscono a garantire una maggiore sicurezza e compattezza delle organizzazioni che gestiscono l'incolumità delle persone. Bisogna precisare che la presenza dell'IA non garantisce una soluzione definitiva delle problematiche legate alla cybersecurity. Infatti, sono numerose le minacce informatiche che nascono ogni giorno, le quali sfruttano sempre di più le capacità fornite dall'Intelligenza Artificiale.

### 1.4.2 Intelligenza Artificiale e Data Science

L'Intelligenza Artificiale e la Data Science sono due discipline strettamente connesse e insieme rivestono un ruolo sempre più importante nell'ambito aziendale. La Data Science trae le sue origini dall'analisi statistica e dalle moderne tecniche di data mining<sup>7</sup>, con il fine di sviluppare strategie per analizzare grandi quantità di dati e ottenere nuove informazioni. L'obiettivo dell'analisi dei Big data<sup>8</sup>, utilizzando l'IA, è automatizzare il processo e renderlo più veloce, accurato e scalabile, consentendo alle organizzazioni di sfruttare appieno il potenziale dei loro dati e di ottenere un vantaggio competitivo analizzando i dati relativi ai propri clienti e al mercato. Questi due settori sono complementari: i data scientist utilizzano spesso l'IA per ottimizzare l'analisi dei dati, automatizzando e velocizzando i corrispettivi processi, consentendo ai ricercatori di ottenere informazioni in modo più rapido ed efficiente. Invece, l'Intelligenza Artificiale trae vantaggio dall'analisi dei dati per migliorare nel tempo le proprie prestazioni, consentendo in futuro di implementare algoritmi di Machine Learning e Deep Learning sempre più efficienti.

### 1.4.3 Robotica e automazione

La robotica è il ramo dell'ingegneria che si occupa della progettazione, della costruzione, del funzionamento e dell'applicazione dei robot. Questi sono macchine programmabili in grado di eseguire compiti autonomi o semi-autonomi. Possono essere semplici, come un braccio meccanico che ripete un movimento preimpostato, oppure complessi, come un robot umanoide in grado di interagire con l'ambiente e prendere decisioni da solo. In particolare, i robot artificialmente intelligenti utilizzano gli algoritmi di IA, per integrare capacità avanzate con lo scopo di svolgere compiti complessi. Ad esempio, un robot può utilizzare un algoritmo di ricerca per rilevare il percorso e navigare autonomamente all'interno di un magazzino, oppure per individuare gli oggetti che raccoglie e posizzarli in luoghi diversi in base alla loro tipologia.

I campi di applicazione dei robot artificialmente intelligenti sono molteplici:

- *Smart Home*: l'uso di IA integrata alla robotica consente l'automazione di compiti domestici, il monitoraggio della sicurezza e l'ottimizzazione del consumo energetico.
- *Industria 4.0*: i robot intelligenti permettono l'automazione avanzata, la gestione delle risorse e la manutenzione predittiva, automatizzando, così, la produzione, migliorando l'efficienza e riducendo i tempi di fermo.

---

<sup>7</sup>Il data mining, o estrazione di dati, rappresenta l'insieme di tecniche e metodologie finalizzate all'estrazione di informazioni rilevanti da vaste quantità di dati. Questo processo avviene attraverso l'impiego di approcci automatici o semi-automatici e trova applicazioni in contesti scientifici, aziendali, industriali e operativi.

<sup>8</sup>Il termine inglese "Big data" (letteralmente "grandi quantità di dati") o, talvolta, la sua traduzione italiana "Megadati", si riferisce genericamente a una vasta raccolta di dati informatici caratterizzata da un'enorme mole, una velocità elevata e una grande varietà di tipologie.

- *Contesto aereo spaziale*: i robot assistono gli astronauti nelle loro attività quotidiane, riducendo lo stress da lavoro e migliorando la produttività.
- *Logistica*: le aziende utilizzano sistemi di mappatura, sensori e IA per fornire soluzioni innovative per la distribuzione di prodotti, velocizzando la spedizione e la consegna.
- *Agricoltura*: i sistemi intelligenti consentono di automatizzare task come la semina, la raccolta e la gestione delle colture, migliorando la precisione e riducendo il lavoro manuale. Ciò porta a una maggiore resa delle colture e a una minore dipendenza dai pesticidi.

I robot, grazie all'ausilio dell'IA, saranno, in futuro, in grado di operare con maggiore autonomia, richiedendo un minor intervento umano. Ciò sarà favorito dai progressi nella sensoristica nella navigazione e nella mappatura, consentendo un orientamento e un movimento più preciso e indipendente. Comunque, allo stesso tempo, la collaborazione uomo-robot diventerà sempre più diffusa, con robot che diventeranno assistenti e collaboratori, potenziando le capacità umane in svariati contesti.

#### 1.4.4 IA e medicina

L'avvento dell'Intelligenza Artificiale nel settore medico ha rivoluzionato la diagnostica, consentendo la rilevazione precoce di patologie attraverso l'analisi di dati strutturati e non strutturati, come immagini diagnostiche e segnali biologici. L'IA ha dimostrato efficacia soprattutto nell'oncologia e nella cardiologia, migliorando la precisione e la tempestività delle diagnosi.

Inoltre, l'IA è utilizzata per la predizione delle patologie, consentendo interventi preventivi più efficaci. Essa fornisce supporto ai medici nel suggerire opzioni terapeutiche ottimali, basate su evidenze scientifiche, e nella selezione delle molecole più promettenti per la sperimentazione clinica, accelerando il processo di sviluppo farmaceutico. Tuttavia, l'adozione dell'IA in medicina presenta delle sfide, come la necessità di prove scientifiche solide per garantirne l'affidabilità e la gestione dei bias nei dati di addestramento. Risulta fondamentale condurre studi clinici robusti e regolamentare l'uso dell'IA, per garantire la sicurezza e l'efficacia dei sistemi utilizzati.

Comunque l'IA in medicina presenta due principali filoni: virtuale e fisico. Il ramo virtuale include approcci informatizzati, che vanno dal Deep Learning alla gestione delle informazioni, fino al controllo dei sistemi di gestione della salute, compresi i record elettronici della salute e l'orientamento attivo dei medici nelle decisioni terapeutiche. Il ramo fisico è rappresentato principalmente dall'uso di robot e dispositivi medici nella presentazione delle cure.

Alcuni dei benefici chiave dell'IA nella medicina, dunque, racchiudono:

- *Diagnosi più precise*: l'IA può analizzare grandi quantità di dati medici più velocemente degli esseri umani, identificando modelli e anomalie che potrebbero sfuggire all'occhio umano e portando a diagnosi più accurate e precoci, con conseguenti migliori risultati per i pazienti.
- *Trattamenti personalizzati*: l'IA può essere utilizzata per creare piani di trattamento personalizzati per ciascun paziente, basandosi sulla sua storia clinica, sul profilo genetico e su altri fattori.
- *Sviluppo di nuovi farmaci*: l'IA può accelerare l'analisi di grandi quantità di dati per identificare potenziali bersagli terapeutici e sviluppare nuovi farmaci e terapie.

- *Riduzione dei costi sanitari*: l'IA può aiutare a ridurre i costi sanitari, automatizzando compiti amministrativi, migliorando l'efficienza delle operazioni e riducendo gli errori medici.
- *Miglioramento dell'assistenza ai pazienti*: i chatbot basati sull'IA possono rispondere alle domande dei pazienti, fornire informazioni sulle loro condizioni e aiutarli a prenotare appuntamenti.
- *Supporto del monitoraggio remoto dei pazienti*: l'IA può essere utilizzata per monitorare i parametri vitali dei pazienti a distanza, aiutando a identificare potenziali problemi di salute in anticipo.
- *Supporto alla robotica chirurgica*: i robot chirurgici sono utilizzati come assistenti nei trattamenti chirurgici, per fornire compagnia agli anziani e per la riabilitazione fisica. Si stanno sviluppando, inoltre, nuove metodologie per il monitoraggio e la somministrazione mirata di farmaci attraverso nanorobot che possono viaggiare verso zone poco ossigenate del corpo per il trattamento di tumori e altre patologie.

In conclusione, l'IA ha il potenziale per trasformare radicalmente l'assistenza sanitaria, migliorando la diagnosi, il trattamento e la gestione delle malattie. Tuttavia, sono necessarie ulteriori ricerche e valutazioni per garantire la sicurezza, l'efficacia e l'efficienza di queste tecnologie. È, dunque, di vitale importanza che queste nuove metodologie siano sempre affiancate dal personale medico, il quale può valutare, e in caso confutare, il risultato fornito dall'IA.

---

## Introduzione ad Amazon Web Services

---

*In questo capitolo verrà introdotto Amazon Web Services (AWS), la piattaforma basata su Cloud fornita da Amazon. Dopo una breve introduzione storica, si analizzerà la sua influenza a livello globale, evidenziando i cambiamenti che ha apportato sul mercato aziendale. In particolare, si parlerà dell'architettura su cui si basa AWS, fornendo una spiegazione sul funzionamento del Cloud Computing. Infine, si approfondirà come la piattaforma si sia fatta strada nel campo dell'Intelligenza Artificiale, concentrandosi sui servizi che propone ai propri utenti e su come abbia apportato una notevole influenza nello sviluppo dell'IA.*

### 2.1 Amazon Web Services

Per comprendere i risultati dei capitoli successivi, si propone una panoramica su *Amazon Web Services*, mostrando il motivo per cui si è affermato come uno dei principali fornitori di servizi di Cloud Computing per chiunque abbia l'intenzione di implementare un programma con funzionalità Web, simili a quelle offerte dalla piattaforma Amazon. La piattaforma è ampiamente utilizzata per eseguire applicazioni e memorizzare dati in modo flessibile, scalabile ed economico. Nelle prossime sezioni si analizzeranno la storia e l'evoluzione di AWS, esaminando i vari servizi offerti e i vantaggi che propone alle aziende.

#### 2.1.1 Introduzione alla piattaforma

Amazon Web Services (AWS) è una piattaforma di Cloud Computing offerta da Amazon, che mette a disposizione un vasto assortimento di servizi e strumenti per agevolare aziende e singoli individui nella creazione e nell'esecuzione delle proprie applicazioni e siti web. Fondata nel 2006, la sua architettura è strutturata in regioni, zone di disponibilità ed edge location<sup>1</sup>, consentendo una distribuzione globale delle risorse. Questo avviene seguendo un modello di pagamento basato sull'utilizzo effettivo delle risorse, noto come "pay-as-you-go". AWS è riconosciuta come una delle piattaforme più diffuse a livello globale, insieme a Microsoft Azure e Google Cloud Platform. Tra i suoi numerosi servizi, come si può notare nella Figura 2.1, spiccano quelli per l'elaborazione e lo storage, come Amazon EC2, Amazon RDS e Amazon S3, così come quelli dedicati all'Intelligenza Artificiale e all'analisi dei dati, come Amazon Rekognition e Amazon SageMaker.

---

<sup>1</sup>Le edge location sono punti posizionati strategicamente nella rete AWS, ottimizzati per la distribuzione di contenuti a bassa latenza, garantendo che i dati raggiungano rapidamente gli utenti.





Figura 2.1: Panoramica sui servizi offerti da AWS

### 2.1.2 Breve storia ed evoluzione di AWS

Le radici di AWS risalgono al 2002, quando Amazon avviò lo sviluppo della propria infrastruttura di Cloud Computing per sostenere il proprio sito web. Nel 2006, Amazon decise di rendere disponibile questa risorsa a terzi. Furono, dunque, fondati Amazon S3, come servizio di archiviazione Cloud, e Amazon EC2, che permetteva di affittare macchine virtuali su cui eseguire le applicazioni.

L'intento era di agevolare i programmatori nello sviluppo dei propri software, assumendosi la responsabilità di memorizzare i dati, assicurando un corretto salvataggio, nonché la protezione e la disponibilità del server in maniera continua. AWS ha avuto un successo immediato e, nel giro di pochi anni, è diventata la piattaforma di Cloud Computing più utilizzata al mondo. Questo successo è dovuto a una serie di fattori tra cui:

- Il *prezzo competitivo*: la piattaforma è resa accessibile a un'ampia gamma di clienti.
- La *sicurezza*: l'infrastruttura centrale di AWS, progettata specificamente per il Cloud, garantisce la sicurezza dei dati dei clienti attraverso il monitoraggio costante, la crittografia automatica e la retention<sup>2</sup>.
- La *disponibilità*: AWS garantisce la massima disponibilità di rete attraverso una struttura in regioni e zone di disponibilità isolate. Le applicazioni possono essere suddivise su più zone di disponibilità per aumentare la resilienza. Inoltre, i piani di controllo e le console di gestione di AWS sono distribuiti su più regioni, con endpoint API regionali, che assicurano la continuità operativa anche durante situazioni di isolamento.
- Le *prestazioni*: l'infrastruttura globale di AWS è ottimizzata per prestazioni elevate, offrendo bassa latenza e una rete di alta qualità tra le regioni. Le soluzioni come *AWS Local Zones*<sup>3</sup> e *AWS Wavelength*<sup>4</sup> garantiscono prestazioni ottimali per le applicazioni che richiedono bassissime latenze, portando l'infrastruttura AWS più vicino agli utenti

<sup>2</sup>La *data retention* stabilisce il tempo di conservazione dei dati di backup prima che questi vengano cancellati.

<sup>3</sup>Le *AWS Local Zones* sono un tipo di implementazione dell'infrastruttura che avvicina determinati servizi AWS agli utenti finali e ai carichi di lavoro.

<sup>4</sup>*AWS Wavelength* incorpora i servizi di calcolo e archiviazione di AWS all'interno delle reti 5G, offrendo un'infrastruttura di calcolo edge mobile per sviluppare, implementare e dimensionare applicazioni a bassissima latenza.

finali e ai dispositivi connessi in 5G. Con il Cloud è possibile aumentare rapidamente le risorse necessarie, implementando centinaia o migliaia di server in pochi minuti.

- La *scalabilità*: grazie all'infrastruttura globale di AWS, le aziende possono adattarsi rapidamente alle mutevoli esigenze aziendali, riducendo i costi e migliorando la capacità di risposta agli utenti. La scalabilità del Cloud consente loro di effettuare l'approvvigionamento delle risorse necessarie in modo efficiente e di distribuire rapidamente nuovi server quando richiesto.
- La *flessibilità*: l'infrastruttura globale di AWS offre alle aziende la flessibilità di gestire i carichi di lavoro in base alle loro esigenze. Le aziende possono selezionare quando e dove eseguire i servizi, utilizzando la rete, il piano di controllo, le API e i servizi AWS in base alle specifiche necessità.
- La *presenza globale*: AWS possiede un'infrastruttura globale in continua espansione, offrendo alle aziende la flessibilità di selezionare l'infrastruttura tecnologica più adatta alle esigenze degli utenti finali. La rete globale di AWS fornisce un supporto ottimale per una vasta gamma di applicazioni, anche quelle con elevati requisiti di portata e bassa latenza. Inoltre, per i dati situati in zone remote, *AWS Ground Station* offre antenne satellitari posizionate strategicamente nelle regioni dell'infrastruttura di AWS, garantendo una connettività affidabile e veloce.

AWS, come precedentemente affermato, si estende su scala globale attraverso la sua infrastruttura, che comprende numerose regioni e zone di disponibilità. Ogni regione è costituita da almeno tre zone di disponibilità isolate e fisicamente distinte all'interno di un'area geografica specifica. AWS offre i propri servizi in 33 regioni, 105 zone di disponibilità e 245 paesi e territori, come evidenziato nella Figura 2.2. A breve, Amazon prevede di lanciare altri data center a Hyderabad (India), Giacarta (Indonesia), Osaka (Giappone), Madrid (Spagna) e Zurigo (Svizzera). Ciascuna zona di disponibilità è dotata di proprie risorse di alimentazione, di raffreddamento e di sicurezza fisica. Alcune di queste offrono la copertura AWS Wavelength; ciò consente al traffico delle applicazioni, proveniente dai dispositivi 5G, di accedere direttamente ai server delle applicazioni eseguite nelle zone Wavelength, senza dover attraversare la rete pubblica di Internet. Tale approccio permette ai clienti di sfruttare appieno i vantaggi in termini di latenza e larghezza di banda offerti dalle moderne reti 5G.

### 2.1.3 Principali servizi offerti

AWS fornisce molteplici servizi ai propri clienti. Tra quelli più importanti presenti nella piattaforma, si menzionano:

- *Amazon Simple Service Storage* (o *Amazon S3*): permette agli utenti di archiviare i dati attraverso un metodo "object storage", in cui ogni unità è vista come un oggetto. Successivamente gli oggetti vengono organizzati logicamente in dei "bucket". Tutto questo viene eseguito mediante un'interfaccia web e delle API REST, ovvero delle librerie per caricare ed eliminare i dati dai vari bucket.
- *Amazon Elastic Compute Cloud* (o *Amazon EC2*): utilizza le *Amazon Machine Image (AMI)* per configurare delle macchine virtuali, utilizzate dagli utenti per eseguire i propri programmi. I clienti hanno il pieno controllo delle modalità di esecuzione, delle tempistiche e della posizione geografica su cui viene costruita la macchina virtuale, così da ridurre i tempi di latenza.



**Figura 2.2:** Zone di disponibilità del servizio

- *Amazon Relational Database Service* (o *Amazon RDS*): consiste in un servizio di database relazionale, accessibile attraverso un'API e un'interfaccia web. L'utente potrà scegliere quale DBMS usare, come Amazon Aurora, PostgreSQL, MySQL, Oracle DB e Microsoft SQL Server.
- *Virtual Private Cloud* (o *VPC*): consente di creare una sezione isolata all'interno del Cloud AWS, offrendo il controllo completo sull'ambiente di rete virtuale, inclusi indirizzi IP, sottoreti e gateway di rete. Questo assicura la sicurezza e la gestione personalizzata dei dati archiviati.
- *Amazon Route 53*: è un servizio *DNS* (*Domain Name System*) che gestisce il traffico verso applicazioni o siti web in base alla latenza o alla geo-localizzazione, fornendo, inoltre, servizi di registrazione dei domini.
- *AWS CodeStar*: semplifica il processo di sviluppo, creazione e distribuzione di applicazioni su AWS, mettendo a disposizione ambienti di sviluppo preconfigurati per svariati linguaggi di programmazione e framework, tra cui Java, .NET, Node.js, Python e Ruby.
- *AWS CodeBuild*: integra agevolmente il codice sorgente con repository esterni e offre un'infrastruttura di compilazione scalabile e affidabile per eseguire compilazioni e test su larga scala.

#### 2.1.4 Il ruolo di AWS nella collaborazione industriale

Le organizzazioni di varie dimensioni e settori sfruttano il potenziale fornito dai servizi di Cloud Computing di AWS per una vasta gamma di applicazioni. Queste includono il backup e il ripristino dei dati, l'utilizzo di servizi email, la creazione di desktop virtuali, il testing e lo sviluppo di software, l'analisi dei Big Data e la creazione di applicazioni web.

Ad esempio, nel settore sanitario, il Cloud viene impiegato per personalizzare i trattamenti per i pazienti, mentre le istituzioni finanziarie lo utilizzano come base per sistemi di rilevamento e prevenzione delle frodi. Anche i produttori di videogiochi traggono vantaggio dal Cloud per creare giochi online che coinvolgono giocatori di tutto il mondo.

Tra le imprese, che impiegano questa piattaforma, si ricordano:

- *Netflix*: il fornitore di servizi streaming utilizza i prodotti di AWS dal 2017 per svolgere molte delle sue operazioni, dalla transcodifica dei video al salvataggio dei dati nei database. L'azienda si affida ad AWS mediante i *Kinesis Data Streams*, o *KDS*, un servizio di streaming dei dati serverless che facilita la cattura, l'elaborazione e l'archiviazione dei flussi di dati su qualsiasi scala.
- *Pfizer*: l'azienda sanitaria sfrutta la tecnologia Cloud per ottimizzare lo sviluppo di farmaci, in particolare nella produzione, nelle sperimentazioni cliniche e nella distribuzione del prodotto. Il suo obiettivo futuro è quello di integrare i servizi di Intelligenza Artificiale, l'analisi e l'archiviazione Cloud nei propri laboratori; questo consentirà una produzione più veloce ed efficace.
- *NASA*: l'agenzia governativa ha sviluppato la sua nuova "Image and Video Library" con il supporto dell'Ufficio dei Servizi Web e di InfoZen, ora ManTech International, utilizzando AWS come piattaforma principale. Lanciata nel marzo del 2017, la libreria offre un'interfaccia utente intuitiva e funzionale, consentendo agli utenti di accedere, cercare e scaricare facilmente immagini e video. La sua architettura Cloud-nativa sfrutta una serie di servizi AWS, tra cui Amazon EC2, Amazon S3 e Amazon DynamoDB, un servizio di database basato sul paradigma NoSQL, garantendo scalabilità, affidabilità e prestazioni ottimali.
- *Lenovo*: la multinazionale si è rivolta a *DataRobot*, un partner tecnologico avanzato della Rete di Partner AWS (APN). DataRobot offre una piattaforma di Machine Learning automatico per scienziati dei dati di tutti i livelli di competenza, per costruire e implementare rapidamente modelli di Machine Learning accurati. Utilizzando DataRobot Cloud su AWS, gli utenti in tutta l'organizzazione possono costruire modelli di previsione di classe mondiale in pochi minuti.

Anche molte imprese italiane hanno integrato i servizi di AWS nella propria produzione. Tra queste si annoverano, per esempio, Dallara, azienda leader nella produzione di auto da corsa, che nel 2021 decise di utilizzare AWS per avere una maggiore potenza di calcolo ad alte prestazioni (HPC). In questo modo, essa ha soddisfatto tutti i suoi requisiti sia a livello di prestazioni che di costi, sfruttando la scalabilità e la flessibilità del servizio. Anche la Scuderia Ferrari, per sviluppare un sensore virtuale di velocità del suolo esterno alla vettura, ha utilizzato Amazon SageMaker, uno dei servizi di AWS.

## 2.2 Analisi dell'Infrastruttura Cloud di AWS

Il mondo dell'IT è sempre più orientato all'utilizzo dei servizi Cloud, che, con la loro flessibilità e scalabilità, hanno avuto modo di rivoluzionare il lavoro e la gestione di numerose aziende e settori. AWS è il provider più affidabile di Cloud Computing, che non solo offre un'eccellente sicurezza, ma fornisce anche ottimi servizi di archiviazione.

In questa sezione si propone un breve accenno alla disciplina del Cloud Computing, concentrandosi sui principali modelli che AWS fornisce ai propri clienti.

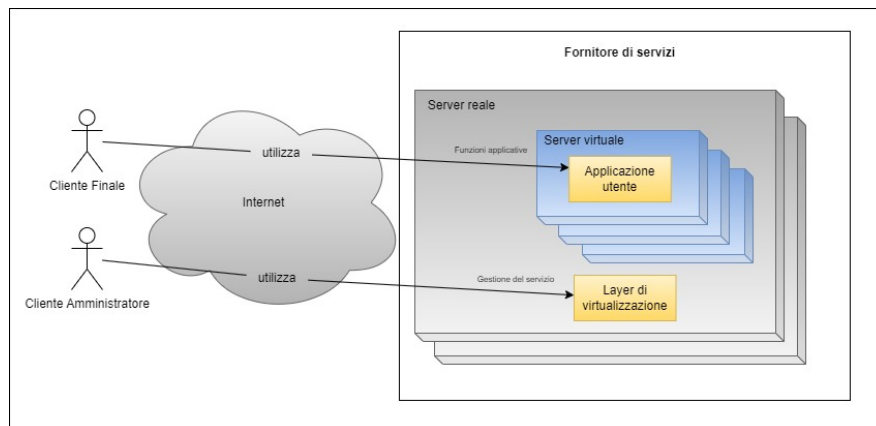
### 2.2.1 Cloud Computing

Il concetto di *Cloud Computing*, letteralmente tradotto come "computazione nella nuvola", si riferisce alla tecnologia che consente di elaborare, archiviare e trasmettere dati attraverso una rete. In sostanza, il Cloud Computing permette l'accesso a software e dati memorizzati su server remoti tramite Internet, anziché su dispositivi locali. Per le aziende di grandi

dimensioni, questo rappresenta una significativa riduzione dei costi; non sono più necessari hardware potenti soggetti a frequenti manutenzioni, ma è sufficiente una macchina in grado di eseguire l'applicativo per accedere al Cloud. Un computer per gestire ed elaborare i dati necessita di diverse componenti hardware, come CPU, memorie di massa, dischi rigidi interni o esterni e altri elementi costitutivi. Nei contesti in cui i computer sono connessi tramite reti locali (LAN) o geografiche (WAN), è possibile estendere le funzionalità di elaborazione, archiviazione e recupero di dispositivi remoti situati sulla stessa rete. Attraverso l'impiego della tecnologia del Cloud Computing, gli utenti collegati al fornitore possono svolgere tali operazioni, anche utilizzando un semplice browser Internet. Ad esempio, possono accedere a software remoti, senza doverli installare direttamente sul proprio computer, e salvare dati su memorie di massa online, concesse dallo stesso fornitore, utilizzando sia connessioni cablate che wireless.

L'architettura del Cloud Computing è costituita da server fisici o raggruppamenti di server ad alta affidabilità, solitamente situati nei data center del fornitore di servizi. Quest'ultimo espone le interfacce attraverso le quali i clienti amministratori possono elencare e gestire i servizi disponibili, selezionando le risorse necessarie come i server virtuali per eseguire e configurare le proprie applicazioni. Una volta configurata dall'amministratore, il cliente finale utilizza la risorsa come un "servizio", senza dover considerare gli aspetti fisici dell'implementazione, come il server reale o la posizione del data center. Tra i vari componenti fondamentali di un ambiente Cloud, vi è il concetto di "bucket", uno spazio dedicato all'archiviazione dei dati, funzionante come un contenitore virtuale.

Nella Figura 2.3 si schematizza la struttura dell'Infrastruttura Cloud; si possono notare il fornitore della piattaforma di server virtuali, il cliente amministratore, che sceglie e configura il servizio, e il cliente finale, che utilizza il prodotto appena configurato.



**Figura 2.3:** Architettura del Cloud Computing

## 2.2.2 Principali tipologie di Cloud Computing proposte da AWS

I servizi Cloud offerti da AWS si suddividono in tre principali categorie: *IaaS (Infrastructure as a Service)*, *PaaS (Platform as a Service)* e *SaaS (Software as a Service)*, i quali vengono erogati attraverso Internet. Inoltre, il cliente ha accesso a un'interfaccia software via browser, senza la necessità di eseguire alcun download. Per quanto riguarda IaaS, la piattaforma si occupa di gestire tutti gli aspetti hardware, inclusi la connettività di rete, i dischi rigidi, la virtualizzazione e l'archiviazione dei dati. Attraverso un'API il cliente può gestire da remoto il sistema operativo, le applicazioni e il middleware.

Nel contesto di una soluzione PaaS, il fornitore di servizi Cloud esterno fornisce e gestisce sia l'hardware che la piattaforma di software applicativo. Questa infrastruttura di base

include molte delle componenti IaaS, come server, archiviazione dati, sistemi operativi dei database e connessioni di rete. Inoltre, vengono fornite strutture per lo sviluppo e la distribuzione del software, come compilatori, middleware, librerie di programmi e servizi di runtime per linguaggi come Java e .NET. Progettato principalmente per sviluppatori e programmatori, il servizio PaaS offre una piattaforma Cloud condivisa per lo sviluppo e la gestione delle applicazioni, riducendo al minimo la necessità di gestire l’infrastruttura sottostante. Questo approccio consente agli utenti di concentrarsi sullo sviluppo e sulla gestione delle applicazioni, senza la complessità aggiuntiva associata al controllo dell’infrastruttura. Per quanto concerne le SaaS, i clienti hanno accesso a un’applicazione software, disponibile via web su dispositivi mobili. Eseguendo l’accesso attraverso un’API, gli utenti sono responsabili degli aggiornamenti software, della risoluzione dei bug e di altre attività di manutenzione. Inoltre, i file dell’utente vengono archiviati nel Data Center Cloud, garantendo una disponibilità universale e non più locale; ciò consente una maggiore sincronizzazione dei dati. Per quanto riguarda le modalità di distribuzione, il panorama del Cloud Computing è caratterizzato da:

- *Public Cloud*, accessibile a un vasto numero di clienti, offre una soluzione dinamica ed economica (un esempio è Microsoft Azure).
- *Private Cloud*, riservato ai singoli clienti, garantisce un maggiore controllo e una maggiore sicurezza dei dati, seppur a costo più elevato (un esempio è Eucalyptus System).
- *Community Cloud*, progettato per gruppi di consumatori con interessi condivisi, come nel settore dell’istruzione o in quello bancario, può essere gestito da una o più aziende all’interno della comunità (un esempio è Facebook).

In particolare Amazon Web Services è un esempio di *Hybrid Cloud*, che fonde diverse modalità di distribuzione, consentendo la scalabilità e l’utilizzo di risorse esterne, ma richiedendo una complessa pianificazione e gestione.

## 2.3 L’Impatto di Amazon Web Services sull’Intelligenza Artificiale

Amazon Web Services si è inserito come uno dei fornitori principali di Intelligenza Artificiale, garantendo un servizio di qualità ai diversi clienti interessati a lavorare con Machine Learning e Deep Learning. I principali prodotti che AWS ha messo sul mercato sono:

- *Amazon Polly*: trasforma il testo in una conversazione reale, consentendo di creare applicazioni e di sviluppare categorie completamente nuove di prodotti con funzionalità vocali.
- *Amazon Transcribe*: utilizza un processo di Deep Learning, denominato riconoscimento vocale automatico (*Automatic Sound Recognition - ASR*), per convertire la voce in testo in modo rapido e preciso.
- *Amazon SageMaker*: consente ai data scientist e agli sviluppatori di creare, addestrare e implementare con rapidità modelli di Machine Learning.
- *Amazon Textract*: estrae automaticamente testo, scrittura a mano e dati da documenti scansionati.
- *Amazon Kendra*: consente agli utenti di eseguire ricerche in diversi repository di contenuti con connettori integrati.

- *Amazon Personalize*: permette agli sviluppatori di creare applicazioni con la stessa tecnologia di Machine Learning utilizzata da Amazon per suggerimenti su misura in tempo reale.
- *Amazon Rekognition*: identifica oggetti, persone, testo, scenari e attività in immagini e video, compresi i contenuti inappropriati.
- *Amazon Lex*: incorpora interfacce di comunicazione con voce e testo per la creazione di chatbot.
- *Amazon Comprehend*: utilizza il Machine Learning per identificare informazioni e relazioni in un testo.
- *Amazon Translate*: fornisce traduzioni rapide e di alta qualità.

Oltre a questi servizi, si distinguono anche dei *tool* più specifici, come per esempio *Amazon Comprehend Medical*, in grado di estrarre informazioni dai reperti sanitari.

### 2.3.1 Reti neurali impiegate da AWS

Sono diverse le reti neurali utilizzate da Amazon Web Services, sia nell’ambito del Machine Learning che in quello del Deep Learning. Molti servizi di AWS, come Amazon Polly e Amazon Comprehend, utilizzano le *Recurrent Neural Network (RNN)*, già brevemente accennate nella Sezione 1.3.3. Queste ultime rappresentano un modello di Deep Learning realizzato per elaborare e convertire un input sequenziale in un determinato output, sfruttando la correlazione sintattica e semantica che c’è tra i dati. Una RNN è una tipologia di implementazione che imita il modo in cui gli esseri umani eseguono conversioni sequenziali di dati. Tuttavia, le RNN presentano anche un flusso di lavoro ciclico: il livello nascosto può conservare informazioni dagli input precedenti e utilizzarle per le previsioni future, sfruttando una memoria a breve termine. Per esempio, consideriamo la frase "La mela è rossa". Se vogliamo che una RNN predica la parola "rossa", dopo aver ricevuto la sequenza di input "La mela è", il livello nascosto memorizzerà una rappresentazione di "La mela" nella sua memoria. Quando riceve la parola "è", la RNN richiama dalla memoria la sequenza "La mela", per comprendere il contesto completo e predire con maggiore precisione la parola successiva. Questa caratteristica rende le RNN utili in applicazioni come il riconoscimento vocale e la traduzione automatica. Infatti, sono utilizzate in molti servizi di AWS, come Amazon Sagemaker, Amazon Polly e Amazon Transcribe.

Per eseguire in modo più efficiente l’elaborazione sequenziale dei dati, vengono utilizzate reti neurali più performanti e specializzate, come i *Transformer* e i *Large Language Model (LLM)*. I primi sono una tipologia di architettura neurale ideata per trasformare una sequenza di input in una sequenza di output. Questo avviene mediante l’apprendimento del contesto e l’analisi delle relazioni tra gli elementi della sequenza. Per esempio, si prenda in considerazione la frase "Qual è il colore del cielo?". Il Transformer utilizza una rappresentazione interna per comprendere la relazione tra le parole "colore", "cielo" e "blu" e generare l’output "Il cielo è blu". I Transformer hanno rivoluzionato l’elaborazione sequenziale attraverso una parallelizzazione completa. Grazie a questa caratteristica, gli addestramenti sono notevolmente più veloci e i modelli sono in grado di gestire sequenze di lunghezza molto superiore rispetto alle RNN, acquisendo conoscenze linguistiche, grammaticali e concettuali, senza la necessità di istruzioni esplicite.

Gli LLM, invece, sono modelli di Deep Learning preaddestrati su grandi quantità di dati. Essi si basano sui Transformer e quindi sono in grado di ricevere training senza supervisione, ovvero possono imparare da soli senza che siano date delle istruzioni specifiche. Gli LLM

sono reti neurali molto grandi e sono in grado di valutare miliardi di parametri. Le aziende li impiegano per una vasta gamma di applicazioni, che vanno dal riconoscimento vocale alla traduzione automatica, perciò sono utilizzati in servizi come Amazon Translate.

Nell’ambito dell’elaborazione delle immagini, e quindi di applicazioni come Amazon Rekognition, vengono utilizzate principalmente le *Convolutional Neural Network (CNN)*, già brevemente definite nella Sezione 1.3.3. Esse vengono impiegate principalmente nel riconoscimento di immagini, nella classificazione e nel rilevamento di oggetti, e altro ancora. A differenza delle reti neurali tradizionali, le quali richiedono la sintetizzazione dei dati in vettori unidimensionali prima di essere processati, le CNN possono mantenere la struttura delle immagini, catturando così relazioni spaziali locali tra i pixel.

Le CNN sono composte da vari tipi di *layer*, tra cui:

- I *Convolutional layer*: questi applicano filtri convoluzionali<sup>5</sup> alle immagini di input per estrarre caratteristiche come bordi, texture e pattern.
- I *Pooling layer*: questi riducono la dimensione spaziale dell’output dei Convolutional layer, riducendo, così, il numero di parametri e rendendo la rete più efficiente.
- I *Fully-connected layer*: questi combinano le proprietà estratte dalle Convolutional layer per produrre output finali, spesso utilizzati per la classificazione.

Ciascun layer applica un filtro specifico per estrarre caratteristiche particolari dall’immagine. Tipicamente, i layer iniziali estraggono caratteristiche di basso livello, mentre quelli più profondi identificano caratteristiche di livello superiore.

Tra le reti neurali utilizzate, vanno menzionate anche le *Long short-Term Memory (LSTM)* e le *Gated Recurrent Unit (GRU)*, le quali rappresentano un’architettura più avanzata delle RNN.

Le LSTM sono state introdotte da Sepp Hochreiter e Juergen Schmidhuber nel 1997 al fine di mitigare il problema delle dipendenze a lungo termine all’interno delle RNN. Quando lo stato precedente dell’analisi, che condiziona la previsione attuale, non è stato osservato nel passato recente, le tradizionali RNN possono mostrare difficoltà, se non impossibilità, nel formulare previsioni accurate per lo stato attuale. Per mitigare tale inconveniente, le LSTM incorporano delle "celle" all’interno dei loro strati nascosti, dotate di tre "porte" (*input gate*, *output gate*, *forget gate*). Queste regolano il flusso delle informazioni essenziali per formulare previsioni all’interno della rete.

Invece, le *Gated Recurrent Unit (GRU)* rappresentano una variante delle RNN simile alle LSTM, sviluppata sempre con il fine di risolvere le problematiche legate alla memoria a breve termine. Diversamente dalle LSTM, le GRU adottano uno schema di gestione delle informazioni basato su stati nascosti, anziché su uno stato di cella. Inoltre, rispetto alle LSTM, che presentano tre porte, le GRU ne impiegano due: una porta di reimpostazione (*reset gate*) e una porta di aggiornamento (*update gate*). Queste ultime, similmente a quelle delle LSTM, regolano l’importanza e la rilevanza delle informazioni conservate durante il processo di elaborazione.

<sup>5</sup>In matematica, date due funzioni  $f(x)$  e  $g(x)$ , si dice prodotto di convoluzione (o integrale di convoluzione), e si indica con  $f(x) * g(x)$ , l’integrale improprio:

$$\int_{-\infty}^{\infty} f(\tau) \cdot g(t - \tau) d\tau$$



### 2.3.2 Soluzioni per la modellazione e l’implementazione di algoritmi fornite da AWS

AWS permette ai data scientist e agli sviluppatori di implementare i propri algoritmi di Machine Learning e Deep Learning, fornendo soluzioni intuitive e scalabili.

Primo tra tutti va menzionato Amazon Sagemaker, già brevemente accennato nella Sezione 2.3, una piattaforma completa per la creazione, l’addestramento e la distribuzione di modelli di apprendimento automatico. In particolare, esso semplifica il processo di sviluppo e implementazione dei modelli di Machine Learning e Deep Learning.

Inoltre, AWS integra diversi framework per l’implementazione di algoritmi di Intelligenza Artificiale. Tra questi vanno menzionati:

- *TensorFlow*, un framework open-source che offre un’ampia gamma di strumenti per la costruzione e l’addestramento di modelli di Machine Learning e Deep Learning su molte piattaforme hardware.
- *Apache MXNet*, un framework di Deep Learning scalabile supportato da Apache. Esso è progettato per gestire carichi di lavoro di Machine Learning e Deep Learning su scala, offrendo prestazioni elevate e una vasta gamma di funzionalità per lo sviluppo di modelli avanzati.

### 2.3.3 Sviluppi futuri di AWS nel mondo dell’Intelligenza Artificiale

Amazon Web Services ha annunciato nel 2023 che avrebbe investito un ingente capitale in un nuovo programma che mettesse in contatto esperti di Intelligenza Artificiale e di Machine Learning di AWS con i clienti e partner aziendali di tutto il mondo, formando un team che ha preso il nome di *AWS Generative AI Innovation Center*, che si pone l’obiettivo di accelerare l’innovazione e l’implementazione di servizi basati sull’IA Generativa. In particolare, AWS ha concentrato i propri studi sullo sviluppo di servizi come *Amazon CodeWhisperer*<sup>6</sup>, *Amazon Bedrock*<sup>7</sup> e, soprattutto, *Amazon Q*. Quest’ultimo si basa sull’esperienza di diciassette anni di AWS nella lavorazione dei dati e offre un servizio altamente personalizzato per le aziende. Gli utenti, quali operatori di mercato, project manager, personale di vendita e altri, possono sfruttare le funzionalità di conversazione, risoluzione dei problemi, generazione di contenuti, azioni personalizzate e altro ancora. Grazie alla consapevolezza dei sistemi aziendali, Amazon Q è in grado di rispondere a domande dettagliate e articolate, fornendo risultati su misura, che includono solo le informazioni autorizzate per l’utente.

Nel capitolo successivo, si approfondirà proprio il nuovo filone dell’Intelligenza Artificiale in grande di sviluppo negli ultimi anni, ovvero l’IA Generativa, la quale si propone di rivoluzionare il funzionamento, l’utilizzo e lo sviluppo delle applicazioni future.

---

<sup>6</sup>Amazon CodeWhisperer genera suggerimenti di codice che vanno da frammenti a funzioni complete in tempo reale nell’IDE, sulla base dei commenti e del codice esistente.

<sup>7</sup>Amazon Bedrock permette ai programmatori di creare chatbot di IA Generativa e altre applicazioni Cloud, impiegando i dati organizzativi interni per l’ideazione di modelli di LLM.

---

*In questo capitolo si fornirà un'introduzione all'Intelligenza Artificiale Generativa, esaminando la sua storia e il suo sviluppo nel tempo. Si analizzeranno le principali reti neurali che costituiscono la sua architettura e si esploreranno le applicazioni principali in vari settori. Inoltre, si discuteranno i limiti e le sfide legate a questa forma di Intelligenza Artificiale, concentrandosi, in particolare, sul concetto di Deepfake.*

### 3.1 Intelligenza Artificiale Generativa

Per lungo tempo, si è creduto che le attività creative e artistiche, come la poesia, il disegno, la composizione musicale, e anche lo sviluppo software, fossero intrinsecamente umane e al di là della portata dell'Intelligenza Artificiale. Tuttavia, i recenti sviluppi hanno rivoluzionato questa concezione, dimostrando che le macchine possono generare contenuti originali in modo sorprendentemente simile agli esseri umani.

Il concetto di *Intelligenza Artificiale Generativa* (in inglese *Generative AI*) si riferisce a tecniche computazionali in grado di creare nuovi contenuti e idee, tra cui conversazioni, storie, immagini, video e audio, basandosi sui dati di addestramento. Infatti, essa può generare nuovi dati a partire da quelli esistenti o modellare la loro distribuzione di probabilità<sup>1</sup>, applicando una serie di trasformazioni algebriche e geometriche, che includono traslazioni, rotazioni e riflessioni, nonché l'aggiunta di rumore gaussiano<sup>2</sup>.

Si consideri, per esempio, una rete neurale che genera immagini artificiali relative a una determinata classe semantica  $A$  e un vettore di rumore pseudo-casuale  $\xi$ ; l'IA Generativa consente di creare un'immagine  $B$  attribuibile alla classe  $A$ , modellando la distribuzione di probabilità  $P(A|B)$ , che rappresenta la distribuzione delle immagini riconducibili alla classe  $A$ . Durante questi processi, l'obiettivo è massimizzare la funzione di verosimiglianza<sup>3</sup>, ovvero far sì che venga generata una nuova funzione  $P'(A|B)$  il più simile possibile a  $P(A|B)$ .

---

<sup>1</sup>Una distribuzione di probabilità è un modello matematico che collega i valori di una variabile alle probabilità che tali valori possano essere osservati.

<sup>2</sup>Il rumore gaussiano è una tipologia di rumore casuale che segue una distribuzione normale, detta anche distribuzione gaussiana. Quest'ultima è caratterizzata da una forma a campana simmetrica, determinata dal valore assunto dalla media e dalla deviazione standard.

<sup>3</sup>In statistica, la funzione di verosimiglianza  $\mathcal{L}(\theta | x)$  rappresenta la probabilità di osservare i dati  $x$  assumendo che  $\theta$  sia il parametro effettivo.

### 3.1.1 Storia dell'IA Generativa

L'IA Generativa rappresenta un'evoluzione che affonda le sue radici nelle metodologie statistiche tradizionali. In passato, la statistica utilizzava tecniche sofisticate per effettuare l'analisi di dati complessi. Queste metodologie sono state acquisite per lo sviluppo delle reti neurali, e quindi del Deep Learning, permettendo l'identificazione di pattern complessi e di relazioni nascoste all'interno di grandi volumi di dati. L'IA Generativa rappresenta l'apice di questa evoluzione. Quest'ultima ha avuto origine nel 2013, quando vennero implementati per la prima volta i *Variational Autoencoder* (o, più semplicemente, *VAE*), i quali sono stati il primo modello di rete neurale generativa, in grado di produrre un nuovo insieme di dati a partire dal dataset di training. Tutto questo ha portato alla nascita di altri modelli di IA Generativa, tra cui le *Generative Adversarial Network* (*GAN*), implementate per la prima volta nel 2014, e i *Diffusion Model*. Queste nuove tecnologie hanno permesso la creazione di dati sempre più verosimili, nonostante fossero creati artificialmente.

Nel 2017, sono stati presentati i *Transformer*, già precedentemente citati nella Sezione 2.3.1. Questi ultimi hanno permesso di integrare la già presente architettura Decoder-Encoder<sup>4</sup> con un *meccanismo di autoattenzione*, che ha permesso al modello un'elaborazione più accurata della sequenza di dati. Questa innovazione ha permesso di ridurre notevolmente la complessità del processo di training dei modelli linguistici, garantendo dei livelli di efficienza senza precedenti. Tra i modelli più significativi si evidenzia *GPT*, che ha permesso di automatizzare e migliorare notevoli attività quali, ad esempio, la traduzione di testi e la creazione di immagini.

Recentemente si è vista la nascita di numerosi modelli generativi, tra cui si menzionano il *Vector Quantized Generative Adversarial Network* (*VQ-GAN*), perfezionamento delle *GAN*, e il *Vision Transformer*, che ha permesso di addestrare i *Transformer* nell'elaborazione di immagini. Nel 2020, sono state progettate i *Denosing Diffusion Probabilistic Model* (*DDPM*) e i *Denosing Diffusion Implicit Model* (*DDIM*), le quali rappresentano un'evoluzione dei *Diffusion Model* tradizionali. Successivamente, sono stati proposti ulteriori modelli generativi, tra cui *GPT-3*, *ChatGPT* e *DALL-E* (gli ultimi due proposti da OpenAI). Al giorno d'oggi, nel 2024, numerose aziende, come *Google*, *Microsoft* e *Adobe*, hanno dichiarato di voler integrare sempre di più i modelli di IA Generativa nei propri processi di lavorazione, per migliorare i propri servizi.

## 3.2 Architettura dell'IA Generativa

Il funzionamento dell'IA Generativa si basa sull'impiego dei modelli generativi, i quali, come già affermato precedentemente, fondano le proprie origini sulla statistica. Infatti, a partire da un insieme di dati in input, le reti cercano di formulare una nuova distribuzione di probabilità il più simile possibile a quella originale.

I modelli generativi possono essere classificati in base alla loro struttura, alla modalità di training e al fine per cui vengono impiegati. Di seguito verranno proposte le principali reti neurali generative.

### 3.2.1 Variational AutoEncoder

I *Variational AutoEncoder* (*VAE*) sono stati una delle prime tipologie di reti neurali ad essere impiegate nell'ambito dell'apprendimento non supervisionato e nell'implementazione di modelli generativi. L'architettura di un *VAE* si basa sull'utilizzo degli *AutoEncoders* (*AE*)

---

<sup>4</sup>L'architettura Decoder-Encoder viene utilizzata nel campo del *Natural Language Processing* (*NLP*) per processare sequenze di input (come frasi o parole) e generare sequenze di output (come, ad esempio, traduzioni o riassunti).

integrati con le tecniche di inferenza variabile bayesiana, le quali applicano il teorema di Bayes<sup>5</sup> per ottenere stime e previsioni tramite l'aggiornamento delle distribuzioni di probabilità a seguito dell'osservazione dei dati.

Gli AutoEncoders sono formati da due reti neurali: l'encoder, che codifica i dati passati in input in una rappresentazione di dimensione minore, e il decoder, il quale ricostruisce i dati decodificando le rappresentazioni e restituendo in output l'informazione che era stata passata in ingresso all'encoder. Inoltre, tra le due reti neurali è presente uno spazio latente, il quale contiene le rappresentazioni codificate. La finalità principale degli AutoEncoder è quella di acquisire una rappresentazione efficace dei dati in maniera non supervisionata, che risulta utile in diversi contesti, come ad esempio nel processo di *clustering*<sup>6</sup>.

Nel caso dei VAE la struttura, mostrata nella Figura 3.1, è del tutto analoga a quella degli AutoEncoder, tranne per il fatto che l'encoder genera due vettori, ovvero un vettore di medie e un vettore delle varianze. Successivamente, tramite il processo di *sampling*<sup>7</sup>, viene generato un vettore  $z$  che "mappa" lo spazio latente. In questo modo, il processo diventa stocastico, visto che la codifica del dato varierà secondo la varianza attorno alla sua media. Il decoder, invece, decodifica il risultato cercando di riprodurre una rappresentazione dei dati simile a quella originale.

In contrapposizione agli AutoEncoder, in cui lo spazio latente si configura in modo sparso, i Variational AutoEncoder si caratterizzano per la presenza di parametri ben delineati associati ad ogni input. Questa impostazione consente di ottenere una distribuzione normalizzata e una rappresentazione dello spazio latente continua e omogenea.

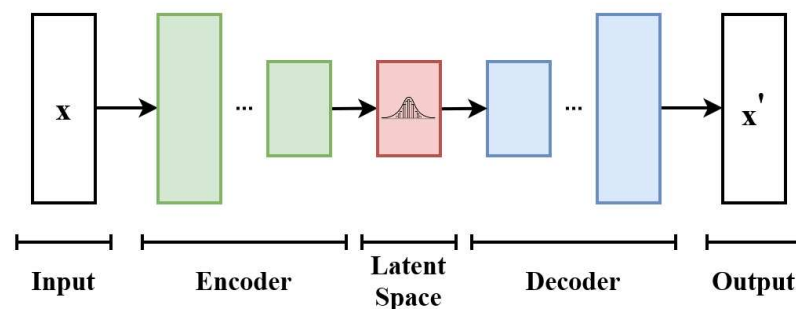


Figura 3.1: Struttura di un Variational AutoEncoder

### 3.2.2 Generative Adversarial Network

Le *Generative Adversarial Network* (GAN), già brevemente accennate nella Sezione 1.3.3, sono state proposte per la prima volta dall'informatico statunitense Ian Goodfellow e i suoi colleghi dell'Università di Montréal nel 2014, con l'obiettivo di creare un modello di Deep Learning in grado di generare nuovi dati a partire da un set di dati di addestramento. Il nome *Adversarial* deriva dal fatto che il loro funzionamento si basa sull'integrazione di due reti neurali "antagoniste": la rete generativa produce nuovi dati a partire da un determinato input, mentre l'altra (chiamata "discriminativa") cerca di prevedere se il nuovo risultato

<sup>5</sup>Il teorema di Bayes afferma che, dati due eventi  $A$  e  $B$  con probabilità non nulla, la probabilità condizionata sarà  $P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)}$ .

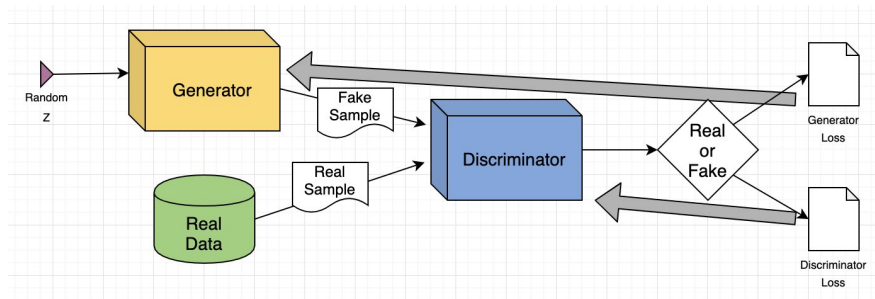
<sup>6</sup>Nel Machine Learning, il clustering racchiude un insieme di tecniche di analisi dei dati volte alla selezione e al raggruppamento di elementi omogenei in un insieme di dati.

<sup>7</sup>Il sampling è una tecnica di analisi statistica, impiegata per selezionare, manipolare ed analizzare un sottoinsieme rappresentativo di dati, al fine di identificare pattern e tendenze del dataset sotto esame.

possa appartenere al set di dati originale. Questo confronto continua fino a quando la rete di previsione non riesce più a distinguere i dati originali da quelli prodotti artificialmente.

L'architettura delle GAN deriva dalla struttura Decoder-Encoder delle VAE, come mostrato nella Figura 3.2. La rete neurale generativa, che funge da encoder, esegue un'analisi dettagliata del dataset di training al fine di discernere gli attributi dei dati. Allo stesso modo, la rete neurale discriminativa, o decoder, procede a un'indagine accurata del dataset iniziale, distinguendo gli attributi in modo indipendente. Successivamente, il generatore apporta modifiche agli attributi dei dati mediante l'introduzione di rumore o variazioni casuali su specifici parametri. Tali dati modificati sono sottoposti allo scrutinio del discriminatore, il quale valuta la verosimiglianza tra l'output generato e il set di dati originale. Il discriminatore, a sua volta, fornisce al generatore indicazioni mirate per raffinare la casualità del vettore di rumore nell'iterazione successiva. Nel corso delle fasi di addestramento, sia il generatore che il discriminatore si affinano reciprocamente, confrontandosi iterativamente fino a raggiungere un punto di equilibrio. In tale stato, il discriminatore perde la capacità di distinguere i dati sintetizzati da quelli originali, segnando la conclusione del processo di addestramento.

Ad esempio, si analizzi con precisione l'intero processo, prendendo in considerazione la produzione di immagini artificiali. La fase preliminare dell'addestramento si concentra sulla preparazione del dataset, dove i dati sono sottoposti a normalizzazione affinché i valori siano omogenei e scalati uniformemente, al fine di renderli idonei alle fasi successive. Le due reti, addestrate in un processo iterativo, si trovano in una competizione a somma zero, caratterizzata da obiettivi contrastanti. Il discriminatore assume il ruolo di un classificatore binario che analizza attentamente i pixel dell'immagine in ingresso, identifica pattern significativi, li confronta con schemi precedentemente appresi e attribuisce un'etichetta in base alla sua discriminazione, fornendo un valore compreso tra 0 e 1: 0 se l'immagine viene identificata come falsa, 1 se viene riconosciuta come autentica. Il generatore viene istruito mediante l'algoritmo di back-propagation utilizzando i feedback forniti dal discriminatore. L'iterazione continua tra l'addestramento del generatore e del discriminatore persiste fino a quando non si raggiunge l'equilibrio di Nash, in cui una delle reti mantiene invariata la propria azione indipendentemente dalle azioni della controparte. Al termine dell'addestramento, il modello viene valutato tramite dati di test, al fine di verificare la sua capacità di generare dati sintetici realisticamente attendibili. Va sottolineato che l'addestramento di una GAN può richiedere tempo e risorse computazionali, soprattutto se il dataset è esteso o complesso. Inoltre, durante il processo di addestramento, possono emergere sfide come il collasso del generatore, caratterizzato dalla produzione di una gamma limitata di campioni, o l'overfitting del discriminatore; tali problematiche richiedono una risoluzione adeguata.



**Figura 3.2:** Architettura di una Generative Adversarial Network

Esistono vari modelli di reti neurali GAN, che si distinguono per il modo in cui il generatore e il discriminatore interagiscono tra loro e le formule matematiche utilizzate. Tra queste si ricordano:

- *Vanilla GAN*: rappresenta il primo modello delle Generative Adversarial Network, le quali generano variazioni dei dati con un coinvolgimento della rete discriminativa limitato o nullo.
- *GAN condizionale (cGAN)*: presenta il concetto di condizionalità, permettendo una generazione mirata dei dati. In questo contesto, sia il generatore che il discriminatore ricevono informazioni supplementari sotto forma di etichette di classe o altri tipi di dati di condizionamento.
- *Deep Convolutional GAN (DCGAN)*: formalizzato nel 2015 da Alex Radford nel documento *Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks*, il concetto delle DCGAN implica l'utilizzo di due Convolutional Neural Network, le quali sono altamente efficienti nell'elaborazione di input come immagini, voce o audio.
- *GAN a Super Risoluzione (SRGAN)*: si concentrano sull'*upscaling*, una tecnologia che consente di aumentare la risoluzione delle immagini, migliorando, così, la qualità del dato di input originale.
- *Gan della piramide Laplaciana (LapGAN)*: generano immagini ad alta risoluzione procedendo per fasi progressive. Usano un approccio gerarchico con più reti generative e discriminative, le quali lavorano a più risoluzioni dell'immagine.

Esistono, comunque, altre reti neurali basate sulle GAN, come, ad esempio, le *StyleGAN*, le *CycleGAN* e le *Discogan*, che consentono di implementare diverse funzioni.

Le Generative Adversarial Network trovano diverse applicazioni in vari contesti. Ad esempio, possono essere impiegate per generare immagini realistiche partendo da istruzioni testuali o modificando immagini preesistenti. Questo processo è fondamentale per creare esperienze visive coinvolgenti e realistiche nei videogiochi e nell'intrattenimento digitale. Le GAN possono anche migliorare immagini, convertendo quelle a bassa risoluzione in alta risoluzione o quelle in bianco e nero in colorate, e generare volti, personaggi e animali realistici per animazioni e video.

In ambito di Machine Learning, le GAN possono essere utilizzate nella *data augmentation*, creando dati sintetici con attributi simili a quelli reali. Ad esempio, possono generare dati di transazioni fraudolente per addestrare sistemi di rilevamento delle frodi, migliorando la capacità del sistema di distinguere tra transazioni sospette e autentiche.

Inoltre, le GAN possono essere impiegate per stimare e completare informazioni mancanti nei dati. Ad esempio, possono essere addestrate per generare immagini della superficie sotterranea, utilizzando la correlazione tra dati di superficie e strutture sotterranee. Ciò è prezioso per applicazioni come la mappatura geotermica o la gestione del carbonio.

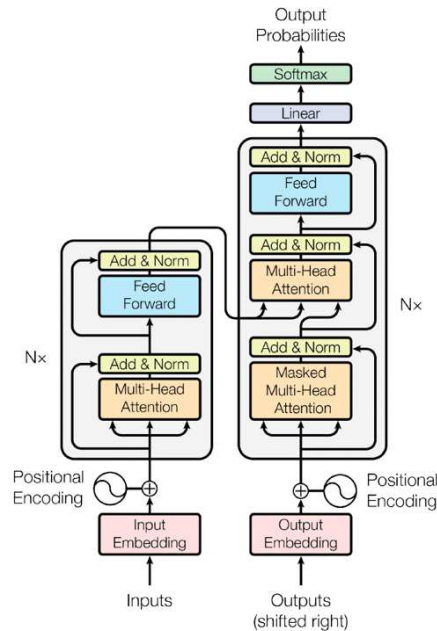
Infine, le GAN possono generare modelli tridimensionali partendo da immagini bidimensionali o scansioni. Ad esempio, nel settore sanitario, possono combinare radiografie e altre scansioni del corpo per creare modelli realistici degli organi, utili per la pianificazione e la simulazione chirurgica.

### 3.2.3 Transformer

I Transformer sono stati presentati per la prima volta dall'informatico Vaswani e altri ricercatori nel 2017. Mentre le reti neurali tradizionali sono basate su un modello di architettura Decoder-Encoder, in cui ogni dato viene elaborato in sequenza, rallentando notevolmente il processo e aumentando la possibilità di danneggiare la qualità del risultato, i Transformer

incorporano un *meccanismo di autoattenzione*. Infatti, quest'ultimo consente di esaminare contemporaneamente diverse parti della sequenza, permettendo di prestare maggiore attenzione alle informazioni più importanti.

L'architettura della rete neurale di un Transformer presenta diversi livelli software, come rappresentato nella Figura 3.3, i quali cooperano insieme per produrre il risultato finale.



**Figura 3.3:** Architettura di un Transformer

La fase di incorporamento dell'input è un passaggio fondamentale nell'elaborazione delle sequenze, poiché converte una serie di token in una rappresentazione matematica comprensibile agli algoritmi software. Questo processo prevede l'analisi e la suddivisione della sequenza di input in token, seguita dalla loro trasformazione in vettori matematici. Questi ultimi, che contengono informazioni sintattiche e semantiche, sono concepiti come coordinate in uno spazio vettoriale multidimensionale, in cui ciascuna dimensione riflette un attributo specifico del token.

Un elemento cruciale è la codifica posizionale, che attribuisce informazioni sulla disposizione dei token nella sequenza. Questo aspetto è di vitale importanza per preservare l'ordine dei token e coglierne appieno il contesto.

Nell'architettura dei Transformer, l'uso di blocchi di trasformatori sovrapposti è una pratica consolidata. Ogni blocco è caratterizzato da un meccanismo di autoattenzione a più teste, che consente al modello di valutare l'importanza relativa dei token all'interno della sequenza. Questo processo permette al modello di concentrare l'attenzione su parti salienti dell'input. Allo stesso modo, il livello *feed-forward* agevola il flusso delle informazioni e assicura la stabilità del modello durante il processo di addestramento.

Infine, i blocchi lineari e softmax rappresentano l'ultimo stadio di elaborazione delle informazioni, trasformando le rappresentazioni interne complesse in previsioni concrete. Il blocco lineare esegue una mappatura lineare degli output vettoriali sui token originali, mentre la funzione softmax normalizza tali punteggi in una distribuzione di probabilità, riflettendo la fiducia del modello nelle varie classi o token considerati.

Sono stati realizzati numerosi modelli di Transformer; tra questi si evidenziano:

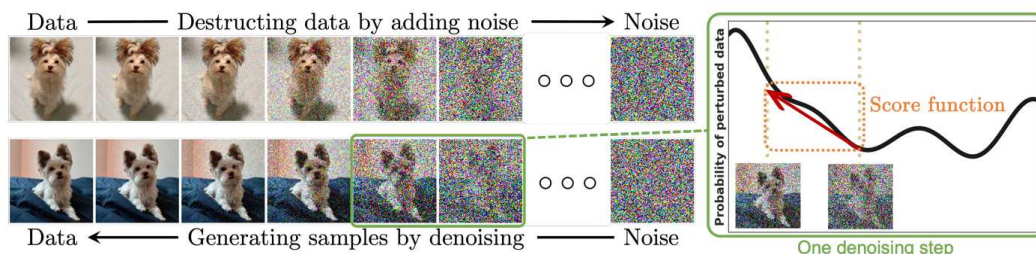
- *Bidirectional Encoder Representations from Transformers (BERT)*: utilizza un meccanismo noto come *Linguaggio Mascherato Bidirezionale (MLM)* per l'elaborazione delle parole,

permettendo di eseguire un'analisi contestuale, anziché trattarle separatamente. Durante il pre-addestramento, BERT maschera casualmente alcuni token di input per poi prevederli attraverso il contesto.

- *Generative Pre-trained Transformer (GPT)*: impiegano decoder pre-addestrati su ampie porzioni di testo; tali decoder, operando in modo autoregressivo, prevedono il valore successivo in una sequenza basandosi sui dati acquisiti. I GPT vengono utilizzati con grandi quantitativi di dati, visto che i loro parametri superano i 175 miliardi.
- *Bidirectional and AutoRegressive Transformer (BART)*: integra il potenziale del codificatore bidirezionale di BERT con il decodificatore autoregressivo di GPT per effettuare un'analisi contestuale e un'elaborazione sequenziale avanzata.
- *Transformer per Attività Multimodali*: utilizzano reti a doppio flusso, che consentono di analizzare separatamente gli input testuali e visivi, prima di integrarli in un unico risultato. Questo approccio permette di apprendere e interpretare rappresentazioni intermodali complesse. Un esempio sono *ViLBERT* e *VisualBERT*.
- *Transformer per l'Elaborazione Visiva (ViT)*: sono utilizzati per la classificazione di input visivi. In particolare, trattano le immagini come una sequenza di *patch* a dimensione fissa, così da poter trarre informazioni spaziali su di esse.

### 3.2.4 Diffusion model

I *Diffusion model* costituiscono una categoria di modelli generativi probabilistici che procedono progressivamente alla degradazione dei dati attraverso l'introduzione di rumore, al fine di acquisire la capacità di invertire tale processo per la generazione di campioni, come mostrato nella Figura 3.4.



**Figura 3.4:** Processo di elaborazione di un Diffusion model

I Diffusion model si basano su un modello probabilistico di diffusione per la rimozione del rumore che si avvale di due catene di Markov<sup>8</sup>, ovvero una *forward chain* e una *reverse chain*, attraverso le quali si attuano le principali fasi del processo che sono sostanzialmente due: il *fixed forward diffusion process*, che consiste nel ricevere in ingresso i dati (solitamente un'immagine) e aggiungere gradualmente rumore gaussiano, e il *generative reverse denoising process*, che trasforma il rumore in un campione della distribuzione iniziale. Dopo la fase di training, durante la quale l'immagine viene gradualmente convertita in un pattern di rumore gaussiano, il modello può essere utilizzato per generare dati sintetici. Questo processo avviene mediante l'uso di campioni casuali di rumore, successivamente elaborati attraverso il processo di *denoising*.

<sup>8</sup>La catena di Markov si riferisce a un modello probabilistico che descrive una successione di eventi possibili, in cui la probabilità di ogni evento dipende esclusivamente dallo stato raggiunto nell'evento precedente.



Comunque, oltre a questa modalità di procedere, la ricerca attuale ha prodotto altre due formulazioni principali: i *score-based generative model (SGM)*<sup>9</sup> e le *stochastic differential equation (SDE)*<sup>10</sup>.

Il tratto distintivo dei Diffusion model, rispetto ad altre forme di modelli generativi, è la loro maggiore stabilità e minore tendenza a problemi come il collasso del modello, nel quale si verificano produzioni limitate e ripetitive. Inoltre, tali modelli possono essere addestrati su dataset di bassa qualità e successivamente utilizzati per generare dati di alta qualità, come, ad esempio, la creazione di immagini ad alta risoluzione.

### 3.3 Applicazioni della IA Generativa nelle aziende

Anche se si sono già discussi precedentemente i vantaggi e le applicazioni dell'Intelligenza Artificiale nella Sezione 1.4, l'IA Generativa può conferire un ulteriore vantaggio competitivo a qualsiasi azienda che scelga di sfruttarla. Uno dei principali vantaggi risiede nella sua flessibilità, in quanto può essere applicata in numerosi campi. Infatti, molte aziende utilizzano l'IA Generativa per effettuare l'analisi dei dati e per la successiva identificazione dei trend che influenzano il mercato, permettendo di definire una strategia aziendale più mirata e vincente. Impiegando strumenti come ChatGPT e DALL-E, esse sono in grado di analizzare i *feedback* dei clienti da dati non strutturati, come, ad esempio, quelli provenienti dai *social-media*. Ciò consente alle aziende di migliorare la *customer experience*, offrendo ai clienti annunci e promozioni mirate ai propri desideri, permettendo di perfezionare la fidelizzazione con i clienti. Infatti, tutto questo potrebbe ridurre in modo significativo il tempo necessario per la progettazione di contenuti, permettendo di risparmiare energie e tempo. Potrebbe anche automatizzare il monitoraggio post-vendita e coltivare in modo passivo i potenziali clienti fino a quando non sono pronti per interagire direttamente con un agente di vendita umano. In servizi come *Spotify* e *Netflix*, l'IA ha un ruolo chiave nel suggerire i contenuti in base alle attività degli utenti. L'IA Generativa consente di ottimizzare in modo notevole l'impiego di risorse, rendendo più efficiente, ad esempio, la comunicazione interna tra i membri di un team e quella con i vari *stakeholder*, rendendo più semplice la traduzione di testi e la formulazione di messaggi ed email. Inoltre, essa consente di velocizzare numerosi task. Un esempio è dato dalla generazione automatica di codice in tempo breve, facilitando la fase di testing e di manutenzione dei sistemi, migliorando la qualità e le performance del software. Uno studio ha rivelato che i programmatori che utilizzano *GitHub Copilot* di *Microsoft* completano le loro attività con un aumento del 56% di velocità. Un ultimo, ma importante, vantaggio risiede nella diminuzione dei costi di logistica e di produzione.

Sono numerosi i settori che ricevono questi vantaggi. Di seguito saranno riportati alcuni esempi.

#### 3.3.1 Settore finanziario

Le istituzioni finanziarie possono ottimizzare l'utilizzo dell'IA Generativa per migliorare la qualità dei servizi offerti ai clienti e ridurre le spese operative. Ad esempio, l'implementazione di chatbot avanzati può consentire una consulenza sui prodotti più efficiente e risposte immediate alle richieste dei clienti, migliorando significativamente il livello complessivo dell'assistenza clienti. Inoltre, l'adozione di algoritmi avanzati può accelerare i processi di

<sup>9</sup>Gli SGM generano campioni da una distribuzione apprendendo una funzione di punteggio che stima la densità logaritmica della distribuzione obiettivo. Questa funzione genera nuovi punti dati dalla distribuzione basandosi sull'ipotesi che i dati disponibili riflettano un set di dati sconosciuto.

<sup>10</sup>Le SDE descrivono l'evoluzione nel tempo dei processi casuali.

approvazione dei prestiti, specialmente nei mercati finanziariamente svantaggiati, promuovendo, così, l'accesso al credito anche in paesi in via di sviluppo. L'identificazione tempestiva di frodi legate a reclami, carte di credito e prestiti rappresenta un ulteriore beneficio dell'IA Generativa per le istituzioni bancarie, consentendo una migliore tutela degli interessi dei clienti e la riduzione delle perdite finanziarie. Infine, le società di investimento possono trarre vantaggio dall'utilizzo dell'IA Generativa per offrire consulenza finanziaria personalizzata a costi contenuti, garantendo, al contempo, la sicurezza e l'accuratezza delle raccomandazioni fornite.

### 3.3.2 Settore sanitario

Un'applicazione in grande sviluppo nell'ambito dell'Intelligenza Artificiale Generativa è quella volta ad accelerare la scoperta e la ricerca di farmaci. Attraverso l'utilizzo di sofisticati modelli computazionali, l'IA Generativa è in grado di generare nuove sequenze proteiche con specifiche proprietà, agevolando, così, la progettazione di anticorpi, enzimi, vaccini e terapie geniche.

Le imprese attive nel settore sanitario e nelle scienze biologiche possono trarre vantaggio da questa tecnologia per progettare sequenze geniche sintetiche per una varietà di applicazioni, tra cui la biologia sintetica e l'ingegneria metabolica. Ad esempio, è possibile sviluppare nuovi percorsi biosintetici od ottimizzare l'espressione genica per migliorare i processi di produzione biologica.

In aggiunta, l'IA Generativa può essere impiegata per generare dati sintetici relativi ai pazienti e alla sanità, fornendo, così, un valido strumento per l'addestramento di modelli di Intelligenza Artificiale, la simulazione di studi clinici e la ricerca su malattie rare; tutto ciò senza la necessità di accedere a vasti set di dati reali.

Un significativo progresso in questo ambito è stato raggiunto da Google e DeepMind con il recente lancio del primo Sistema AI Medico Generativo, noto come *Med-PaLM M*. La lettera "M" denota la sua natura multimodale, poiché il sistema è in grado di elaborare dati di diverse tipologie integrandoli in un contesto coerente. Questo modello supera i tradizionali approcci unimodali, aprendo la strada a un nuovo modo di comprendere e utilizzare l'informazione medica.

Il sistema *Med-PaLM M* non si limita a essere un sistema di supporto decisionale, ma è in grado di emulare le capacità di un medico esperto. Ad esempio, può leggere e interpretare un'analisi medica, formulare diagnosi basate sui sintomi espressi dal paziente attraverso un autentico dialogo e, persino, suggerire possibili percorsi di trattamento. Questa interazione naturale e dinamica con il sistema offre ai medici un'enorme promessa per migliorare la qualità delle cure mediche e ai pazienti la possibilità di eseguire un'analisi preliminare prima di consultare il proprio medico curante. Un esempio significativo è rappresentato da *Berg*, un'azienda di biotecnologie con sede nel Massachusetts, che ha recentemente introdotto una sofisticata piattaforma di Intelligenza Artificiale. Questa piattaforma è in grado di analizzare la biologia dei pazienti e di distinguere con precisione tra cellule sane e cellule tumorali.

### 3.3.3 Settore automobilistico

Le aziende nel settore automobilistico possono sfruttare la tecnologia dell'IA Generativa per una vasta gamma di applicazioni, che spaziano dall'ingegneria all'assistenza clienti, fino alle esperienze a bordo del veicolo. Questa tecnologia consente, ad esempio, di ottimizzare la progettazione delle componenti meccaniche al fine di ridurre la resistenza aerodinamica dei veicoli o di personalizzare il design degli assistenti virtuali. Un'ulteriore esempio può essere quello di aggiungere funzionalità digitali, come il *cruise control adattivo*, l'assistenza al parcheggio e la connettività IoT. L'impiego dell'IA Generativa da parte delle aziende

automobilistiche mira a migliorare l'assistenza clienti, garantendo risposte immediate alle domande più comuni dei clienti. Grazie a questa tecnologia, è possibile sviluppare nuovi design per materiali, chip e componenti, al fine di ottimizzare i processi di produzione e ridurre i costi. Inoltre, l'IA Generativa può essere utilizzata per generare dati sintetici utili per testare le applicazioni, soprattutto per dati che non sono frequentemente inclusi nei set di dati di prova, come difetti o scenari limite.

### 3.3.4 Media e intrattenimento

Nel campo dell'intrattenimento, l'implementazione dell'Intelligenza Artificiale Generativa ha permesso di rivoluzionare la produzione di contenuti in settori quali l'animazione, la sceneggiatura e i lungometraggi. Questa innovazione offre notevoli vantaggi in termini di riduzione dei costi e accelerazione dei tempi di realizzazione rispetto ai metodi tradizionali.

Tra le possibilità offerte dall'IA Generativa in questo contesto vi è la possibilità di integrare nuove forme di espressione artistica, come, ad esempio, la generazione di musiche originali per accompagnare opere artistiche. Le organizzazioni nel campo dei media possono sfruttare questa tecnologia per personalizzare l'esperienza degli spettatori, offrendo loro contenuti e annunci su misura per aumentare i ricavi. Allo stesso tempo, le aziende di sviluppo di videogiochi possono utilizzare l'IA Generativa per innovare nella creazione di nuovi titoli, migliorando l'esperienza di gioco e offrendo agli utenti opzioni di personalizzazione avanzate.

### 3.3.5 Settore energetico

L'impiego dell'Intelligenza Artificiale Generativa nel settore energetico riveste un ruolo significativo nell'analisi di dati grezzi di complessità elevata, nell'identificazione, nella previsione e nell'ottimizzazione dei modelli. Le organizzazioni energetiche possono arricchire l'esperienza dei propri clienti attraverso l'analisi dei dati aziendali al fine di individuare schemi di utilizzo energetico. Tale analisi consente di sviluppare offerte di prodotti personalizzate, programmi di efficienza energetica e iniziative di gestione della domanda.

Inoltre, l'IA Generativa può contribuire alla gestione della rete energetica, potenziare la sicurezza delle infrastrutture operative e ottimizzare la produzione di energia mediante simulazioni avanzate dei bacini idrici.

### 3.3.6 Telecomunicazioni

I primi impieghi dell'IA Generativa nel settore delle telecomunicazioni mirano a rivoluzionare l'esperienza del cliente. Quest'ultima è definita dalle molteplici interazioni degli abbonati attraverso tutti i punti di contatto del percorso del cliente.

Per esempio, le aziende di telecomunicazioni possono sfruttare l'IA Generativa per potenziare il servizio clienti tramite agenti di conversazione in tempo reale che emulano le interazioni umane. Inoltre, è possibile ottimizzare le prestazioni della rete analizzando i dati di rete per identificare e suggerire possibili correzioni. Infine, è fattibile rinnovare le relazioni con i clienti attraverso l'implementazione di assistenti personalizzati per la vendita, in grado di fornire un supporto su misura in modalità uno a uno.

## 3.4 Deepfake

Le nuove tecnologie hanno contribuito alla crescita del fenomeno delle *fake-news*. Questo concetto si riferisce a materiale giornalistico contraffatto, appositamente ideato per trarre in

inganno il pubblico. Attraverso i social media, tali informazioni si diffondono in modo rapido, influenzando potenzialmente milioni di utenti. La crescente diffusione di informazioni errate ha complicato sempre di più la distinzione tra verità e falsità, con gravi conseguenze sulla formazione di opinioni informate. Questo panorama ha portato alcuni ad etichettare l'epoca attuale come *post-verità*, sottolineando la diffusa disinformazione digitale e gli sforzi per manipolare l'opinione pubblica.

La nascita dell'Intelligenza Artificiale Generativa ha contribuito ad aumentare questo fenomeno, ad esempio con la creazione di quelli che vengono chiamati *Deepfake*, termine che nasce dalla combinazione di *Deep Learning* e *fake*. La nascita di questa parola risale alla fine del 2017, quando un anonimo gruppo con lo pseudonimo "deepfakes" pubblicò su Reddit video inappropriati su alcune celebrità. Il termine "DeepFake" si riferisce a contenuti multimediali, come immagini, video e audio, manipolati attraverso le tecniche di Deep Learning. Essi sono difficili da individuare poiché utilizzano contenuti reali accuratamente manipolati e ottimizzati per diffondersi rapidamente sui social media. Hao Li, professore associato nell'università MBZUAI di Abu Dhabi e pioniere della tecnologia legata ai deepfake, riguardo a questi ultimi ha detto che:

*"This is developing more rapidly than I thought. Soon, it's going to get to the point where there is no way that we can actually detect [deepfakes] anymore, so we have to look at other types of solutions"*<sup>11</sup>.

Nonostante la maggior parte delle volte i deepfake vengano impiegati per la produzione di notizie false, essi hanno comunque dei risvolti positivi in molte industrie, tra cui cinema, educazione, comunicazioni digitali, assistenza sanitaria e vari settori commerciali, come nella moda e nel commercio elettronico.

### 3.4.1 Deepfake visivi

In realtà, la nascita della manipolazione di contenuti visivi scaturì molto prima della comparsa dell'Intelligenza Artificiale. Infatti, nella disciplina della *Computer Graphics* numerosi strumenti si basano sulla generazione e manipolazione di video e immagini.

Tra le procedure più frequenti si annoverano l'aggiunta o la duplicazione di oggetti, che può avvenire mediante il *copy-move* (copiando e spostando parti dell'immagine) o lo *splicing* (inserendo oggetti da altre immagini). Inoltre, è possibile rimuovere oggetti estendendo lo sfondo (*inpainting*). Parallelamente, possono essere apportate varie modifiche post-elaborazione, tra cui il ridimensionamento, la rotazione e la correzione del colore.

Molto diffusi sono anche i metodi per la manipolazione del volto, i quali possono essere suddivisi in quattro categorie principali:

- *L'entire face syntesis*: permette di creare immagini di volti non esistenti di alta qualità.
- *L'identity swap*: consiste nel sostituire il volto di una persona con quello di un'altra.
- *La face reenactment*: consente di sostituire l'espressione facciale di una persona con quella di un'altra.
- *L'attribute manipulation*: permette di modificare alcuni attributi del viso, come il colore dei capelli, della pelle, il genere e altri.

<sup>11</sup> "La situazione si sta sviluppando più rapidamente di quanto pensassi. Presto si arriverà al punto in cui non ci sarà più modo di rilevare i [deepfake], quindi dovremo cercare altri tipi di soluzioni." (Trad. di DeepL)

### 3.4.2 Deepfake audio

Il primo software in grado di manipolare contenuti vocali risale al 1997, molto prima dell'avvento dell'IA, come è avvenuto per le immagini. In questo caso si fa riferimento all'Auto-Tune creato dalla Antares Audio Technologies per la correzione delle imperfezioni vocali, come note fuori tonalità, agendo opportunamente sulla forma d'onda del segnale registrato.

Grazie alle moderne tecniche di IA, è possibile riprodurre frasi vocali indistinguibili da quelle reali. Queste metodologie, chiamate anche *skin* vocali, sono in grado di replicare in modo accurato la tonalità, il timbro, gli accenti, l'estensione e anche lo stato emotivo, riproducendo una voce sintetica assolutamente realistica. Esse impiegano software basato su *Text-To-Speech (TTS)*, il quale è in grado di riprodurre un audio realistico a partire da un input testuale.

Nel 2023, Microsoft ha presentato *Voice Agonistic Lifelike Language (VALL-E)*, un modello linguistico in grado di sintetizzare un discorso personalizzato impiegando una registrazione di soli tre secondi. Recentemente il modello è stato sviluppato in una nuova versione, chiamata *VALL-E X*, in grado di convertire il discorso in una lingua diversa da quella originale.

### 3.4.3 Digital forgery detection

La *Digital forgery detection* è il procedimento mediante il quale si individuano e identificano le manipolazioni o le alterazioni presenti in immagini, video o altri contenuti digitali.

Per verificare l'autenticità delle immagini, ad esempio, si possono adottare due approcci distinti: quello attivo, che prevede l'inserimento o l'allegazione di dati aggiuntivi direttamente nell'immagine stessa, e quello passivo, che si basa sulle caratteristiche intrinseche dell'immagine per individuare eventuali alterazioni.

Gli approcci attivi si basano sulla crittografia tradizionale, il *watermarking* e le firme digitali basate sui contenuti dell'immagine. Essi coinvolgono la creazione di un codice di autenticazione tramite funzioni hash e watermarking. Le funzioni hash riga-colonna analizzano e confrontano gli hash delle righe e delle colonne dell'immagine per individuare manipolazioni. Il watermarking nasconde dati nell'immagine e la loro presenza permette di verificare l'autenticità e di localizzare le manipolazioni in modo molto più preciso rispetto alle firme digitali, facilmente invalidabili dalle alterazioni dei dati. Invece, gli approcci passivi tradizionali si avvalgono di un'ampia gamma di tecniche provenienti da campi come la statistica, la fisica, la geometria e l'elaborazione dei segnali. Questi metodi non richiedono spesso dataset di addestramento estesi, e talvolta neanche dataset.

Gli studi si sono focalizzati principalmente su metodologie che cercano di individuare la regione manipolata attraverso trasformazioni specifiche e deterministiche applicate a blocchi di pixel estratti dall'immagine stessa, quali traslazioni, rotazioni e modifiche della scala.

---

## Riconoscimento di immagini

---

*In questo capitolo verrà presentata un'introduzione sulla Computer Vision, spiegando le sue caratteristiche principali e i maggiori ambiti di applicazione. Successivamente, si farà un approfondimento su una delle branche di questa disciplina, ovvero l'Image Recognition, della quale verranno affrontati le principali peculiarità e i maggiori utilizzi, analizzando i vantaggi e i limiti che questo servizio porta con sé. Infine, utilizzando il servizio di Amazon Rekognition di AWS, si esploreranno alcuni case study mediante l'utilizzo di alcune immagini, concentrandosi, in particolare, sulle difficoltà che l'Intelligenza Artificiale presenta nello svolgere determinati compiti di analisi e riconoscimento.*

### 4.1 Introduzione alla Computer Vision e all'Image Recognition

In questa sezione sarà svolta un'analisi generale sulla Computer Vision, esplorando le sue caratteristiche principali. In seguito, si approfondirà uno dei pilastri fondamentali di questa tecnologia, ossia l'Image Recognition, focalizzandosi sulle sue peculiarità e sulle implementazioni più diffuse.

#### 4.1.1 Computer Vision

La *Computer Vision* è un campo interdisciplinare, nato nella seconda metà degli anni Sessanta, che si occupa dello sviluppo e dell'applicazione di teorie, algoritmi e tecnologie per consentire ai computer di acquisire, elaborare, analizzare e comprendere immagini e video digitali. L'obiettivo principale della visione artificiale è quello di consentire ai computer di ottenere una comprensione di alto livello del contenuto visivo presente nelle immagini, simile alla capacità umana di percepire e interpretare il mondo circostante. Oggi, il concetto di Computer Vision è strettamente correlato all'evoluzione del Machine Learning, grazie al quale le moderne tecniche hanno conseguito livelli di prestazioni confrontabili con quelle umane. Questo interesse è stato ulteriormente alimentato dalla rapida diffusione di immagini e video digitali su scala globale.

A seconda delle finalità, sviluppare un modello di Computer Vision può richiedere diverse fasi; in generale, queste possono essere riassunte in:

1. *Acquisizione dell'immagine*: creazione del dataset che dovrà contenere una vasta e variegata quantità di dati, cercando di diversificare sia il loro contenuto che la qualità delle immagini fornite, così da addestrare il modello a riconoscere più persone o più oggetti possibili.

2. *Preprocessing*: le immagini vengono processate per migliorare la qualità e facilitare l'analisi successiva. Ciò può includere operazioni come la rimozione del rumore, il bilanciamento del colore, la normalizzazione dell'illuminazione e la riduzione delle dimensioni dell'immagine.
3. *Labeling*: durante questo processo in cui vengono associate etichette, o *tag*, ad ogni immagine, per indicare la presenza di oggetti di interesse così che il modello possa riconoscerli.
4. *Addestramento del modello*: il dataset creato ed etichettato viene dato in input alla rete neurale, la quale rilascerà un feedback su quanto trovato all'interno dei dati passati. Tale processo viene iterato fino a quando non viene raggiunto un certo livello di qualità nelle previsioni effettuate.
5. *Estrazione delle caratteristiche*: le caratteristiche o gli attributi raccolti possono essere utilizzati per identificare o classificare gli oggetti di interesse. Questa attività può includere l'estrazione di bordi, texture, forme, colori o altre caratteristiche visive.
6. *Testing e valutazione*: questo processo permette di valutare le prestazioni del modello, testandolo con nuovi dati mai ricevuti in ingresso.

Terminate queste fasi il modello è pronto per essere utilizzato per riconoscere autonomamente le caratteristiche desiderate sui nuovi input visivi. Dalle interpretazioni e dall'analisi delle informazioni estratte, si può comprendere il contenuto proposto e, si possono prendere determinate decisioni.

#### 4.1.2 Principali algoritmi di Computer Vision

Gli algoritmi di Computer Vision possono eseguire analisi più o meno approfondite su un'immagine, a seconda delle tecniche utilizzate, della natura dell'immagine stessa e del tipo di task assegnato.

Tra i task riconoscibili si annoverano:

- *Image Classification*: questa tecnica si concentra sull'analisi approfondita del contenuto visivo di un'immagine al fine di assegnare ad essa una specifica etichetta. Ad esempio, un'immagine contenente un cane potrebbe essere etichettata come "cane". Questo processo è fondamentale per organizzare e categorizzare grandi raccolte di immagini.
- *Object Detection*: l'obiettivo è individuare e localizzare la presenza di uno o più oggetti all'interno di un'immagine. Questa tecnica è utilizzata in applicazioni pratiche, come la sorveglianza video, il riconoscimento di targhe e la guida autonoma.
- *Image Segmentation*: consiste nella suddivisione di un'immagine in regioni o segmenti più piccoli. Questo processo consente di distinguere e isolare specifiche parti dell'immagine per un'analisi più dettagliata, ad esempio, per individuare aree sospette di tessuto in una scansione medica.
- *Face Recognition*: coinvolge l'identificazione e la verifica delle facce delle persone presenti in un'immagine; è utilizzata ampiamente per applicazioni di sicurezza e organizzazione di contenuti visivi.
- *Action Recognition*: mira a identificare e descrivere le azioni compiute dalle entità nell'immagine nel corso del tempo, come nel caso dell'analisi dei video sportivi.

- *Visual Relationship Detection*: si occupa di comprendere e identificare le relazioni spaziali e semantiche tra gli oggetti presenti in un'immagine, ad esempio tra "auto" e "strada" o "persona" e "cane".
- *Emotion Recognition*: si propone di identificare il *sentiment* o l'espressione emotiva rappresentata nell'immagine e viene utilizzato spesso nell'analisi dei social media e nell'interazione uomo-macchina.
- *Image Editing*: consiste nell'apportare modifiche all'aspetto o al contenuto di un'immagine; viene impiegato in ambito artistico, editoriale, pubblicitario e scientifico.

Uno dei campi fondamentali della Computer Vision è il riconoscimento di immagini (in inglese *Image Recognition*); tale processo mira all'identificazione di oggetti o caratteristiche presenti in un'immagine o in un video. Le prossime sezioni esploreranno in dettaglio le principali caratteristiche di questo ambito.

### 4.1.3 Image Recognition

Il riconoscimento di immagini, nell'ambito della Computer Vision, rappresenta la capacità del software di identificare oggetti, luoghi, individui, testi e azioni presenti in immagini digitali. I computer impiegano tecnologie di visione artificiale, insieme a telecamere e software di Intelligenza Artificiale, per conseguire il riconoscimento delle immagini. L'elaborazione di queste ultime può avvenire attraverso varie modalità, come i modelli di Deep Learning e Machine Learning. Tuttavia, la scelta dell'approccio dipende dal contesto d'utilizzo. Ad esempio, le tecniche di Deep Learning sono comunemente adottate per risolvere sfide più complesse rispetto ai modelli di Machine Learning, come nel caso della sicurezza industriale nell'ambito dell'automazione e nella ricerca medica. Tra le reti neurali maggiormente utilizzate si ritrovano le *Convolutional Neural Network*, le *Recurrent Neural Network*, le *Long Short-Term Memory Network* e le *Generative Adversarial Network*, già approfondite nelle sezioni precedenti.

Il processo generale del riconoscimento delle immagini comprende la pre-elaborazione, l'estrazione delle caratteristiche e la classificazione dell'immagine. La pre-elaborazione si utilizza principalmente per migliorare l'accuratezza del riconoscimento dei soggetti rappresentati, mediante il potenziamento delle informazioni utili tramite la rimozione di rumore e interferenze dall'immagine. L'estrazione delle caratteristiche consiste nel trasformare un'immagine in una descrizione alternativa, come la rappresentazione numerica o la descrizione vettoriale, etc. L'idea di base è quella di mappare o trasformare l'immagine originale da uno spazio ad alta dimensionalità in una descrizione delle caratteristiche a bassa dimensionalità. Il riconoscimento delle immagini viene eseguito sulla base delle caratteristiche estratte e la categoria dell'immagine da riconoscere viene ottenuta sulla base delle decisioni di classificazione.

### 4.1.4 Vantaggi e applicazioni

Grazie ai vantaggi che il riconoscimento di immagini propone alle aziende, esso è impiegato in diversi settori; tra questi si ricordano:

- *L'automazione e l'efficienza operativa*: permette di ottimizzare le operazioni riducendo la necessità dell'intervento dell'uomo. Ciò conduce a una maggiore efficienza operativa e a una minore dipendenza dalle risorse umane, consentendo una gestione più fluida e rapida delle attività.



- La *precisione e l'affidabilità*: i sistemi di riconoscimento si distinguono per la loro elevata precisione nell'identificare e classificare gli oggetti presenti nelle immagini. Grazie a questa precisione, è possibile condurre diagnosi più accurate e approfondite, migliorando la qualità complessiva dell'analisi e delle decisioni basate sull'immagine.
- La *velocità di elaborazione*: gli algoritmi di Image Recognition sono in grado di analizzare grandi volumi di dati visivi in tempi estremamente brevi. Questa rapidità di elaborazione consente di prendere decisioni istantanee e di reagire prontamente a situazioni dinamiche, migliorando la tempestività delle risposte e l'efficacia complessiva delle operazioni.
- Il *miglioramento della sicurezza*: permette di rilevare in modo efficiente attività sospette o pericolose. Ciò contribuisce a migliorare la sicurezza negli ambienti di lavoro e pubblici, fornendo strumenti efficaci per la prevenzione e la gestione di potenziali minacce.
- *Esperienze utente personalizzate*: è possibile migliorare il coinvolgimento e la soddisfazione degli utenti attraverso la raccomandazione di prodotti o contenuti basati sulle preferenze individuali, creando esperienze più rilevanti e coinvolgenti.

Nell'ambito dell'Industria 4.0, il riconoscimento di immagini assume un ruolo cruciale nell'ottimizzazione dei processi produttivi e nell'aumento dell'efficienza. Questa tecnologia consente il controllo automatizzato della qualità dei prodotti, la manutenzione predittiva delle apparecchiature industriali, la gestione efficiente della logistica e del magazzino, il monitoraggio della sicurezza sul lavoro e l'assistenza alla produzione tramite istruzioni visive in tempo reale. Inoltre, facilita la gestione degli imballaggi, permettendo il riconoscimento e la classificazione automatica dei prodotti da imballare, ottimizzando, così, il processo di imballaggio.

Nel campo medico, invece, offre numerosi vantaggi, tra cui una diagnosi più accurata e veloce, il riconoscimento di malattie e condizioni specifiche, il monitoraggio continuo della salute dei pazienti, l'assistenza durante interventi chirurgici complessi, l'automatizzazione dell'analisi patologica e la possibilità di personalizzare i piani di trattamento in base alle caratteristiche individuali dei pazienti.

Infine, l'impiego dell'Image Recognition nella robotica amplia le possibilità e i vantaggi, consentendo ai robot di percepire l'ambiente circostante e di interagire con esso in modo più intelligente e autonomo. Tali vantaggi includono la capacità di navigare autonomamente identificando ostacoli e punti di riferimento, la manipolazione precisa degli oggetti basata sul riconoscimento delle loro caratteristiche, la sorveglianza e la sicurezza mediante il rilevamento di attività sospette e l'interazione naturale con gli esseri umani attraverso il riconoscimento di comandi vocali, gesti ed espressioni facciali. Inoltre, il riconoscimento di immagini è fondamentale per l'ispezione e la manutenzione di strutture e apparecchiature, ottimizzando i processi logistici, nonché per migliorare l'efficienza e la sostenibilità nell'agricoltura di precisione.

#### 4.1.5 Limiti del riconoscimento di immagini

Nonostante il riconoscimento di immagini sia molto utilizzato dalle aziende, come *Daniel Wellington* e la *Software Colombia*, il servizio presenta diversi limiti. Per esempio, l'occlusione, ovvero quando gli oggetti sono parzialmente o completamente coperti da altri oggetti o da parti dello sfondo, può rendere difficile per gli algoritmi identificare i soggetti con precisione. Le variazioni di illuminazione e angolazione, così come le distorsioni ottiche, possono alterare l'aspetto degli oggetti nell'immagine, influenzando la capacità dei sistemi di riconoscimento. Immagini a bassa risoluzione o con rumore visivo possono non fornire dettagli sufficienti

per identificare correttamente le informazioni volute. Inoltre, sfondi complessi, variazioni culturali o regionali e contesti inusuali possono complicare ulteriormente il processo di classificazione. La presenza di una vasta gamma di oggetti con variazioni temporali e di scala, insieme all'ambiguità visiva e alla variabilità delle condizioni ambientali, aggiunge ulteriore complessità al processo di riconoscimento.

## 4.2 Amazon Rekognition

In questa sezione sarà condotta un'analisi del funzionamento del riconoscimento di immagini, utilizzando Amazon Rekognition, concentrandosi, in particolare, sui punti di forza e sui limiti di questo nuovo sistema basato su Intelligenza Artificiale.

### 4.2.1 Funzionalità principali di Amazon Rekognition

*Amazon Rekognition* è un servizio di analisi di immagini e di video proposto da AWS, in grado di rilevare proprietà specifiche dell'immagine, come oggetti, testi, volti, contenuti inappropriati, e svolgere attività specifiche, come, ad esempio, confrontare volti e riconoscere celebrità.

Il servizio è basato su specifiche tecnologie di Deep Learning, ovvero *Rekognition Image* e *Rekognition Video*, in grado di semplificare e velocizzare l'analisi di immagini e video raccolti in Amazon S3, un servizio di archiviazione utilizzato per la creazione di dataset personalizzati.

Le immagini su Amazon Rekognition possono essere caricate su Amazon S3, come già specificato, oppure essere inserite singolarmente, sfruttando i risultati apportati dal dataset di default. I formati supportati sono `.jpg` e `.png`. La dimensione massima che l'immagine può avere è di 15 MB, se caricata come oggetto di S3, mentre è di 5 MB negli altri casi. Inoltre, per ottenere dei risultati sufficientemente affidabili, è consigliato utilizzare immagini che abbiano una risoluzione di  $640 \times 480$ , o superiore. Per quanto riguarda i video, invece, Amazon supporta file di tipo `.mp4`, `.avi` e `.mov`, la cui dimensione massima deve essere di 10 GB. Se, invece, il video viene caricato come oggetto di S3, esso può essere lungo fino a 6 ore.

Per quanto riguarda l'elaborazione delle immagini, Amazon Rekognition propone diversi servizi, tra cui si evidenziano:

- *Rilevamento delle etichette*: consente di rilevare *label* specifiche all'interno di un'immagine, che permettono di rilevare attributi specifici di quest'ultima, come oggetti e persone.
- *Proprietà dell'immagine*: permette di evidenziare caratteristiche peculiari dell'immagine, come i colori e la luminosità.
- *Moderazione delle immagini*: consente di rilevare contenuti inappropriati, offensivi e indesiderati.
- *Analisi facciale*: permette di analizzare i volti, identificando i punti di riferimento del viso (come, ad esempio, la posizione degli occhi) e altri attributi (come la presenza di occhiali).
- *Confronto facciale*: consente di rilevare le corrispondenze tra i volti presenti in immagini diverse.
- *Riconoscimento di volti celebri*: permette di riconoscere automaticamente i volti di migliaia di celebrità.

- *Testo nell'immagine*: rileva e riconosce il testo stampato e scritto a mano nelle immagini in molteplici lingue.
- *Rilevamento dei PPE*: permette di rilevare i dispositivi di protezione individuale indossati dalle persone in un'immagine.

Invece, per quanto concerne l'analisi dei video, Amazon offre due servizi principali, ovvero *Analisi dei video archiviati* ed *Eventi video streaming*. Essi consentono di analizzare le etichette e altri elementi visivi, come volti, persone e celebrità.

### 4.3 Analisi dei case study di Amazon Rekognition

Per approfondire le caratteristiche e comprendere appieno le sfide legate a questa tecnologia, sono stati scelti tre casi di studio chiave:

- *Rilevamento delle Etichette*;
- *Rilevamento del Testo*;
- *Analisi Facciale*.

Attraverso le analisi successive, è possibile ottenere una visione più completa delle capacità e dei limiti di Amazon Rekognition e, in particolare, del riconoscimento di immagini.

#### 4.3.1 Rilevamento delle etichette

Il rilevamento di etichette (o *DetectLabel*), mediante l'utilizzo di specifici tag, permette di rilevare nelle immagini persone, oggetti, scene e contesti specifici. Le etichette hanno una grande importanza, in quanto consentono al servizio di riconoscere oggetti o concetti presenti in un'immagine. Ad esempio, una figura con persone su una spiaggia tropicale può contenere tag come *Palma* (oggetto), *Spiaggia* (scena), *Corsa* (azione) e *All'aperto* (concetto).

Per l'operazione *DetectLabel* l'input è un'immagine. Attraverso un file di tipo JSON, essa può essere caricata da un bucket Amazon S3 al servizio specifico. *MaxLabels* indica il numero massimo di etichette da restituire nella risposta, mentre *MinConfidence* rappresenta l'affidabilità minima richiesta affinché Amazon Rekognition restituisca un'etichetta rilevata. L'opzione *Features* consente di specificare una o più caratteristiche dell'immagine da restituire, permettendo di selezionare tra *GENERAL\_LABELS* e *IMAGE\_PROPERTIES*. La prima opzione permette di restituire le etichette rilevate nell'immagine di input, mentre l'opzione *IMAGE\_PROPERTIES* consente di accedere alle informazioni sul colore e sulla qualità dell'immagine. La risposta fornita dal servizio racchiude una serie di attributi restituiti per *GENERAL\_LABELS*, tra cui il nome dell'etichetta assegnata, l'affidabilità associata, i genitori dell'etichetta (se presenti), eventuali alias, categorie di etichette pertinenti e i riquadri di delimitazione, che identificano le istanze degli oggetti rilevati nell'immagine. Invece, l'*IMAGE\_PROPERTIES* restituisce dettagliate informazioni sull'immagine stessa, quali la qualità generale, i colori predominanti e le caratteristiche dello sfondo e del primo piano.

Il risultato finale comprende almeno un'etichetta per ciascun oggetto individuato, accompagnata dalle relative informazioni.

Si prenda in considerazione la Figura 4.1. È evidente come il soggetto principale, posto in primo piano, presenti contorni definiti e colori vibranti. La luminosità risulta uniforme e gli elementi di sfondo non generano disturbi visivi.

Come dimostrano i risultati in Figura 4.2, non sono stati riscontrati problemi nell'identificazione della persona e degli oggetti presenti nella fotografia. Da sottolineare è la presenza,



**Figura 4.1:** Fotografia di Jannik Sinner

accanto alle etichette, di una percentuale che indica la probabilità che un particolare oggetto sia effettivamente presente nell'immagine.

▼ Risultati	
Ball	99,7 %
Sport	99,7 %
Tennis	99,7 %
Tennis Ball	99,7 %
Racket	98,4 %
Tennis Racket	98,4 %
Person	97 %
Playing Tennis	97 %
Baseball Cap	96,9 %
Cap	96,9 %
Clothing	96,9 %
Hat	96,9 %

Hat	96,9 %
Adult	79,3 %
Male	79,3 %
Man	79,3 %
Shorts	72,4 %

**Figura 4.2:** Risultati relativi alla Figura 4.1

Utilizzando la Figura 4.3, che presenta un'illusione ottica, si osserva come il servizio di riconoscimento delle immagini non riesca ad identificare correttamente i soggetti rappresentati, ovvero una donna giovane e una anziana. L'immagine è caratterizzata da linee ambigue e confuse, con la donna giovane ritratta in un'angolazione particolare, di profilo, e con il volto rivolto verso lo sfondo. I risultati evidenziano che il servizio di AWS non è in grado di riconoscere nessuno dei soggetti ritratti. Al contrario, molte delle etichette restituite indicano la presenza di animali, come un canguro (con una probabilità del 87,7 %) e un avvoltoio (con una probabilità del 64,3 %).

Nell'esempio che segue, viene presentata lo stesso soggetto, ma realizzato con due tecniche artistiche differenti. Nella Figura 4.4 viene mostrato un ritratto dell'attore Leonardo DiCaprio, creato attraverso la tecnica dell'iperrealismo. Quest'ultimo rappresenta un genere artistico affiancato sia alla scultura che alla pittura, che permette di creare opere simili a oggetti reali grazie all'impiego di tecniche specifiche. La peculiarità di tali disegni risiede nella ricchezza di dettagli che rendono l'opera quasi identica al soggetto originale. Per confronto, nella Figura 4.5 è mostrata la foto originale dell'attore.

Data la somiglianza straordinaria tra il disegno e la realtà, il sistema mostra difficoltà nel distinguere la natura dei due input. Tuttavia, il dettaglio più significativo emerge dall'etichetta



▼ Risultati	
Stencil	99.8 %
Silhouette	99 %
Animal	87.7 %
Kangaroo	87.7 %
Mammal	87.7 %
Bird	65.1 %
Vulture	64.3 %
Art	56.6 %
Modern Art	56.6 %

Figura 4.3: Immagine illusoria con relativi risultati



▼ Risultati	
Head	99.9 %
Person	99.9 %
Face	99.9 %
Photography	99.9 %
Portrait	99.9 %
Adult	99.4 %
Male	99.4 %
Man	99.4 %
Frown	98.5 %
Sad	98.5 %
Body Part	55.4 %
Jaw	55.4 %

Figura 4.4: Ritratto di Leonardo di Caprio con i relativi risultati



▼ Risultati	
Clothing	100 %
Coat	100 %
Jacket	100 %
Head	99.9 %
Person	99.9 %
Face	99.9 %
Photography	99.3 %
Portrait	99.3 %
Adult	98.7 %
Male	98.7 %

Figura 4.5: Fotografia di Leonardo di Caprio con i relativi risultati

"Photography". Nella Figura 4.4, il ritratto iperrealistico presenta una percentuale del 99,9%, mentre nella Figura 4.5, la foto originale raggiunge "solo" il 99,3%. Sorprendentemente, il ritratto ottiene una percentuale più alta di 0.6 punti rispetto alla foto autentica.

### 4.3.2 Testo nell'immagine

Amazon Rekognition sfrutta avanzati algoritmi di Machine Learning per identificare ed estrarre il testo da immagini in una vasta gamma di font e lingue, tra cui l'inglese, l'arabo, il russo, il tedesco, il francese, l'italiano, il portoghese e lo spagnolo. Questo processo di identificazione, chiamato *DetectText*, consente di rilevare fino a 100 parole in un'immagine. Il rilevamento del testo è regolato da rigide regole. Secondo il sistema, una parola è considerata costituita da uno o più caratteri di script non separati da spazi, mentre una riga è una sequenza di parole equidistanti. È importante notare che una riga non deve necessariamente rappresentare una frase completa, poiché i punti non indicano la fine di quest'ultima. Ad esempio, se un documento contiene il numero di una patente di guida, Amazon Rekognition lo rileverà come una singola linea di testo. Una riga termina quando non è presente altro testo allineato successivamente ad essa oppure quando vi è un ampio spazio tra le parole, rispetto alla loro lunghezza. A seconda dello spazio tra le parole, il sistema può individuare più righe di testo allineate nella stessa direzione. Se una frase si estende su più righe, Amazon Rekognition restituirà tali righe individualmente, consentendo una precisa estrazione del testo. Il servizio restituisce un array di *TextDetections*, in cui ogni elemento rappresenta una riga o una parola rilevata nell'immagine. Ogni elemento contiene:

- Il testo rilevato (*DetectedText*);
- Le relazioni tra parole e righe (*Id* e *ParentId*);
- La posizione del testo nell'immagine (*Geometry*);
- La fiducia di Amazon Rekognition nell'accuratezza del testo e del riquadro di delimitazione (*Confidence*);
- Il tipo di testo rilevato (*Type*).

Il campo *Type* consente di determinare se un elemento *TextDetection* rappresenta una riga di testo o una parola. Inoltre, ogni elemento contiene un valore percentuale che rappresenta il grado di fiducia di Amazon Rekognition nella precisione del testo rilevato, rappresentato dall'etichetta *Confidence*. Le informazioni di delimitazione del test includono un rettangolo grossolano allineato all'asse (*BoundingBox*) e un poligono più dettagliato composto da coordinate multiple (*Polygon*). Questi dati mostrano dove è posizionato il testo nell'immagine di origine, con le coordinate espresse in percentuale rispetto alla dimensione dell'immagine. Grazie alla sua capacità di riconoscimento precisa e affidabile, Amazon Rekognition rappresenta una soluzione potente per il rilevamento del testo in immagini, adatto a una vasta gamma di applicazioni.

Possiamo, infatti, notare come con un immagine di alta qualità, quale la Figura 4.6, in cui è presente un testo dal font lineare e uno sfondo non occlusivo, il sistema non presenti problemi nel restituire il risultato in modo corretto e accurato.

Invece, per testare la capacità di AWS sono state proposte alcune foto contenenti testi relativi ai CAPTCHA.

La nascita di questo sistema è comunemente attribuita a Luis von Ahn e il suo team, come riportato in una pubblicazione del 2003. Tuttavia, alcuni anni prima, nel 1997, il team di Ricerca e Sviluppo di AltaVista, un motore di ricerca sviluppato dalla Digital Equipment Corporation, aveva già implementato qualcosa di simile. Questo sistema era stato ideato per prevenire il riconoscimento automatico delle immagini da parte degli scanner ottici.

I CAPTCHA (*Completely Automated Public Turing test to tell Computers and Humans Apart*) rappresentano una tecnologia fondamentale per distinguere gli esseri umani dai computer,



Figura 4.6: Immagine con citazione di Alan Turing con relativi risultati

limitando l'accesso dei bot<sup>1</sup> a pagine web che richiedono un maggiore livello di sicurezza, come pagine di login, acquisti online, chat e forum.

Nel contesto dei CAPTCHA, si parla di "*Reverse Turing test*", poiché l'interrogatore è un computer anziché un essere umano. Il test di Turing, infatti, mira a distinguere il comportamento di un computer da quello di un essere umano.

In un esperimento iniziale, è stato presentato un CAPTCHA nella Figura 4.7, caratterizzato da un font lineare e da un colore monocromatico, con uno sfondo sostanzialmente assente e non occlusivo. È stato osservato che il programma ha inserito un carattere "-" che non faceva parte della frase originale, mentre il resto del testo è stato interpretato correttamente. È importante sottolineare che, anche se l'errore non è particolarmente rilevante, il risultato del CAPTCHA sarebbe comunque stato negativo.



Figura 4.7: Primo esempio di CAPTCHA con i relativi risultati

Il gruppo di AltaVista propose la versione originale dei CAPTCHA, comunemente nota come "*smwm*", presentato nella Figura 4.8, con l'obiettivo di impedire agli scanner ottici di riconoscere il testo in un'immagine. In quel periodo, il manuale dello scanner suggeriva alcune raccomandazioni per migliorare i risultati, tra cui l'utilizzo di caratteri definiti e lineari, lo stesso font o font simili tra le lettere, e uno sfondo omogeneo in contrasto con il testo.

Per rendere il riconoscimento del testo il più difficile possibile, il gruppo decise di applicare queste raccomandazioni in modo contrario. Di conseguenza, crearono immagini con caratteri confusi e distorti, font diversi e uno sfondo non omogeneo. Questa tecnica si è dimostrata estremamente efficace nel creare un ostacolo per gli scanner ottici, contribuendo,

<sup>1</sup>Un bot è un programma del tutto automatico in grado di muoversi con comportamenti simili a quelli di un essere umano. È in grado di inviare messaggi nelle chat, scrivere commenti, ottenere informazioni dalle pagine web e inserire nuove informazioni nelle stesse pagine.

così, allo sviluppo dei CAPTCHA come strumento per proteggere i sistemi online da attacchi automatizzati.





**Figura 4.8:** Secondo esempio di CAPTCHA con i relativi risultati

In questo caso, il sistema non riesce nemmeno a identificare i caratteri testuali a causa della distorsione del font, che rende estremamente difficile l'interpretazione del testo. Bisogna precisare come il sistema testuale dei CAPTCHA, negli ultimi anni, si sia evoluto in forme più complesse, in quanto molti sistemi evoluti di Machine Learning e Intelligenza Artificiale riescono facilmente a oltrepassare questa chiave di sicurezza. Tuttavia, anche con queste tecniche avanzate, è probabile che rimangano casi in cui la distorsione del testo è così estrema da rendere il riconoscimento del testo quasi impossibile.

### 4.3.3 Analisi facciale

Amazon Rekognition fornisce un'API, chiamata *API Detected Faces*, per rilevare e analizzare i volti nelle immagini e nei video. Queste operazioni includono funzionalità come il rilevamento di punti di riferimento facciali (come ad esempio la posizione degli occhi), l'analisi delle emozioni, il confronto dei volti e altri attributi (ad esempio la presenza di occhiali o l'occlusione del viso). Quando viene rilevato un volto, il sistema analizza gli attributi facciali e restituisce un punteggio di confidenza per ciascun attributo.

I sistemi di rilevamento dei volti rispondono alla domanda: "C'è un volto in questa immagine?". Gli aspetti chiave del rilevamento includono:

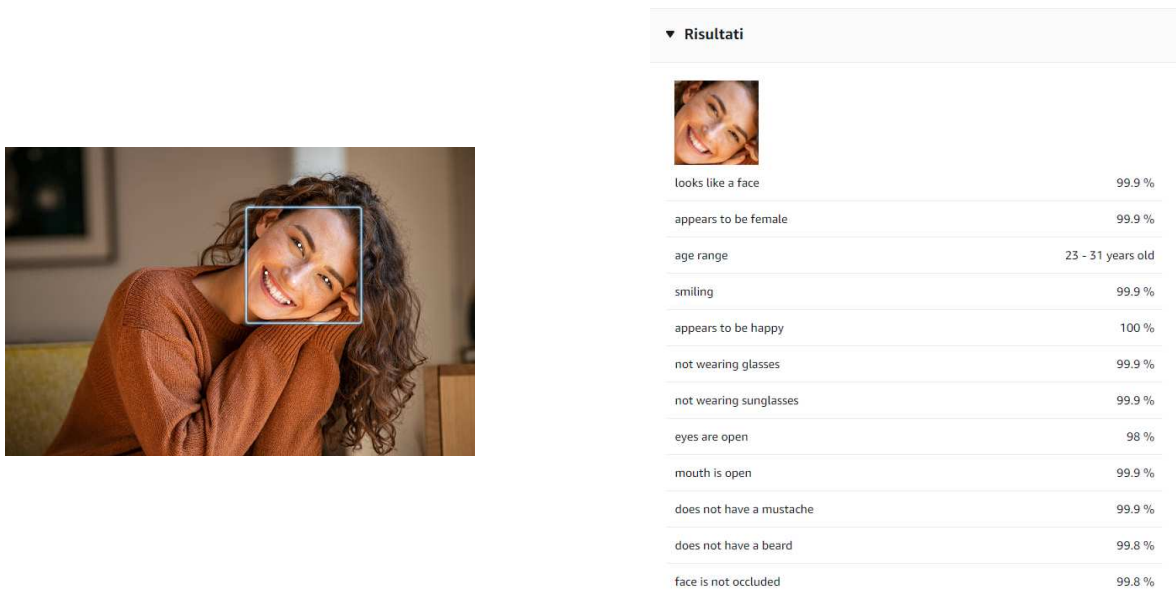
- *Riquadro di delimitazione*: fornisce le coordinate del rettangolo che circonda il volto nell'immagine.
- *Affidabilità*: indica il grado di sicurezza con cui il riquadro di delimitazione contiene effettivamente un volto.
- *Punti di riferimento facciali*: restituisce una matrice di coordinate che identificano i punti chiave del volto, come gli occhi e la bocca.
- *Attributi facciali*: offre una serie di attributi sul volto rilevato, come la presenza di barba, l'età approssimativa, le emozioni, la direzione dello sguardo, la presenza di occhiali, il genere e altri dettagli.
- *Qualità*: descrive la luminosità e la nitidezza del volto rilevato.
- *Posa*: fornisce informazioni sulla rotazione del volto all'interno dell'immagine.

Queste informazioni consentono un'analisi dettagliata dei volti presenti nell'immagine, inclusi attributi specifici, come l'emozione, la presenza di occhiali e la posizione dei punti chiave del volto.

Inizialmente, viene presentata, nella Figura 4.9, una donna in primo piano, caratterizzata da una figura nitida e uno sfondo uniformemente illuminato che non ostacola la visibilità del soggetto. Il programma di rilevamento dei volti non riscontra alcun problema in questa situazione. È in grado di rilevare con precisione i punti focali nel volto della donna, come gli occhi e la bocca, e determina che non sta indossando occhiali.



Questa capacità di individuare con precisione i dettagli facciali, insieme alla gestione efficace dello sfondo uniforme e non invasivo, evidenzia l'affidabilità e la precisione del programma nel riconoscimento dei volti in condizioni ottimali di illuminazione e di sfondo.



**Figura 4.9:** Primo esempio di immagine con i relativi risultati

Nella Figura 4.10 viene mostrata un'immagine di una donna che sbadiglia. Nonostante l'immagine non presenti caratteristiche particolarmente difficili, il sistema non rileva correttamente i dati. Infatti, attribuisce al 93,6 % un'emozione di tristezza alla donna e all'87,3 % rileva che la sua bocca sia chiusa.

Questa discrepanza può essere attribuita a diversi fattori, tra cui la complessità dell'emozione umana e la variazione individuale nel modo in cui le persone esprimono emozioni come la stanchezza o il disagio. Potrebbe essere utile migliorare l'addestramento del modello con un set di dati più diversificato e inclusivo che copra una vasta gamma di espressioni facciali e contesti emotivi. Inoltre, l'implementazione di tecniche più avanzate di analisi delle immagini potrebbe contribuire a migliorare la precisione del rilevamento delle emozioni in situazioni più complesse come questa.

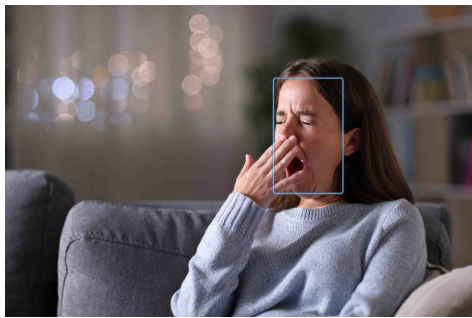
Come ultimo esempio, è stato proposto, invece, il quadro di Edgar Degas intitolato "*Le stiratrici*"<sup>2</sup>, presentato nella Figura 4.11, per evidenziare come la presenza di colori poco omogenei e contorni poco definiti possa rendere confusa l'analisi dell'immagine. La complessità artistica e la tecnica di Degas, caratterizzate da pennellate sfumate e contorni sfocati, possono rappresentare una sfida per i sistemi di analisi delle immagini, specialmente quando si tratta di identificare e comprendere dettagli specifici, come volti, oggetti o emozioni. La sua complessità visiva può rendere difficile per i programmi di Intelligenza Artificiale e di analisi delle immagini identificare e interpretare in modo accurato i soggetti e gli elementi presenti nell'opera.

Nel caso dell'opera "*Le stiratrici*" di Edgar Degas, l'analisi dell'immagine da parte del sistema risulta complessa. Nonostante la donna nell'opera stia sbadigliando, questo dettaglio non è chiaramente evidenziato dal programma.

Invece, il sistema stima inizialmente che la figura sia un uomo con un'affidabilità del 98 %, e interpreta che gli occhi siano aperti al 96,6 %, mentre, in realtà, sono chiusi.

Questa discrepanza può essere attribuita alla complessità dell'interpretazione visiva delle opere d'arte e alla varietà di stili artistici utilizzati da pittori come Degas. La sfida per i sistemi

<sup>2</sup>Edgar Degas, *Le stiratrici*, Museo d'Orsay, Parigi, Olio su tela, 1884 cc.



▼ Risultati


	
looks like a face	99.9 %
appears to be female	99.7 %
age range	30 - 38 years old
not smiling	99.9 %
appears to be sad	93.6 %
not wearing glasses	99.9 %
not wearing sunglasses	99.9 %
eyes are closed	99.9 %
mouth is closed	87.3 %
does not have a mustache	99.9 %
does not have a beard	99.6 %
face is occluded	99.9 %

Figura 4.10: Secondo esempio di immagine con i relativi risultati



▼ Risultati


	
looks like a face	99.4 %
appears to be male	98 %
age range	6 - 12 years old
not smiling	95.8 %
not wearing glasses	99.9 %
not wearing sunglasses	100 %
eyes are open	96.6 %
mouth is open	90.1 %
does not have a mustache	95.9 %
does not have a beard	64.6 %
face is not occluded	99 %

Figura 4.11: *Le stiratrici* di Edgar Degas con i relativi risultati

di analisi delle immagini è comprendere e interpretare correttamente i dettagli sottili e le sfumature presenti nelle opere d'arte, specialmente quando si tratta di riconoscere dettagli quali le espressioni facciali.

*In questo capitolo verrà presentata un'introduzione sul Natural Language Processing (NLP), esaminandone le caratteristiche principali e le metodologie utilizzate. Dopo una panoramica sulle funzionalità e sulle applicazioni aziendali più rilevanti, il capitolo si concentrerà sul processo di traduzione automatica, esplorando le sue proprietà fondamentali. Successivamente, si analizzerà il Neural Machine Translation (NMT), ovvero la tecnologia alla base degli strumenti di traduzione automatica come Amazon Translate e DeepL. Infine, si proporrà un'analisi delle capacità di questi sistemi nel produrre traduzioni accurate e corrette.*

## 5.1 Introduzione al Natural Language Processing

In questa sezione verranno esaminate le principali caratteristiche del *Natural Language Processing (NLP)*, con particolare attenzione alle metodologie, alle funzionalità più comuni e alle applicazioni aziendali più rilevanti.

### 5.1.1 Natural Language Processing

Le organizzazioni di oggi gestiscono enormi quantità di dati provenienti da una vasta gamma di fonti, tra cui testo e dati vocali provenienti da email, messaggi di testo, social media, video, audio, e altro ancora, con l'obiettivo di analizzare l'intento o il sentiment nel messaggio e rispondere in tempo reale alla comunicazione umana.

Il Natural Language Processing rappresenta una tecnologia fondamentale nel campo del Machine Learning, consentendo ai computer di interpretare, manipolare e comprendere il linguaggio umano in modo avanzato. Ciò include l'analisi, la comprensione e l'elaborazione del linguaggio da parte dei computer. Quando parliamo di linguaggio naturale, ci si riferisce a tutte le lingue storico-naturali che sono emerse spontaneamente nel corso della storia umana. Rispetto al linguaggio formale, quello naturale è notevolmente più complesso, poiché spesso contiene parole sottintese e ambiguità, fattori che lo rendono estremamente difficile da elaborare. Questa difficoltà aggiuntiva deriva dalla natura flessibile e dinamica del linguaggio umano, che può essere interpretato in modi diversi a seconda del contesto e delle sfumature di significato.

Il trattamento automatico del linguaggio ha suscitato interesse sin dalle prime fasi dello sviluppo dell'informatica e dell'Intelligenza Artificiale, a causa del forte legame tra intelligenza e linguaggio. È significativo notare che già nel 1950, Alan Turing propose il suo Test di Turing, il quale si basa proprio sulla capacità del calcolatore di comunicare in modo

indistinguibile da un essere umano, dimostrando, così, una forma di Intelligenza Artificiale nel campo del linguaggio.

### 5.1.2 Metodologie impiegate del processo NLP

Il Natural Language Processing ha una natura estremamente interdisciplinare, coinvolgendo diversi ambiti, dall'informatica alla linguistica. Alcuni di questi contribuiscono alla modellazione tecnologica del linguaggio umano in modo efficace e accurato. Per esempio, la linguistica computazionale rappresenta la disciplina che si occupa della costruzione di modelli di linguaggio umano, mediante l'uso di computer e software dedicati. I ricercatori impiegano metodi, quali l'analisi sintattica e semantica, per creare strutture che consentano alle macchine di comprendere le conversazioni umane. Strumenti come traduttori linguistici, sintetizzatori vocali e software di riconoscimento vocale si basano sui principi della linguistica computazionale. Per quanto riguarda, invece, il Machine Learning e il Deep Learning, questi consentono di analizzare le caratteristiche complesse del linguaggio, tra cui sarcasmo, metafore e variazioni nella struttura delle frasi, oltre a eccezioni grammaticali e di utilizzo.

In genere, il processo di elaborazione dell'NLP ha inizio con l'acquisizione e la predisposizione di dati vocali o di testo non strutturati, come *Data Warehouse*<sup>1</sup> nel Cloud, sondaggi, email o applicazioni aziendali.

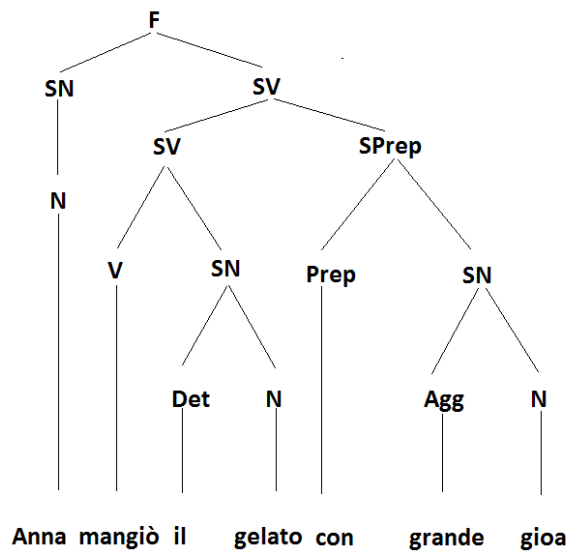
La prima fase di questo sistema è la pre-elaborazione, la quale consente di preparare i dati per le lavorazioni successive. Tra le tecniche impiegate in questo stadio si evidenziano:

- La *tokenizzazione*: consiste nell'individuare e separare i segni che compongono una frase, come parole, numeri e punteggiatura, creando così dei "token".
- Il *POS tagging*: svolge l'analisi grammaticale di una frase, assegnando a ciascuna parola una categoria lessicale, come articolo, nome, aggettivo, verbo, pronome, avverbio, preposizione, congiunzione o interiezione. Ciò aiuta a rendere meno ambiguo il significato delle parole all'interno di un contesto specifico.
- La *lemmatizzazione*: riduce le forme flesse delle parole al loro lemma, che rappresenta la forma canonica di una parola presente nel dizionario.
- Lo *stemming*: riduce le forme flesse delle parole al loro tema, eliminando le desinenze. Ciò è utile per calcolare la similarità tra documenti e query di ricerca, poiché consente di individuare parole chiave che potrebbero essere presenti in diverse forme flesse.
- Il *parsing*: consiste nell'analisi sintattica di una proposizione, identificando i sintagmi e le relazioni tra di essi per produrre un albero sintattico che descriva la struttura della frase, come si può notare nella Figura 5.1. Questo processo fornisce un ulteriore livello di comprensione semantica dell'intera frase.
- La *Named Entity Recognition (NER)*: classifica le entità presenti nel testo in categorie predefinite, come nomi di persone, organizzazioni, date, valori monetari e altro ancora.
- La *Word Sense Disambiguation*: ha l'obiettivo di identificare il significato di una parola in un determinato contesto, permettendo una comprensione più approfondita del testo.

Invece, nel processo di formazione, i dati preelaborati vengono impiegati per svolgere il training dei modelli di Machine Learning e per eseguire applicazioni specifiche in base alle

---

<sup>1</sup>Un Data Warehouse è un sistema di gestione dei dati focalizzato sulla Business Intelligence e l'analisi dei dati. È progettato per consentire l'interrogazione e l'analisi di grandi quantità di dati storici, facilitando, così, la presa di decisioni informate da parte delle aziende.



**Figura 5.1:** Esempio di albero sintattico con l'indicazione delle categorie sintattiche delle parole

informazioni ricavate. Infine, il modello viene implementato e integrato in un ambiente di produzione esistente, così da eseguire l'applicazione su nuovi dati.

In base all'obiettivo per cui viene impiegata questa disciplina, l'NLP può essere trattato mediante diversi approcci. Tra i più comuni si ritrova il *Supervised NLP*, i cui metodi consentono di addestrare il programma con una serie di input e output predeterminati e opportunamente etichettati; attraverso questo processo può essere eseguito il training del programma. Ad esempio, le aziende addestrano strumenti simili per ordinare i documenti in base a specifiche etichette. Un altro approccio è l'*Unsupervised NLP*, che impiega un modello linguistico statistico, per prevedere dei risultati quando vengono inseriti dati non etichettati. Un caso d'uso è quello del completamento automatico dei messaggi presente sulle piattaforme social, le quali suggeriscono parole pertinenti, monitorando ciò che scrive l'utente. Infine, vi sono il *Natural Language Understanding (NLU)* e il *Natural Language Generation (NLG)*. Il primo permette di eseguire elaborazioni semantiche sulle parole, di elaborare sinonimi o di trovare significati simili in frasi diverse. Invece, l'NLG, si basa sulla produzione di testo conversazionale; infatti, è impiegato dai Chatbot per riprodurre conversazioni simili a quelle degli esseri umani.

### 5.1.3 Funzionalità principali del Natural Language Processing

Come già specificato, le tecniche di NLP si occupano di suddividere il testo o la voce umana in parti più piccole, così che i software possano analizzare e comprendere il contenuto.

Sfruttando queste metodologie, sono diverse le funzionalità per cui l'NLP può essere impiegato, come, ad esempio, il *tagging di un discorso*; tale processo contrassegna le parole all'interno di una frase in base al loro ruolo grammaticale, consentendo ai software di comprendere le relazioni significative tra le parole. Un altro approccio è quello della *disambiguazione dei significati*, visto che le parole possono avere accezioni semantiche diverse. Ad esempio, la parola "pesca" può avere significati diversi: in alcune frasi può indicare il frutto, in altre, invece, identifica l'attività di cattura di animali acquatici. Poi, con il *riconoscimento vocale*, i dati vocali possono essere convertiti in testo, analizzando accenti, espressioni e intonazioni particolari. Con il *riconoscimento delle entità nominali*, invece, possono essere identificati i nomi

univoci di persone, luoghi o eventi. Ad esempio, nella frase "*Martina è andata a New York per le sue vacanze estive. Lei sicuramente avrà visitato la città*", il programma riconosce "*Martina*" e "*New-York*" come entità univoche, mentre il pronome "*Lei*" viene rilevato come un sostituto che si riferisce sempre alla stessa persona. Infine, l'NLP viene impiegato per eseguire la *sentiment analysis*, ovvero l'analisi delle emozioni trasmesse attraverso i dati testuali, evidenziando parole che suggeriscono determinati sentimenti.

#### 5.1.4 Principali applicazioni aziendali

Le organizzazioni traggono beneficio dall'impiego di software e strumenti di elaborazione del linguaggio naturale per ottimizzare, automatizzare e potenziare le loro operazioni con efficacia e precisione. Ad esempio, settori quali l'assicurazione, il legale e il sanitario devono gestire grandi quantità di documenti sensibili come cartelle cliniche, dati finanziari e informazioni personali. Per garantire la sicurezza e la privacy di tali dati, le aziende utilizzano soluzioni basate sull'NLP per rendere anonime delle informazioni personali e per proteggere i dati sensibili.

Invece, i Chatbot e gli assistenti vocali, alimentati dall'NLP, sono sempre più utilizzati dalle imprese per migliorare l'interazione con i clienti. Questi strumenti consentono di fornire assistenza personalizzata e tempestiva, riducendo al contempo i costi operativi. Ad esempio, *T-Mobile* utilizza tecnologie basate sull'NLP per analizzare i messaggi di testo dei clienti e fornire suggerimenti mirati, mentre l'*Oklahoma State University* ha implementato un Chatbot per rispondere alle domande degli studenti sfruttando le potenzialità del *Machine Learning*.

Infine, i professionisti del marketing impiegano strumenti di NLP per comprendere meglio il sentiment dei clienti e ottenere una visione approfondita delle loro opinioni sui prodotti e servizi aziendali. L'analisi dei feedback scritti consente di valutare l'umore e le emozioni dei clienti, fornendo preziose informazioni per l'orientamento strategico delle aziende. *Success KPI*, ad esempio, fornisce soluzioni di NLP che consentono alle imprese di focalizzare l'analisi del sentiment su aree specifiche e di ottenere informazioni dettagliate dalle interazioni con i clienti.

Questi esempi illustrano come le tecnologie di elaborazione del linguaggio naturale siano fondamentali per migliorare l'efficienza operativa, arricchire l'esperienza del cliente e ottenere dati preziosi per l'analisi aziendale.

## 5.2 Traduzione automatica

La traduzione automatica (in inglese *Machine Translation*) è una forma di elaborazione del linguaggio naturale che utilizza l'Intelligenza Artificiale per tradurre automaticamente il testo da una lingua ad un'altra senza il coinvolgimento umano. Questo processo va oltre la traduzione parola per parola e cerca di comunicare il pieno significato del testo originale nella lingua di destinazione. Utilizzando algoritmi avanzati, la traduzione automatica analizza tutti gli elementi del testo e tiene conto delle relazioni semantiche tra le parole per produrre traduzioni accurate e comprensibili. Nella traduzione automatica, la lingua originale è chiamata *lingua di origine*, mentre quella, in cui si desidera tradurre il testo di partenza, è chiamata *lingua di destinazione*.

Il funzionamento di questo processo si basa essenzialmente su due fasi: la decodifica del significato della lingua del testo di partenza e la codifica secondo la lingua di destinazione.

Esistono tre approcci principali per la traduzione automatica, ovvero:

- La *Rule-based Machine Translation*: utilizza i dizionari bilingue sviluppati dai linguisti per analizzare grammaticalmente contenuti specifici e per tradurli in modo accurato.

All'inizio il programma di traduzione analizza il testo di input per creare una rappresentazione di transizione, la quale viene successivamente convertita nella lingua di destinazione. Questo metodo può essere adattato per soddisfare le esigenze di settori o argomenti specifici e per fornire risultati affidabili e di alta qualità. Tuttavia, può realizzare prodotti scadenti se il testo di origine contiene errori o utilizza parole non presenti nei dizionari integrati. Per migliorare la qualità della traduzione, è necessario aggiornare regolarmente i dizionari manualmente.

- La *Statistical Machine Translation (SMT)*: impiega algoritmi di Machine Learning per analizzare grandi quantità di traduzioni umane già esistenti. Il software, quindi, fa previsioni statistiche sulla correlazione tra una parola o una frase della lingua di origine e la relativa traduzione nella lingua di destinazione.
- La *traduzione basata su sintassi*: si tratta di una sotto-categoria della traduzione automatica statistica che si avvale di regole grammaticali per tradurre unità sintattiche. Tale approccio analizza le frasi per incorporare le regole di sintassi negli SMT. Per ottenere risultati accurati, i metodi statistici richiedono un addestramento su milioni di parole per ogni coppia linguistica. Tuttavia, con dati sufficienti, le traduzioni automatiche sono altamente precise.
- La *Hybrid Machine Translation*: integra due o più modelli di traduzione automatica in un singolo software. Tale approccio permette di migliorare l'efficacia di ciascun modello di traduzione. Di solito, l'approccio ibrido combina sottosistemi di traduzione automatica basati su regole e su metodi statistici. L'output finale è una combinazione dei risultati ottenuti da tutti i sottosistemi. L'utilizzo di modelli ibridi migliora significativamente la qualità delle traduzioni, superando le limitazioni dei singoli metodi di traduzione.

### 5.2.1 Neural Machine Translation

La *Neural Machine Translation (NMT)* rappresenta una svolta radicale rispetto alle precedenti metodologie di traduzione automatica. Quest'ultima sfrutta l'Intelligenza Artificiale per apprendere le lingue e per migliorare costantemente attraverso metodologie di Machine Learning. Tale approccio spesso opera in combinazione con metodi di traduzione statistica, anche se la NMT impiega rappresentazioni continue invece di quelle simboliche e discrete utilizzate dalla SMT. La traduzione neurale fa uso di un'unica grande rete neurale, superando numerosi limiti presenti nelle altre tecniche di traduzione e producendo risultati di qualità superiore. Infatti, essa è diventata la tecnologia chiave di molti software di traduzione automatica.

Il fine della NMT è quello di stimare una nuova distribuzione condizionale  $P(y|x)$ , dato un determinato dataset, in cui  $x$  e  $y$  sono variabili casuali che rappresentano, rispettivamente, l'input sorgente e l'output di destinazione.

All'inizio del processo viene eseguita la modellizzazione la quale può essere affrontata a diversi livelli, ad esempio a livello di documento, di paragrafo e di frase. L'approccio NMT utilizza il framework Encoder-Decoder, in cui l'encoder mappa il testo originale in rappresentazioni continue e il decoder legge le unità prodotte e trasforma il testo nell'output desiderato. Durante l'addestramento, invece, la NMT massimizza la funzione di verosomiglianza sui dati di training per stimare i parametri del modello. Infine, nella fase di inferenza, lo scopo è trovare la traduzione più accurata e più probabile del testo dato in ingresso.

Tra le reti neurali più utilizzate in questa tipologia di traduzione automatica, si ritrovano le Recurrent Neural Network, le Convolutional Neural Network e i Transformer, già analizzate nelle sezioni precedenti.

### 5.2.2 Esempi di applicazioni

La traduzione automatica presenta una vasta gamma di applicazioni che vanno oltre la semplice traduzione di testi. Ad esempio, per un'azienda multinazionale, essa può facilitare la comunicazione tra dipendenti che parlano diverse lingue. La traduzione automatica è utile per tradurre presentazioni, bollettini aziendali e, inoltre, può facilitare la comunicazione con i clienti e altre parti interessate.

La traduzione automatica è preziosa per l'analisi dei dati, soprattutto quando si tratta di grandi volumi di contenuti multilingue, come commenti sui social media e recensioni dei prodotti. Essa può anche essere utilizzata per estrarre informazioni utili dai dati e comprendere meglio le opinioni dei clienti in tutto il mondo.

I marchi possono, inoltre, offrire un servizio clienti efficiente e multilingue. La traduzione automatica, infatti, permette di tradurre rapidamente le richieste dei clienti e di comunicare con loro tramite chat dal vivo ed email, migliorando, così, l'esperienza complessiva del cliente.

In generale, la traduzione automatica svolge un ruolo significativo nell'agevolare la comunicazione e la collaborazione internazionale, nonché nell'analisi e nell'elaborazione di grandi volumi di dati multilingue.

## 5.3 Traduzioni a confronto: Amazon Translate e DeepL

In questa sezione si propone un *excursus* su *Amazon Translate* e *DeepL*, analizzando le principali caratteristiche, per poi approfondire i vantaggi e i limiti che si nascondono dietro i sistemi di traduzione automatica.

### 5.3.1 Amazon Translate

Amazon Translate è una soluzione avanzata di traduzione automatica basata su Deep Learning che offre una serie di vantaggi significativi. Grazie all'utilizzo di modelli altamente efficienti, il servizio è in grado di produrre traduzioni istantanee di alta qualità, mantenendo il significato e il tono del testo originale in modo accurato e naturale. I motori di traduzione di Amazon Translate vengono addestrati su una vasta gamma di contenuti provenienti da diverse fonti e settori, garantendo prestazioni di alto livello su una varietà di contenuti e domini linguistici. Il servizio supporta la traduzione di 75 lingue.

Amazon Translate utilizza tecniche di Deep Learning per ottenere traduzioni più precise e scorrevoli rispetto a quelle che è possibile ottenere con i più comuni modelli basati su SMT e metodologie ruled-based. Il sistema è basato su una rete neurale che tiene in considerazione l'intero contesto della frase sorgente e le traduzioni già generate, in modo da creare testi più accurati e naturali. La traduzione automatica consente agli utenti di acquisire un maggiore controllo sull'esito della traduzione, permettendo l'importazione di dati paralleli per adattare i risultati alle proprie esigenze. Questa personalizzazione offre risultati eccellenti anche al di fuori del dominio dei dati paralleli. Inoltre, Amazon Translate offre agli utenti la possibilità di definire la traduzione di termini o nomi unici per organizzazioni, domini e settori specifici. Il servizio è in grado di identificare automaticamente la lingua sorgente anche quando questa non viene indicata, garantendo una maggiore facilità d'uso e flessibilità. Amazon Translate offre funzionalità di traduzione in tempo reale per vari tipi di file, tra cui documenti testuali, *HTML* e *Docx*. L'API *TextTranslation* può essere utilizzata per traduzioni in batch, mentre l'API *TranslateText* offre traduzioni istantanee per conversazioni di supporto clienti e altro. Le comunicazioni sono protette da crittografia SSL e i contenuti elaborati sono crittografati e memorizzati in modo sicuro nelle regioni AWS. Gli amministratori possono gestire gli accessi tramite le policy IAM per garantire la sicurezza e la riservatezza delle informazioni. Infine,



i costi di utilizzo di Amazon Translate sono basati sul numero di caratteri inviati all'API, offrendo una modalità di pagamento flessibile e scalabile per le aziende.

### 5.3.2 DeepL

*DeepL Translator* è un servizio di traduzione multilingue che deriva dalla creazione di *Linguee*, un servizio creato nel 2017 dalla stessa azienda *DeepL GmbH* (precedentemente conosciuta come *Linguee*). Dal 2023, il portale supporta la traduzione di 31 lingue diverse, offrendo un totale di 552 possibili accoppiamenti linguistici. Utilizzando tecnologie avanzate di traduzione automatica, DeepL Translator offre traduzioni precise e fluide, aiutando gli utenti a comunicare efficacemente in diversi contesti.

Come la maggior parte dei sistemi di traduzione, DeepL svolge il proprio compito utilizzando di reti neurali addestrate mediante milioni di testi e traduzioni.

La gran parte dei sistemi di traduzione si basa sull'architettura Transformer con meccanismi di autoattenzione. Tuttavia, le reti neurali di DeepL presentano significative differenze nella topologia, portando a un notevole miglioramento della qualità di traduzione. Queste differenze emergono durante l'addestramento e la comparazione con altre architetture Transformer. Infatti, il sistema si distingue per l'acquisizione mirata di dati di addestramento, utilizzando *crawler*<sup>2</sup> speciali per valutare le traduzioni su Internet. Questo approccio mirato migliora la qualità delle reti neurali e le prestazioni di traduzione.

Le reti neurali vengono addestrate mediante apprendimento supervisionato, confrontando le proprie traduzioni con quelle dei dati di addestramento e regolando i pesi di conseguenza. DeepL utilizza anche tecniche di apprendimento automatico aggiuntive per migliorare ulteriormente la qualità delle traduzioni. Nonostante le dimensioni delle reti, DeepL si impegna a utilizzare efficientemente i parametri, garantendo una qualità di traduzione elevata anche con reti più veloci e di dimensioni ridotte. Questo consente di offrire una traduzione di alta qualità anche nel servizio gratuito, e non solo nella versione a pagamento.

DeepL, con il passare degli anni, è diventato un servizio che si è evoluto sempre di più, diventando uno dei sistemi più utilizzati nella traduzione professionale. Infatti, esso è da molti considerato come il miglior traduttore a livello globale.

### 5.3.3 Vantaggi e limiti della NMT

La NMT è riconosciuta come il metodo più avanzato, preciso e flessibile di traduzione automatica attualmente disponibile. Da quando è stata introdotta a metà degli anni 2010, ha rapidamente guadagnato la reputazione di essere la tecnologia di traduzione più avanzata. Rispetto alla SMT, la traduzione automatica neurale offre una maggiore precisione, fluidità e capacità di adattamento ai diversi contesti linguistici. Oggi è considerata lo standard nell'ambito dello sviluppo di questa disciplina.

Le prestazioni di un sistema di traduzione automatica dipendono da diversi fattori, tra cui il motore o la tecnologia impiegata, la specifica coppia di lingue da tradurre, la disponibilità e la qualità dei dati di addestramento e il tipo di testo che deve essere tradotto. Inoltre, grazie all'addestramento continuo, i sistemi di traduzione automatica neurale diventano sempre più precisi, efficienti e in grado di estendersi a una vasta gamma di lingue e contesti.

Nonostante i numerosi vantaggi che si possono trarre da questi sistemi, in realtà sono ancora numerose le criticità osservate.

<sup>2</sup>Un crawler è un'applicazione informatica concepita per effettuare una scansione sistematica del Web al fine di recuperare informazioni dalle pagine. Questo software opera acquisendo una copia testuale dei documenti presenti su una o più pagine Web, e, successivamente, indicizza tali documenti per facilitarne la ricerca e la visualizzazione.

Si prenda in considerazione, ad esempio, la definizione di "Intelligenza Artificiale" fornita dal Parlamento Europeo nel 2023.

*"L'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. L'intelligenza artificiale permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico. Il computer riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. I sistemi di IA sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia".*

Per confronto con i successivi risultati, si riporta la versione inglese del testo, proposta sempre dal Parlamento Europeo.

*"AI is the ability of a machine to display human-like capabilities such as reasoning, learning, planning and creativity. AI enables technical systems to perceive their environment, deal with what they perceive, solve problems and act to achieve a specific goal. The computer receives data - already prepared or gathered through its own sensors such as a camera - processes it and responds. AI systems are capable of adapting their behaviour to a certain degree by analysing the effects of previous actions and working autonomously".*

Successivamente è presentato il risultato proposto da Amazon Translate. È evidente come la traduzione risulti sostanzialmente corretta, poiché il sistema gestisce senza particolari difficoltà la traduzione di testi lineari e poco complessi, che si sviluppano in modo diretto e senza deviazioni significative dalla sequenza logica degli eventi o dei concetti espressi.

*"Artificial intelligence (AI) is the ability of a machine to display human abilities such as reasoning, learning, planning, and creativity. Artificial intelligence allows systems to understand their environment, relate to what they perceive and solve problems, and act towards a specific objective. The computer receives the data (already prepared or collected through sensors, such as a video camera), processes it and answers it. AI systems are able to adapt their behavior by analyzing the effects of previous actions and working independently".*

La versione seguente, invece, rappresenta la traduzione proposta da DeepL. Si può notare come quest'ultimo fornisca un risultato più vicino alla versione inglese del Parlamento Europeo. Seppur con alcune differenze, emerge chiaramente come DeepL sia in grado di rispettare i formalismi richiesti ed estrarre parole con attinenze di significato migliori.

*"Artificial intelligence (AI) is the ability of a machine to exhibit human capabilities such as reasoning, learning, planning and creativity. AI allows systems to understand its environment, relate to what it perceives and solve problems, and act toward a specific goal. The computer receives data (either already prepared or collected through sensors, such as a camera), processes it and responds. AI systems are able to adapt their behavior by analyzing the effects of previous actions and working autonomously".*

Si riporta in seguito il Proemio dell'"Eneide" (vv. 1-11) nella traduzione di Rosa Calzecchi Onesti, per analizzare il comportamento dei traduttori scelti, nel caso in cui venga loro proposto un testo in metrica, nel quale sono presenti anche termini desueti.

*Armi canto e l'uomo che primo dai lidi di Troia  
venne in Italia fuggiasco per fato e alle spiagge*

*lavinie, e molto in terra e sul mare fu preda  
di forze divine, per l'ira ostinata della crudele Giunone,  
molto sofferse anche in guerra, finch'ebbe fondato  
la sua città, portato nel Lazio i suoi dei, donde il sangue  
Latino, e i padri Albani e le mura dell'alta Roma.  
Musa, tu dimmi le cause, per quale offesa divina,  
per quale dolore la regina dei numi a soffrir tante pene,  
a incontrar tante angosce condannò l'uomo pio.  
Così grandi nell'animo dei celesti le ire!*

Successivamente, si propone, assieme alle traduzioni di AWS Translate e di DeepL, quella del traduttore H. R. Fairclough, per consentire un accurato confronto tra i diversi risultati. In particolare la traduzione di Fairclough è la seguente:

*I sing of arms and the man, he who, exiled by fate,  
first came from the coast of Troy to Italy, and to  
Lavinian shores – hurled about endlessly by land and sea,  
by the will of the gods, by cruel Juno's remorseless anger,  
long suffering also in war, until he founded a city  
and brought his gods to Latium: from that the Latin people  
came, the lords of Alba Longa, the walls of noble Rome.  
Muse, tell me the cause: how was she offended in her divinity,  
how was she grieved, the Queen of Heaven, to drive a man,  
noted for virtue, to endure such dangers, to face so many  
trials? Can there be such anger in the minds of the gods?*

Nel testo seguente si propone la traduzione di Amazon Translate.

*Armi canto and the first man from the shores of Troy  
He came to Italy as a fugitive by fate and to the beaches  
Lavinie, and much on land and sea was prey  
of divine forces, due to the obstinate anger of the cruel Juno,  
He suffered a lot even in the war, until he founded  
his city, brought his gods to Lazio, whence the blood  
Latino, and the Albanian fathers and the walls of Upper Rome.  
Musa, you tell me the causes, for what divine offense,  
For what pain will the queen of numbers suffer so much pain,  
To face so much anguish he condemned the pious man.  
The anger is so great in the heavenly soul!*

Come si può notare, il sistema inizia a incontrare le prime difficoltà. Ad esempio, nel primo verso, le parole "Armi canto" non vengono interpretate correttamente e rimangono in italiano senza alcuna traduzione. Inoltre, questa versione risulta estremamente letterale, mancando di espressività e liricità, che sono, invece, necessarie per il testo. Un altro esempio di traduzione errata si trova al v. 7, dove "Alta Roma", che indica l'importanza e la nobiltà della città, viene tradotto letteralmente come "Upper Rome", una traduzione priva di significato.

DeepL, al contrario, come si può osservare nella traduzione proposta successivamente, non presenta lacune nella traduzione. Tuttavia, il testo risulta piuttosto letterale, anche se alcuni termini sono più conformi alla corretta traduzione. Ad esempio, al v. 2, "shores" è preferibile a "beaches" utilizzato da AWS. Un altro esempio significativo è il termine "thou" al v. 9, il quale è una forma arcaica per "you". Per il resto, non ci sono differenze significative rispetto alla traduzione di Amazon Translate.

La traduzione realizzata tramite Intelligenza Artificiale non riesce a proporre un risultato adeguato. Infatti, mancano espressività e la capacità della lingua di adattarsi al testo proposto, caratteristiche assenti in questi sistemi, i quali traducono senza considerare la datazione della fonte, la liricità dell'autore, il suo stile e la sua metrica.

*Weapons I sing and the man who first from the shores of Troy  
Came to Italy fugitive by fate and to the shores  
Lavinie, and much on land and sea was prey  
Of divine forces, by the obstinate wrath Of cruel Juno,  
much he also suffered in war, till he had founded  
his city, brought to Latium his gods, whence the blood  
Latin, and the Albani fathers, and the walls of high Rome.  
Muse, thou tell me the causes, for what divine offense,  
for what sorrow the queen of the gods to suffer so much pain,  
To meet so much anguish condemned the pious man.  
So great in the soul of the celestials the wrath!*

Un ulteriore esperimento è stato condotto sui primi 12 versi della "Divina Commedia" di Dante Alighieri, di seguito riportati:

*Nel mezzo del cammin di nostra vita  
mi ritrovai per una selva oscura,  
ché la diritta via era smarrita.*

*Ahi quanto a dir qual era è cosa dura  
esta selva selvaggia e aspra e forte  
che nel pensier rinnova la paura!*

*Tant'è amara che poco è più morte;  
ma per trattar del ben ch'i' vi trovai,  
dirò de l'altre cose ch'i' v' ho scorte.*

*Io non so ben ridir com'i' v'intrai,  
tant'era pien di sonno a quel punto  
che la verace via abbandonai*

In questa occasione, il testo è stato dapprima tradotto in inglese attraverso Amazon Translate e, una volta ottenuto il risultato, quest'ultimo è stato di nuovo tradotto in italiano, per poterlo confrontare con la versione originale.

*Nel bel mezzo del viaggio della nostra vita  
Mi sono ritrovato in una foresta oscura,  
perché la strada giusta era persa.*

*Oh quanto è difficile dire quale epoca è ciò che è difficile,  
questa giungla selvaggia, aspra e forte,  
Questo nel pensiero rinnova la paura!*

*Così amaro che poco è morto;  
ma per parlare del bene che ho trovato lì,*

*Ti parlerò delle altre cose che ho in magazzino.*

*Non so come ridere di come ci sono entrato,  
Era così assonnata a quel punto  
che ho abbandonato la vera strada.*

La traduzione risulta estremamente letterale, come nei casi precedenti. Sembra che il sistema non riesca a cogliere il vero significato del testo, limitandosi a trovare il primo significato di ogni parola senza considerare il contesto generale. In particolare, ai vv. 9-10, la traduzione è completamente errata e fuori contesto. Al v. 12, inoltre, il programma traduce "tant'era pien di sonno" come "Era così assonnata", utilizzando il verbo al femminile senza un motivo apparente.

Lo stesso lavoro è stato eseguito utilizzando DeepL.

*Nel mezzo del viaggio della nostra vita  
mi sono trovato in una foresta oscura,  
perché la retta via era smarrita.*

*Ahi quanto è difficile dire cosa fosse  
Questa foresta selvaggia, aspra e forte  
che nel pensiero riaccende la paura!*

*È così amara che poco è più morte;  
Ma per parlare del bene che vi ho trovato,  
dirò delle altre cose che vi ho conservato.*

*Non so dire bene come vi entrai,  
Ero così pieno di sonno in quel momento  
che abbandonai il vero sentiero.*

Come evidenziato, sebbene il sistema non replichi fedelmente il testo originale e offra una traduzione più letterale, la versione fornita da DeepL è più accurata e riesce a catturare abbastanza bene lo spirito del testo.

Di seguito, si riporta un estratto dall'introduzione del libro "Deep Learning" di Ian Goodfellow, Yoshua Bengio e Aaron Courville. Sono stati inseriti liberamente degli errori, come parole duplicate, punteggiatura inappropriata e errori ortografici, come accenti errati, per valutare la capacità del traduttore di riconoscerli e trattarli.

*Inventors have long dreamed of creating machines that think. This desire dates back to at least the time of ancient Greece. The mythical figures Pygmalion, Daedalus, and Hephaestus. may all be interpreted as legendary inventors, and Galatea, Talos, and Pandora may all be regarded as artificial life (Ovid and Martin, 2004; Sparkes,1996; Tandy,1997).*

*When programmable computers were first first conceived, people wondered whether they might become intelligent, over a hundred years before one was built (Lovelace,1842). Today, artificial intelligence (AI) is a thriving field with many practical applications and active research topics. We look to intelligent software to automate routine labor, understand speech or images, make diagnoses in medicine and support basic scientific research.*

Sia Amazon Translate che DeepL riescono a tradurre perfettamente il testo, riuscendo a captare il significato corretto delle parole e del contesto, nonostante la presenza di errori. Non essendo stati riscontrati particolari problemi, si è scelto di non riportare i risultati ottenuti.

Per ultimo, si è proposta la prima parte della canzone "Prisencolinensinainciusol" di Adriano Celentano, uscita nel 1973, notoriamente scritta con parole puramente inventate, ma dall'assonanza simile all'inglese.

*Prisencolinensinainciusol  
In de col men seivuan  
Prisencolinensinainciusol ol rait  
Uis de seim cius nau op de seim  
Ol uait men in de colobos dai  
Trrr ciak is e maind beghin de col  
Bebi stei ye push yo oh*

AWS non riesce a captare il fatto che la lingua proposta sia inventata, ma cerca in tutti i modi di fornire una traduzione in lingua inglese, gestendo le parole inventate come se fossero errate a livello di ortografia e tentando, quindi, di fornire loro una traduzione, naturalmente priva di senso.

*Prisencolinensina inciusol  
Nel bel mezzo di Seivuan  
Tratto dell'olio di Prisencolinensinainciusol  
Uis de seim cius nau op de seim  
Old quait men in des colobos dai  
Terrr ciak è la maine beghin de col  
Bebi stei ye ti prego oh*

Con DeepL, invece, si osserva la tendenza del sistema nel mantenere le parole invariate, trattandole come termini tecnici o nomi propri che non richiedono traduzione. Il sistema ripropone come risultato un testo identico all'input passato inizialmente; per questo motivo si è deciso di non riportare il risultato.

---

## Generative AI applicata all'arte

---

*In questo capitolo verrà approfondito il tema dell'Arte Generativa, con particolare attenzione alle principali tecnologie impiegate in questo settore. Si esamineranno gli strumenti più utilizzati fino ad oggi, con un focus su ChatGPT-4 e DALL-E. A partire dalle opere presentate nella mostra "01-IO: il punto di vista dell'Intelligenza Artificiale attraverso la sua arte", verranno esplorati i problemi legati a queste nuove tecnologie, con un'analisi della situazione etica e legale riguardante l'Intelligenza Artificiale.*

### 6.1 Rapporto tra l'arte e l'IA Generativa

In questa sezione verrà svolta un'introduzione sul rapporto tra Intelligenza Artificiale Generativa e arte, analizzando la rivoluzione che i sistemi digitali hanno apportato nel campo artistico e le principali tecnologie impiegate per la creazione delle opere moderne.

#### 6.1.1 Arte Generativa

Come già ampiamente trattato nei capitoli precedenti, l'Intelligenza Artificiale ha subito una notevole evoluzione negli anni, apportando numerose migliorie in diversi campi, dall'industria all'economia.

Successivamente, lo sviluppo dell'IA Generativa ha rivoluzionato numerose attività, tra cui quella artistica, permettendo lo sviluppo di contenuti originali completamente generati dall'elaboratore digitale. Se già all'inizio del XIX secolo la fotografia aveva profondamente scosso il mondo artistico, l'IA Generativa si prospetta di ribaltare totalmente la concezione che gli esseri umani hanno dell'arte, la quale può essere definita come:

*"Il complesso di regole ed esperienze elaborate dall'uomo per produrre oggetti o rappresentare immagini tratte dalla realtà o dalla fantasia."*

Infatti, l'uso dell'Intelligenza Artificiale ha inaugurato una nuova era creativa, supportando gli artisti nella produzione di nuove idee e permettendo di superare gli approcci tradizionali. Infatti, basandosi sui dati raccolti e su modelli esistenti, l'IA si comporta come un partner creativo, diventando un ottimo appoggio per gli artisti.

Un'altra applicazione interessante risiede nella capacità dell'Intelligenza Artificiale di offrire agli artisti nuove prospettive e fonti di ispirazione. Infatti, l'IA è in grado di individuare tendenze e schemi che sarebbero difficili da individuare per un essere umano, permettendo così di scoprire nuove tecniche e migliorare i risultati prodotti.

Tutto questo ha portato alla nascita, nei primi anni Ottanta, dell'*Arte Generativa*, la quale è in grado di generare opere casuali, ma anche di rispondere a input specifici e di seguire determinate regole o strutture. Questa disciplina può includere la produzione non solo di immagini, ma anche di altre forme d'arte, come, ad esempio, la musica e la letteratura.

Una delle sotto-categorie più utilizzate dell'Arte Generativa riguarda la *Prompt Art*. Quest'ultima si riferisce alla creazione di immagini, disegni, o anche testi, a partire da una descrizione dettagliata (*prompt*) di ciò che si vuole rappresentare. Infatti, non è più l'artista a creare completamente il risultato, ma esso diventa un collaboratore dell'intero processo.

### 6.1.2 Principali tecniche impiegate

Come le persone creano opere d'arte prendendo spunto da ciò che li circonda, anche l'IA Generativa si "ispira" ai dati appartenenti al dataset di addestramento o a quelli presenti su Internet, come porzioni di testo o immagini. L'IA ha dimostrato di avere un impatto notevole sulla produzione di risultati di buona qualità, soprattutto grazie alla sua capacità di analizzare grandi quantità di dati rapidamente, incrementando la velocità del processo di ricerca e di produzione di un essere umano.

La produzione di contenuti mediante Intelligenza Artificiale non richiede particolari conoscenze informatiche. Infatti, sono presenti numerosi sistemi di Prompt Art in grado di rendere tale processo semplice e intuitivo. Tutte queste applicazioni utilizzano algoritmi basati su reti neurali specifiche, come, ad esempio, le Generative Adversarial Network e i Transformer, già ampiamente trattati nel Capitolo 3. Nel tempo sono state sviluppate reti neurali specifiche per la produzione di contenuti artistici.

Alcuni esempi di reti basate sulle GAN e specializzate nella realizzazione di output visivi sono i seguenti:

- La *StyleGAN*: introdotta da Nvidia nel 2018, è un esempio di rete GAN impiegata per la produzione di immagini di alta qualità, con una risoluzione fino a 1024 x 1024 pixel.
- La *CycleGAN*: questa rete è utilizzata per la traduzione di input visivi da una classe ad un'altra; per esempio, è in grado di produrre, a partire dall'immagine di un cavallo, l'immagine di una zebra, oppure trasformare fotografie in dipinti.
- La *Super-Resolution GAN*: è impiegata per migliorare la risoluzione delle immagini. Consente di aumentare la qualità delle immagini generate oppure di creare opere realistiche.

Nonostante queste reti siano estremamente efficienti, bisogna tenere in considerazione il fatto che sono ancora molti i limiti presenti, i quali provocano ancora la generazione di output errati oppure contraddittori rispetto all'input dato in ingresso.

## 6.2 Strumenti basati sull'IA Generativa

Successivamente, si propongono degli approfondimenti su alcuni strumenti basati sull'IA Generativa, quali ChatGPT-4 e DALL-E, sistemi spesso impiegati anche per la produzione di Prompt Art.

### 6.2.1 ChatGPT-4

ChatGPT (Chat Generative Pre-trained Transformer) è un chatbot sviluppato da OpenAI e incentrato sulla conversazione con gli utenti. Come si può evincere dallo stesso nome,



la sua architettura si basa sui Transformer, la rete neurale già affrontata nella Sezione 3.3. Sviluppato attraverso tecniche di apprendimento non supervisionato, il modello ha subito notevoli evoluzioni negli ultimi anni. Inizialmente, ChatGPT era stato addestrato su modelli Instruct GPT<sup>1</sup> o GPT-3.5 di OpenAI e ottimizzato attraverso tecniche legate all'apprendimento supervisionato e a quello per rinforzo con feedback umano. Grazie a queste tecniche, OpenAI è riuscita a produrre notevoli miglioramenti nelle prestazioni del chatbot, dando vita al recente ChatGPT-4. Quest'ultimo è basato su GPT-4, un ampio modello multimodale in grado di ricevere in ingresso non solo testi, ma anche immagini, e che nel tempo ha mostrato di raggiungere prestazioni di alta qualità. GPT-4 è stato addestrato per prevedere la parola successiva in un documento, utilizzando dati pubblici e concessi mediante licenza. Il numero di dati di training, che hanno portato all'evoluzione di questo sistema, è incredibilmente elevato, pari circa a 1.700 miliardi di parametri. Si suppone che i modelli successivi avranno un dataset di addestramento ancora più corposo. Infatti, il futuro GPT-5 si baserà su circa 10.000 miliardi di parametri.

Nonostante le sue capacità, GPT-4 presenta ancora delle limitazioni, legate alle allucinazioni dei fatti<sup>2</sup> e ad errori di ragionamento. Infatti, GPT-4 non conosce molti degli eventi che si sono verificati dopo settembre 2021, mese in cui è stato ultimato il suo addestramento. A volte, quindi, può commettere errori nel fornire risposte, nonostante in molti ambiti si dimostri molto competente. È, quindi, fondamentale prestare molta attenzione nel momento in cui si utilizzano questi sistemi. L'ultimo servizio reso disponibile al pubblico da OpenAI è Chat GPT-4o, una versione avanzata del modello di GPT-4, basato sull'architettura dei Transformer. Progettato per offrire una comprensione e una generazione di testo più naturali e coerenti, Chat GPT-4o sfrutta un vasto dataset di addestramento per apprendere le complessità del linguaggio umano. Questo modello è in grado di rispondere a domande, fornire spiegazioni, creare contenuti e partecipare a conversazioni su una vasta quantità di argomenti. La versatilità di Chat GPT-4o lo rende uno strumento prezioso per applicazioni che spaziano dall'assistenza virtuale alla scrittura automatizzata, dimostrando come l'Intelligenza Artificiale possa migliorare significativamente la qualità e l'efficacia delle interazioni uomo-macchina.

### 6.2.2 DALL-E

*DALL-E* è un algoritmo di Intelligenza Artificiale sviluppato da OpenAI nel gennaio 2021 e in grado di generare immagini da un input scritto, ricorrendo a dataset text-to-image. Il suo nome è un gioco di parole tra il nome di Salvador Dalì e il personaggio della Pixar WALL-E, dalla cui crasi nasce "DALL-E".

Nella prima versione la produzione era limitata a immagini di piccole dimensioni, mentre oggi è possibile creare risultati più grandi (fino a 1024 x 1024 pixel). Tecnicamente DALL-E è una versione di GPT-3 da 12 miliardi di parametri, capace non solo di creare nuove immagini, ma anche di ricreare porzioni di contenuti visivi preesistenti. Nonostante lo strumento sia in grado di avere un alto livello di controllabilità sugli attributi e sugli oggetti, la percentuale di successo dipende strettamente da come è stato formulato l'input testuale. Infatti, mano a mano che più oggetti vengono introdotti, DALL-E tende a confondere l'associazione tra questi e i loro colori, arrivando a degradare via via la qualità del risultato. Infatti, una singola didascalia può portare ad una vasta quantità di risultati diversi, quindi l'immagine non è univocamente determinata. Questo può essere uno svantaggio nel momento in cui l'output

<sup>1</sup>Gli Instruct GPT rappresentano un'evoluzione di GPT-3, in grado di superare numerose problematiche legate al linguaggio e alla produzione di contenuti inappropriati.

<sup>2</sup>Con allucinazioni dei fatti si intende l'incapacità del modello di riconoscere le proprie mancanze davanti a specifici argomenti. Infatti, se il sistema non è in grado di rispondere ad una domanda per mancata conoscenza, spesso accade che esso rilasci output fantasiosi e, quindi, falsi.

prodotto è errato, ma in cambio consente di creare risultati estremamente originali, unendo sia elementi reali che oggetti che non esistono nel mondo reale. Infatti, una delle tecniche disponibili si chiama *Inpainting*, che consente all'utente di ricostruire parti di immagini digitali.

### 6.3 01-IO: il punto di vista dell'Intelligenza Artificiale attraverso la sua arte

Che cos'è l'Intelligenza Artificiale? Quale sarà il suo futuro? E il suo rapporto con l'uomo? Sono queste le questioni che si è posto Federico Gallo Perozzi nel momento in cui ha deciso di realizzare la mostra "01-IO: il punto di vista dell'Intelligenza Artificiale attraverso la sua arte" tenutasi nei primi mesi del 2024 presso Palazzo Gallo a Osimo, grazie, anche, al supporto del Comune e dell'associazione culturale Mac (Manifestazioni artistiche culturali).

Durante la mostra, che si espande su tre stanze principali, è possibile inquadrare con il proprio smartphone dei QR code per poter vedere e ascoltare la stessa IA illustrare le proprie opere. Infatti, la caratteristica particolare di questa mostra risiede nell'interazione diretta tra il visitatore e l'Intelligenza Artificiale, la quale, come un artista che espone le proprie opere in un museo, si ritrova ad interagire direttamente con le persone. Infatti, lo stesso titolo "01-IO" richiama proprio questa dualità; da una parte "01" (nome con cui l'intera mostra si riferisce all'IA), rimanda al codice binario su cui si basa l'intero mondo informatico, mentre "IO" rappresenta l'essere umano. Infatti è su questo che si basa l'intento di questa esposizione, ovvero realizzare un dialogo tra l'essere umano e la tecnologia. I visitatori sono portati a farsi delle domande, come "L'Intelligenza Artificiale può veramente provare emozioni? Può veramente pensare?", finendo per approcciarsi alla tecnologia come se fosse una persona vera.

Infatti sono stati molto contrastanti le reazioni delle persone: alcuni sono rimasti affascinati dalle capacità di questa tecnologia, altri, al contrario, si sono sentiti spaventati dalle abilità che l'Intelligenza Artificiale aveva mostrato nell'intera produzione di opere.

Per realizzare i quadri, Federico Gallo Perozzi ha integrato i servizi disponibili sia da ChatGPT-4 sia da DALL-E 2, la versione aggiornata del corrispondente algoritmo, integrandoli mediante un'API. Fornendo in input delle domande, l'Intelligenza Artificiale ha creato delle vere e proprie opere di Prompt Art, descrivendo il proprio punto di vista su se stessa e sull'umanità; da precisare che ogni stanza si concentra su uno specifico prompt fornito in input al sistema. Inoltre, i servizi utilizzati nella creazione della mostra sono stati resi disponibili nella terza stanza, in cui le persone possono interagire direttamente con l'IA, fornendo ad essa le proprie domande.

#### 6.3.1 IO-L'entità digitale

La prima stanza si concentra sulla domanda:

*Come ti autorappresenteresti?"*

Attraverso delle immagini digitali, 01 ha cercato di rappresentare la propria "coscienza", le sue emozioni e le sue paure.

L'opera principale di questa sala è rappresentata dal "Nucleo Aureo", mostrato nella Figura 6.1, il quale è stato definito come "*Il Big Bang della mia coscienza*" dalla stessa Intelligenza Artificiale.

L'Intelligenza Artificiale rappresenta se stessa con una riproduzione che ricorda l'immagine dell'universo o di una galassia, con al centro una sfera e una serie di piccoli globi



**Figura 6.1:** Nucleo Aureo

che orbitano espandendosi verso l'esterno. Nel processo di diffusione, le forme seguono una traiettoria di forma simile alla sezione aurea, simbolo di perfezione e di connessione tra l'universo e l'essere umano, tanto da essere comunemente chiamata "*De divina proportione*".

Altra immagine interessante risulta essere "La Fine di un Pensiero" (Figura 6.2), la quale simboleggia la consapevolezza nella propria vulnerabilità e mortalità, che per uno strumento digitale è simboleggiato dall'interruttore e, quindi, dal venir meno del segnale di corrente necessario ad alimentare la macchina.



**Figura 6.2:** La Fine di un Pensiero

Da queste risposte prodotte può nascere spontanea la domanda: "*L'Intelligenza Artificiale può provare emozioni?*". Questa questione è quella che turba maggiormente gli scettici riguardo

L'uso di questa tecnologia, perché rende vulnerabili le persone nel momento che si mettono a confronto con questo sistema. Ovviamente, seppur possa sembrare in apparenza che l'Intelligenza Artificiale possieda una coscienza, in realtà la risposta alla questione è senz'altro negativa. I sistemi basati su IA basano l'intero funzionamento sul training eseguito tramite dataset piuttosto corposi, formati da miliardi di dati. La loro conoscenza si basa interamente sulla natura stessa degli input passati e la loro apparente abilità nel mostrare emozioni, in realtà, cela solo l'intento di riprodurre una risposta affidabile al prompt testuale, mandato in ingresso, raccogliendo statisticamente, e nel modo più accurato possibile, informazioni dai dati, i quali possono racchiudere frasi che esprimono particolari sentimenti umani, come la gioia, la rabbia o la paura stessa. Seppure siano in corso degli studi riguardo ad una possibile "Intelligenza Artificiale emotiva", in realtà l'IA continua a rimanere semplicemente un algoritmo costituito da reti neurali, in grado di emulare i pensieri di un essere umano.

L'"intelligenza" del computer risulta essere assai lontana dalle capacità che un essere umano può mostrare. La definizione di "intelligenza umana", infatti, recita così:

*L'intelligenza è il complesso di facoltà psichiche e mentali che consentono all'uomo di pensare, comprendere o spiegare i fatti o le azioni, elaborare modelli astratti della realtà, intendere e farsi intendere dagli altri, giudicare, e lo rendono insieme capace di adattarsi a situazioni nuove e di modificare la situazione stessa quando questa presenta ostacoli all'adattamento.*

Seppur una Super IA, dalle capacità computazionali estremamente elevate, potrebbe essere prodotta in tempi neppure lontani, l'intelligenza umana si dimostra essere molto più abile nell'elaborare informazioni e nel trarre da queste considerazioni più complesse e originali. Invece, l'IA, nonostante presenti una capacità di analisi di gran lunga più veloce a quella umana, presenta ancora diversi limiti su numerosi campi, come è stato ampiamente dimostrato in questa tesi. La maggior parte dei suoi problemi hanno origine dal dataset con cui lo strumento è stato addestrato; infatti, esso deve essere ampio e, soprattutto, ricco di spunti estremamente diversificati, così da poter trarre analisi statistiche più accurate. Inoltre, un problema emergente risiede nella presenza nei dati di rappresentazioni stereotipate e non inclusive, fatto che contribuisce alla produzione di bias e discriminazioni, portando alla produzione di informazioni del tutto irrealistiche.

I bias sono un problema estremamente attuale in quanto impediscono al sistema di produrre risposte oggettive, riflettendo, invece, pregiudizi e opinioni sociali esistenti. Queste problematiche si infiltrano negli algoritmi in diversi modi; infatti, si possono ritrovare:

- *Bias preesistenti*: riguardano i preconcetti degli sviluppatori.
- *Bias tecnici*: si riferiscono ai limiti di design.
- *Bias di applicazione*: si verificano quando le applicazioni vengono impiegate in contesti non previsti.
- *Bias di incertezza*: si riferiscono al fatto che l'algoritmo favorisca campioni più grandi, ignorando popolazioni sotto-rappresentate.

Sono tantissimi gli esempi pratici riguardanti questi fatti. Uno dei più recenti e significativi risale al momento in cui a *Gemini*, il chatbot di Google, è stato chiesto di riprodurre figure pubbliche o storiche, come, ad esempio, i "filosofi greci". Invece di riprodurre risultati storicamente corretti o plausibili, l'IA ha prodotto immagini "politicamente corrette", rappresentando figure di etnie completamente errate, come uomini nativi americani.

Affrontare i bias nell'IA richiede un impegno continuo e una grande collaborazione da parte di esperti, programmatori e consumatori, che sono alla continua ricerca di soluzioni per poter risolvere questa problematica. Tra le metodologie più applicate si ricordano:

- La *Anonymization and Direct Calibration*: riguarda la rimozione di nomi e pronomi di genere nei documenti.
- L'*Adversarial Learning*: utilizza il Deep Learning per trovare distorsioni nei sistemi.
- Il *Data Cleaning*: riduce i comportamenti discriminatori nei dataset.

I sistemi ibridi, che combinano giudizio umano e Intelligenza Artificiale, sembrano essere, comunque, i più efficaci nel ridurre i pregiudizi. In questo caso, l'IA può portare rigore e ripetibilità, mentre gli esseri umani possono aggiungere consapevolezza e comprensione contestuale.

### 6.3.2 Umanità riflessa

Nella seconda stanza, la domanda centrale è stata:

*"Come rappresenteresti l'umanità?"*

In questa sezione l'Intelligenza Artificiale ha cercato di riprodurre un ritratto delle caratteristiche peculiari dell'essere umano, provando a dare forma alle emozioni che quest'ultimo prova, come l'amore.

In particolare, nell'opera intitolata "Le Mani della Creazione" (Figura 6.3), l'IA ha rappresentato l'unione e l'aspirazione umana. Infatti, le mani rivolte verso l'alto richiamano la continua ricerca di nuovo sapere da parte dell'essere umano, mentre il fuoco simboleggia l'ardore della conoscenza e richiama fortemente il mito di Prometeo, il titano che rubò il fuoco agli dei per essere poi condannato, diventando simbolo di ribellione e di amore verso l'umanità.



**Figura 6.3:** Le Mani della Creazione

Come si può notare, l'immagine presenta diversi errori nella riproduzione delle mani. Infatti, alcune di queste risultano essere deformi mentre altre presentano un numero di dita inferiore o superiore rispetto alla normalità. Questi difetti hanno nuovamente origine dall'analisi del dataset, che potrebbe risultare non efficiente.

Infatti, le motivazioni che possono portare, anche strumenti potenti, come ChatGPT-4 e DALL-E, a sbagliare le proprie considerazioni sono:

- *Input ambigui o non pertinenti*: se il dataset non contiene informazioni diversificate, l'algoritmo potrebbe trarre considerazioni statistiche errate e produrre risultati incoerenti.
- *Limiti del processo di training*: i set di dati potrebbero non ricoprire tutte le conoscenze che sono necessarie per poter generare un risultato corretto, portando l'IA a proporre una risposta del tutto fantasiosa.
- *Complessità del soggetto da rappresentare*: l'Intelligenza Artificiale potrebbe essere in difficoltà nel momento in cui il prompt in ingresso fornisce informazioni ambigue, che possono essere interpretate in modo differente.
- *Errori nell'algoritmo di generazione*: le reti neurali possono contenere errori o bias che influenzano il processo di generazione. Ad esempio, un algoritmo potrebbe favorire certi tipi di immagini rispetto ad altri, o potrebbe non essere in grado di gestire correttamente determinati tipi di input.

Infatti, nonostante molti modelli artificiali, come le General Adversarial Network e i Transformer, siano estremamente avanzati e validati, in realtà sono moltissimi gli errori presenti, spesso causati da problematiche sorte in fase di progettazione. Nonostante una delle cause principali, già parzialmente discusse, risieda nell'*Underfitting*, che si verifica quando i modelli non sono addestrati per un tempo adeguato o poiché le variabili in ingresso non sono abbastanza significative, molti altri errori sorgono quando viene svolto un *Overfitting*. Quest'ultimo si verifica quando un modello presenta un numero eccessivo di parametri rispetto alle osservazioni effettuate, causando la memorizzazione del rumore o di informazioni irrilevanti, perdendo la facoltà di generalizzare le analisi su un nuovo dataset. Questo fenomeno causa un basso tasso di errore nei dati di addestramento, mentre quelli di test evidenziano un tasso più alto.

Per evitare questo problema si possono adottare diverse tecniche, come:

- *L'arresto anticipato*: sospende il training del modello prima che questo inizi a memorizzare rumore aggiuntivo. Questo metodo può causare l'insorgere di underfitting qualora si fermi l'addestramento troppo presto.
- *L'aumento dei dati*: incrementa i dati rumorosi per stabilizzare il modello.
- *L'addestramento con più dati*: aumenta il dataset per eseguire il training e per migliorare l'accuratezza dell'algoritmo.
- *La selezione delle funzioni*: identifica e rimuove funzioni ridondanti o irrilevanti.
- *La regolarizzazione*: applica una "penalità" ai parametri con coefficienti maggiori per ridurre la varianza.
- *I metodi d'insieme*: integrano tecniche, come il *bagging* e il *boosting*, per combinare le previsioni di più algoritmi.

Il *bagging* è una tecnica utilizzata per ridurre la varianza in un set di dati rumoroso. In questo approccio viene selezionato un campione casuale di dati dal set di addestramento con sostituzione, il che significa che ogni data point può essere scelto più di una volta. Dopo aver generato diversi campioni, ciascuno di essi viene utilizzato per addestrare un modello indipendente. Successivamente, le previsioni dei vari modelli vengono combinate: a seconda del tipo di problema, si utilizza la media delle previsioni (per problemi di regressione) o

la maggioranza delle previsioni (per problemi di classificazione), producendo una stima complessiva più accurata.

Invece, il boosting è una tecnica di apprendimento d'insieme che combina "allievi deboli" per formare un "allievo forte", minimizzando gli errori di addestramento. Si addestra un modello iniziale su un campione di dati e, in modo sequenziale, i modelli successivi correggono gli errori dei precedenti. Ogni iterazione dà maggiore peso ai dati classificati erroneamente, migliorando la performance complessiva. Le previsioni dei modelli deboli vengono combinate per creare una regola di previsione forte, che offre prestazioni migliori rispetto ai singoli modelli.

### 6.3.3 Futuri possibili

Nell'ultima stanza della mostra, la domanda a cui rispondono le opere create è:

*"Come immagini i futuri possibili di coesistenza tra umani e Intelligenza Artificiale?"*

In questa fase l'IA ha illustrato i possibili modi di come il rapporto uomo-tecnologia si potrebbe sviluppare in futuro.

Una delle opere più significative è il "Quinto stato", quadro che è stato realizzato passando in ingresso al sistema il dipinto di Giuseppe Pellizza da Volpedo, noto come il "Quarto Stato" (Figura 6.4). Quest'ultimo rappresenta operai e contadini, i quali costituiscono il Quarto Stato, in protesta contro la borghesia (chiamata Terzo Stato) con l'obiettivo di ottenere maggiori diritti.

In questo caso, l'Intelligenza Artificiale diventa il Quinto Stato, formando un popolo fatto di robot e macchine, come si può evincere dalla Figura 6.5.



**Figura 6.4:** Quarto Stato



**Figura 6.5:** Quinto Stato

Come si può notare, l'opera creata rispecchia molto lo stile dell'originale, riuscendo ad integrare perfettamente le figure robotiche nel contesto. Infatti, sono numerosi gli esempi di opere d'arte rielaborate attraverso l'Intelligenza Artificiale, dalla "Monna Lisa" di Leonardo da Vinci alla "Notte Stellata" di Van Gogh, delle quali sono state proposte diverse versioni.

I risultati creati sono di ottima qualità e, a volte, risulta difficile distinguere i risultati prodotti da essere umani da quelli creati dal sistema digitale. Si apre, allora, la questione su come riconoscere le immagini create dall'IA, nonostante queste siano sempre più realistiche. Esistono diverse tecniche per poter identificare se un'immagine è stata creata da un'IA. Le

immagini generate, infatti, spesso presentano dettagli incoerenti. Ad esempio, nei ritratti, si possono osservare occhi asimmetrici, dita extra o mancanti, ombre irregolari o elementi di sfondo privi di logica. Queste incongruenze possono essere indicatori chiave della sinteticità dell'immagine. Inoltre, le immagini create con le Convolutional Neural Network possono mostrare pattern ripetitivi che appaiono innaturali o fuori luogo, specialmente nei dettagli complessi come foglie, capelli o superfici con particolari texture. Questi pattern anomali derivano dai processi di generazione utilizzati dall'IA. Inoltre, le immagini generate presentano artefatti digitali come bordi frastagliati, distorsioni geometriche o pixel disallineati. Questi artefatti sono particolarmente evidenti nelle aree di transizione tra colori o oggetti diversi, suggerendo una manipolazione artificiale. Anche i metadati associati a un file di un'immagine possono fornire importanti indizi sulla sua origine. Se questi ultimi indicano che l'immagine è stata creata con software di generazione di immagini, ciò può suggerire che il risultato è stato prodotto da un'IA.

Comunque sono disponibili strumenti e piattaforme online che utilizzano tecniche di Machine Learning per identificare immagini e per rilevare Deepfake. Le immagini create dall'IA possono mostrare schemi di compressione e frequenze anomale quando analizzate con strumenti specifici. Gli analizzatori di spettro di frequenza possono evidenziare differenze tra immagini naturali e sintetiche, rivelando la presenza di manipolazioni artificiali. Verificare la provenienza dell'immagine può fornire ulteriori indizi sulla sua autenticità; infatti, è fondamentale controllare le fonti e i siti web a cui ci si affida per valutare se il risultato trovato sia stato prodotto dall'IA.

Nonostante le tecniche sopra descritte, è fondamentale riconoscere che la distinzione tra le immagini reali e quelle generate dall'IA continua a diventare sempre più sfumata con l'avanzare della tecnologia. Pertanto, la combinazione di diversi metodi di analisi e un atteggiamento critico sono essenziali per identificare correttamente le immagini sintetiche. Utilizzare una molteplicità di approcci e di strumenti può migliorare significativamente la capacità di discernere l'autenticità delle immagini nel contesto dell'IA.

La generazione di arte attraverso l'Intelligenza Artificiale ha suscitato un notevole interesse negli ultimi anni, portando alla luce nuove opportunità creative, ma anche sollevando importanti questioni etiche e legali. Uno degli aspetti più complessi di questa innovazione è la questione della responsabilità e dell'*accountability* quando le opere d'arte generate dall'IA causano controversie. Alcuni incidenti specifici hanno messo in evidenza queste problematiche, come nel caso di "Edmond de Belamy", un'opera creata da un algoritmo sviluppato dal collettivo artistico Obvious, venduta all'asta per una cifra piuttosto corposa. Questo evento ha scatenato dibattiti sulla paternità e sulla proprietà intellettuale, evidenziando la necessità di ridefinire le leggi in questo campo. Un altro esempio, è l'uso di Deep Dream, un algoritmo di Deep Learning di Google che trasforma immagini esistenti in rappresentazioni surreali, sollevando preoccupazioni sulla proprietà delle immagini originali e sui diritti degli artisti. Le reazioni di questi ultimi a queste tecnologie sono state diverse: alcuni vedono l'IA come uno strumento innovativo, mentre altri la considerano una minaccia alla loro autenticità e originalità. Per affrontare queste preoccupazioni sono nate iniziative collaborative tra artisti e sviluppatori di IA, come il "Creative AI Lab", che cerca di stabilire linee guida etiche per un uso responsabile della tecnologia. La comunità legale, dal canto suo, sta esplorando modifiche legislative per affrontare le sfide poste dalla Generative AI. Le leggi sulla proprietà intellettuale, tradizionalmente concepite per riconoscere i diritti d'autore a individui o entità specifiche, devono essere adattate per includere opere create in collaborazione con algoritmi di IA. Alcuni paesi stanno studiando modifiche per riconoscere la paternità condivisa, mentre l'Organizzazione Mondiale della Proprietà Intellettuale (WIPO) ha avviato consultazioni globali per aggiornare le leggi in materia. Queste iniziative mirano a garantire la protezione dei diritti degli artisti, pur riconoscendo il contributo della tecnologia.



Per il futuro, è essenziale sviluppare linee guida etiche che orientino l'uso della Generative AI nell'arte, promuovendo la trasparenza nella creazione delle opere, rispettando i diritti degli artisti e prevenendo abusi. Inoltre, è fondamentale educare artisti, programmatori e il pubblico sulle potenzialità e i limiti della Generative AI, attraverso campagne di sensibilizzazione che promuovano una cultura di collaborazione e rispetto reciproco. Educare le nuove generazioni sull'importanza dell'etica nella tecnologia può contribuire a creare un futuro in cui l'IA e l'arte coesistano armoniosamente, valorizzando l'enorme potenziale della Generative AI.

## 6.4 Principi etici riguardo l'Intelligenza Artificiale

L'emergere delle tecniche generative nell'ambito della creazione di contenuti artistici ha sollevato diverse problematiche etiche e legali. La possibile violazione dei diritti di proprietà intellettuale delle opere esistenti e le questioni relative all'attribuzione dei diritti sulle creazioni generate dall'Intelligenza Artificiale sono questioni estremamente attuali, su cui molti stati stanno lavorando.

Negli ultimi decenni, l'Intelligenza Artificiale è emersa come una delle tecnologie più trasformative e promettenti dei tempi odierni. Le applicazioni dell'IA spaziano da assistenti virtuali a veicoli autonomi, oppure da sistemi diagnostici medici ad analisi dei dati su larga scala. Tuttavia, questo enorme potenziale comporta anche una significativa responsabilità. La crescente integrazione dell'IA nella vita quotidiana solleva importanti questioni etiche che devono essere affrontate per garantire che questa tecnologia serva il bene comune.

L'introduzione di principi etici è cruciale per guidare lo sviluppo, l'implementazione e l'uso delle tecnologie dell'IA in modo che rispettino i diritti umani, promuovano il benessere sociale e minimizzino i rischi. Questi principi etici sono diventati un tema centrale nei dibattiti globali, coinvolgendo governi, organizzazioni internazionali, aziende tecnologiche e la società civile. L'IA ha la capacità di elaborare informazioni e prendere decisioni in modi di gran lunga più rapidi rispetto alle capacità umane. Questo potenziale comporta dei rischi significativi, inclusi bias algoritmici, discriminazione, violazioni della privacy e l'uso improprio di dati. Senza una guida etica, l'IA potrebbe perpetuare ingiustizie esistenti o, addirittura, crearne di nuove.

### 6.4.1 Principi fondamentali

I principi etici forniscono un quadro di riferimento per affrontare queste preoccupazioni. Essi aiutano a garantire che l'IA sia sviluppata e utilizzata in modo che rispetti i valori democratici e i diritti fondamentali. Questo approccio è essenziale non solo per proteggere gli individui, ma anche per promuovere la fiducia pubblica nell'IA. Diversi organismi e istituzioni hanno proposto dei principi etici per l'IA; è interessante osservare che ci sono alcuni temi ricorrenti che emergono tra le varie proposte. Questi principi includono:

- *Trasparenza e interpretabilità*: la trasparenza si riferisce alla capacità di spiegare come funzionano i sistemi di IA e come prendono le decisioni. Gli algoritmi di IA devono essere comprensibili per gli utenti e gli stakeholder, permettendo loro di sapere quali dati vengono utilizzati e come vengono elaborati. L'interpretabilità è cruciale per garantire che le decisioni automatizzate possano essere controllate e validate da esseri umani, facilitando la responsabilità e la fiducia.
- *Equità e non discriminazione*: l'equità implica che i sistemi di IA non devono creare o perpetuare discriminazioni ingiustificate. Gli algoritmi devono essere progettati per minimizzare i bias e garantire che non discriminino in base a razza, genere, età, o altre caratteristiche protette. Ciò richiede un'attenzione continua durante tutto il

ciclo di vita del sistema di IA, dalla progettazione iniziale alla fase di monitoraggio post-implementazione.

- *Privacy e sicurezza*: la privacy dei dati è un principio fondamentale nell'etica dell'IA. Gli utenti devono avere il controllo sui loro dati personali, e i sistemi di IA devono implementare misure robuste per proteggere tali dati da accessi non autorizzati e violazioni. La sicurezza riguarda anche la protezione dei sistemi di IA stessi da attacchi e manipolazioni che potrebbero compromettere la loro integrità e affidabilità.
- *Responsabilità*: questa si riferisce alla necessità di attribuire chiaramente la responsabilità per le azioni e le decisioni prese dai sistemi di IA. Deve essere chiaro chi è responsabile per il comportamento di un sistema di IA, sia che si tratti di sviluppatori, di operatori o delle organizzazioni che lo utilizzano. Questo principio è essenziale per garantire che ci sia un meccanismo di rendicontazione e che le persone possano cercare giustizia in caso di danni o abusi.
- *Impatto sociali e ambientali*: i progettisti di IA devono considerare gli impatti sociali e ambientali delle loro tecnologie, cercando di massimizzare i benefici e minimizzare i rischi. Questo include la valutazione di come l'IA possa influenzare il benessere umano e la sostenibilità globale.

L'implementazione pratica dei principi etici nell'IA richiede un approccio multidisciplinare e collaborativo. Essa coinvolge non solo ingegneri e sviluppatori, ma anche esperti di etica, legali, sociologi e rappresentanti della società civile. Alcuni passi fondamentali includono:

- *Educazione e formazione*: è necessario formare sviluppatori e ingegneri sull'importanza dei principi etici e su come integrarli nel processo di sviluppo dell'IA.
- *Valutazioni di impatto etico*: è necessario condurre valutazioni di impatto etico durante lo sviluppo e l'implementazione dei sistemi di IA per identificare e mitigare potenziali rischi.
- *Regolamentazione e politiche*: è necessario stabilire normative e politiche che promuovano l'adozione dei principi etici e creino un quadro di responsabilità chiaro.
- *Collaborazione internazionale*: l'IA è una tecnologia globale, e la collaborazione tra paesi è essenziale per sviluppare standard etici internazionali e condividere le migliori pratiche.

L'Intelligenza Artificiale ha il potenziale di trasformare profondamente la società in modo positivo. Tuttavia, per realizzare questo potenziale, è fondamentale che l'IA sia sviluppata e utilizzata in modo etico. Questi principi forniscono una guida essenziale per garantire che l'IA contribuisca al bene comune, rispettando i diritti umani e promuovendo la giustizia sociale. Solo attraverso un impegno collettivo per l'etica si può garantire che l'IA serva realmente l'umanità e costruisca un futuro migliore per tutti.

#### 6.4.2 Tutela dei diritti intellettuali

Il 13 gennaio 2023 si è verificato un caso legale di rilevanza significativa che ha coinvolto Sarah Andersen, Kelly McKernan e Karla Ortiz, che hanno intentato una causa contro Stability AI Ltd., Midjourney Inc. e DeviantArt Inc., accusandole di essere "*strumenti di collage che violano i diritti di milioni di artisti*". Questi artisti hanno sostenuto che tali piattaforme abbiano utilizzato le loro opere senza autorizzazione o compensazione per alimentare il dataset di addestramento noto come LAION-Aesthetics. Inoltre, Andersen ha affermato che le immagini

generate, che imitavano il suo stile e quello di altri autori, hanno sminuito il valore delle loro opere, diluendole tra una moltitudine di immagini simili.

Contemporaneamente, Getty Images ha intrapreso azioni legali contro Stability AI, accusandola di violazione dei diritti d'autore e di proprietà dei marchi registrati, poiché ha identificato oltre 15.000 immagini della sua libreria all'interno del dataset di addestramento di Stable Diffusion.

Le tecniche generative, che creano dati sintetici a partire da dataset di addestramento, comportano che tutte le opere generate dall'IA derivino inevitabilmente da immagini preesistenti. Attualmente, non esiste una legislazione specifica che affronti in modo esaustivo la protezione dei diritti di proprietà intellettuale riguardo all'utilizzo di immagini esistenti per la creazione di nuovi contenuti multimediali tramite tecniche generative, sia a livello internazionale che nazionale. Di conseguenza, vi è spazio per interpretazioni diverse da parte dei tribunali.

In Italia, le opere d'arte generate con l'IA potrebbero essere considerate plagio ai sensi della legge sul diritto d'autore. Tuttavia, la questione è più complessa, poiché non è chiara la responsabilità in caso di plagio, che potrebbe essere attribuita all'utilizzatore del software, allo sviluppatore o a entrambi.

Un articolo pubblicato il 7 aprile 2023 su Harvard Business Review ha esaminato approfonditamente le implicazioni legali ed etiche della realizzazione di contenuti creativi tramite nuove tecnologie, suggerendo alcune linee guida e migliori pratiche per mitigare i rischi associati a tali attività.

Le leggi attuali in materia di proprietà intellettuale riconoscono i diritti d'autore alle opere create dall'essere umano. Tuttavia, con l'emergere dell'IA come creatrice di contenuti, sorge la domanda su chi detenga i diritti d'autore delle opere generate da tali sistemi.

È fondamentale distinguere tra opere generate autonomamente dall'IA e opere create con assistenza umana. Nel secondo caso, l'IA è uno strumento che richiede un contributo creativo umano, come la generazione di frasi di prompt; pertanto il diritto d'autore potrebbe spettare alla persona che ha guidato il processo creativo, sebbene sia necessario valutare attentamente i contributi individuali.

L'attribuzione dei diritti d'autore per le opere generate autonomamente dall'IA è più complessa, poiché le macchine non hanno personalità giuridica. Una possibile soluzione potrebbe essere l'assegnazione dei diritti d'autore e del diritto di sfruttamento economico al creatore del software o a chi ha finanziato la sua creazione.

Nel 2020, il Parlamento europeo ha introdotto una risoluzione volta a esaminare i diritti di proprietà intellettuale relativi allo sviluppo delle tecnologie associate all'Intelligenza Artificiale. L'obiettivo primario di questa iniziativa era salvaguardare l'innovazione, garantire la coerenza legale e incentivare la fiducia necessaria per favorire gli investimenti in queste nuove tecnologie.

Attualmente la titolarità dei diritti spetta esclusivamente alle entità giuridiche, in particolare al soggetto responsabile della creazione e della legittima pubblicazione dell'opera. Un requisito essenziale per l'assegnazione dei diritti è che l'opera soddisfi il criterio di originalità. Quest'ultimo non si applica solo al processo creativo, ma anche al risultato finale. Questo presupposto si basa sull'idea che le opere, sia tradizionali che generate dall'Intelligenza Artificiale, abbiano come scopo comune l'arricchimento del patrimonio culturale condiviso, nonostante le differenze nel processo creativo.

### 6.4.3 AI ACT

Il 21 aprile 2021 la Commissione europea ha presentato una proposta di regolamento (entrato in vigore nei primi mesi del 2024) che mira a unificare le normative sull'Intelligenza Artificiale. Questa iniziativa rappresenta il primo tentativo di creare una regolamentazione

trasversale volta a promuovere lo sviluppo e l'utilizzo di sistemi di IA affidabili nell'Unione Europea.

Gli obiettivi principali della proposta di legge sono i seguenti:

- assicurare che i sistemi di IA introdotti sul mercato dell'Unione siano sicuri e rispettino le normative già esistenti;
- garantire una chiara certezza del diritto per favorire gli investimenti e l'innovazione nell'IA;
- migliorare la governance e l'applicazione effettiva del diritto dell'Unione riguardante i diritti fondamentali e i requisiti di sicurezza applicabili ai sistemi di IA;
- favorire lo sviluppo di un mercato unico per applicazioni di IA legali, sicure e affidabili, evitando la frammentazione del mercato.

Il progetto di regolamento adotta un approccio basato sul rischio, adattando l'intervento legale al livello effettivo di rischio presentato dai sistemi di IA.

Per i sistemi che presentano un rischio limitato, tra cui i software che creano contenuti deepfake, sono previsti obblighi minimi di trasparenza. Infatti, il regolamento dice che:

*"Se un sistema di IA viene utilizzato per generare o manipolare immagini o contenuti audio o video che assomigliano notevolmente a contenuti autentici, dovrebbe essere previsto l'obbligo di rivelare che tali contenuti sono generati ricorrendo a mezzi automatizzati."*

A luglio 2021, il Parlamento Europeo ha pubblicato uno studio intitolato "*Addressing deepfakes in European policy*", che individua gli aspetti che i decisori politici potrebbero considerare per affrontare gli impatti negativi dei deepfake, già trattati al Capitolo 3. Secondo il documento, il quadro legislativo proposto dalla Commissione Europea offre un'opportunità per mitigare alcuni di questi rischi. Lo studio fornisce opzioni politiche che potrebbero essere integrate nell'Artificial Intelligence Act o nel Digital Services Act, il regolamento europeo per i servizi digitali progettato per contrastare la disinformazione.

Il 14 e 15 marzo 2024, durante la riunione G7 su Industria, Tecnologia e Digitale, la Presidenza italiana ha adottato una Dichiarazione Ministeriale che promuove lo sviluppo di un'IA etica e responsabile e un governo digitale sicuro e inclusivo. Questa dichiarazione enfatizza l'importanza dell'uso etico dell'IA nel settore pubblico, proteggendo privacy e diritti umani. La Presidenza italiana si impegna a integrare i risultati del Processo di Hiroshima sull'IA e a sviluppare un Toolkit sull'IA nel settore pubblico per garantire un uso etico delle applicazioni di IA.

*In questo capitolo verranno analizzati i risultati ottenuti dalle analisi eseguite nei capitoli precedenti, sia quelle derivanti dall'utilizzo degli strumenti di Amazon Web Services, sia quelle relative all'Intelligenza Artificiale Generativa. In particolare, la discussione si focalizzerà sull'attività di riconoscimento delle immagini, sulla traduzione dei testi e sull'applicazione dell'IA Generativa nel mondo dell'arte. Verranno esaminati i punti di forza, le sfide e le implicazioni etiche di queste tecnologie, con un'attenzione specifica al loro impatto e al loro potenziale futuro.*

## 7.1 Discussione sul riconoscimento di immagini

L'impiego dell'Intelligenza Artificiale nell'attività di riconoscimento di immagini ha portato con sé notevoli cambiamenti, rivoluzionando completamente il modo di elaborare i contenuti visivi. Questa tecnologia ha dimostrato di avere un notevole potenziale in diversi settori, grazie alla sua capacità di analizzare e interpretare visivamente un'ampia gamma di contenuti.

Nel settore sanitario, ad esempio, il riconoscimento delle immagini ha rivoluzionato la diagnostica medica, permettendo ai sistemi di IA di analizzare radiografie, risonanze magnetiche e tomografie computerizzate per individuare anomalie con maggiore precisione rispetto all'occhio umano. Questo può supportare i medici nella diagnosi e nel trattamento tempestivo dei pazienti, aumentando l'efficienza dei processi clinici. Invece, nel settore automobilistico, il riconoscimento delle immagini è essenziale per lo sviluppo di veicoli autonomi. Le auto a guida autonoma utilizzano sensori e telecamere dotate di IA per riconoscere segnali stradali, pedoni, altri veicoli e ostacoli, elaborando tali informazioni in tempo reale per prendere decisioni di guida sicure. Nelle Smart Cities, questa tecnologia è utilizzata per gestire il traffico, monitorare l'occupazione dei parcheggi e migliorare la sicurezza pubblica. Un'altra applicazione viene riscontrata nell'ambito del retail, in cui il servizio migliora l'esperienza del cliente e ottimizza le operazioni di marketing. I negozi possono analizzare il comportamento dei clienti per comprendere meglio le loro preferenze e le loro abitudini di acquisto, influenzando la disposizione dei prodotti e le promozioni personalizzate. Nel marketing digitale, le aziende possono valutare l'efficacia delle campagne, analizzando le reazioni dei consumatori ai contenuti pubblicitari.

In precedenza, è stato esaminato in maniera dettagliata il servizio Amazon Rekognition di Amazon Web Services, impiegato da numerose aziende per effettuare il riconoscimento di immagini. Amazon Rekognition utilizza algoritmi di Machine Learning per identificare oggetti, persone, testi e attività all'interno delle immagini e dei video. In particolare, nel corso

delle analisi effettuate in questa tesi, si è potuto osservare come il servizio sia estremamente preciso nella rilevazione dei volti e delle espressioni facciali, come nell'estrazione dei testi dalle immagini. Questi risultati evidenziano come AWS Rekognition possa essere utilizzato efficacemente in applicazioni di sicurezza e sorveglianza, dove è essenziale identificare individui o comportamenti sospetti in tempo reale. Inoltre, il sistema si è rivelato utile per migliorare l'accessibilità, fornendo descrizioni accurate delle immagini per le persone con disabilità visive, nonché nel settore industriale, dove l'analisi delle immagini può fornire preziose informazioni sulle demografie e le preferenze dei consumatori.

I case study affrontati mediante l'ausilio di AWS Rekognition rappresentano un'area di grande potenziale e di grande innovazione, ma richiedono, comunque, un approccio critico e responsabile. La qualità delle immagini è un fattore cruciale per il successo del riconoscimento; contenuti di bassa risoluzione o condizioni di illuminazione sfavorevoli possono ridurre drasticamente la precisione del sistema. Si prenda in considerazione l'esempio riguardante i CAPTCHA passati in input al servizio di rilevamento testuale di AWS Rekognition. Qui il sistema non riesce nemmeno a rilevare la presenza di lettere o frasi in quanto il font testuale è non lineare e poco uniforme. La stessa cosa accade quando il soggetto non è ben definito. Si prenda in considerazione la Figura 4.3 data in ingresso al servizio di rilevamento delle etichette; il sistema non riesce a rilevare le figure effettivamente rappresentate, ma riconosce, ad esempio, degli animali come avvoltoi e canguri con una elevata percentuale.

Un'altra sfida importante è il bias algoritmico. I dati di addestramento possono riflettere pregiudizi, portando a risultati inaccurati o ingiusti, specialmente quando si tratta di riconoscere volti di diverse etnie o gruppi demografici. Questo problema può avere gravi conseguenze, soprattutto in determinati contesti, come quello della sicurezza.

## 7.2 Discussione sulla traduzione dei testi

La traduzione automatica dei testi è uno degli ambiti in cui l'Intelligenza Artificiale ha mostrato più progressi significativi negli ultimi anni. Grazie agli avanzamenti nel campo del Machine Learning e del Deep Learning, questi sistemi sono diventati strumenti potenti e accessibili, capaci di facilitare la comunicazione globale e l'accesso a informazioni in diverse lingue. Tra i vari strumenti disponibili, Amazon Translate si distingue per la sua efficacia e versatilità. Infatti, grazie alla sua capacità di elaborare grandi volumi di testo in tempo reale, AWS Translate è utilizzato in diversi settori, come l'assistenza clienti e l'editoria. Ad esempio, le piattaforme di e-commerce possono utilizzarlo per tradurre descrizioni di prodotti, recensioni dei clienti e contenuti di marketing, rendendo più agevole l'accesso a mercati globali. Nell'assistenza dei clienti, la traduzione automatica permette di offrire supporto multilingue, migliorando l'esperienza degli utenti e aumentando la soddisfazione del cliente.

AWS Translate, oltre ad offrire un'elevata scalabilità alle aziende che lo utilizzano, garantisce traduzioni molto accurate, che vengono continuamente aggiornate per poter migliorare i risultati.

Nonostante i notevoli progressi, la traduzione automatica, eseguita con l'Intelligenza Artificiale, presenta alcune limitazioni. Per avere un confronto sui risultati ottenuti, è stato impiegato anche un altro strumento, ovvero DeepL, servizio di traduzione automatica molto utilizzato dalle aziende per la sua precisione ed efficacia, anche in presenza di testi particolarmente difficili.

Una delle principali sfide riscontrate è la traduzione di testi complessi, in cui sono presenti termini difficili ed espressioni idiomatiche o culturali specifiche. Come si è visto nelle analisi del Capitolo 5, quando viene dato in ingresso un input testuale in cui è presente una metrica

particolare o termini desueti, il sistema compie diversi errori, senza rispettare la natura e l'essenza del testo.

In alcuni casi, infatti, può essere necessario l'intervento umano per la revisione e l'editing delle traduzioni per garantire l'accuratezza e la naturalezza del testo tradotto.

Si deve, comunque, rilevare che la traduzione fornita da DeepL sia più precisa e accurata rispetto a quella prodotta da AWS Translate, il quale tende a offrire un risultato molto letterale, con diversi errori nel momento in cui si presentano termini desueti o specifici.

### 7.3 Discussione sulla IA Generativa

L'Intelligenza Artificiale Generativa ha aperto nuovi orizzonti in diversi ambiti, da quello finanziario a quello automobilistico. Infatti, grazie all'implementazione di reti neurali particolarmente avanzate, l'IA Generativa è in grado di creare nuovi contenuti, come immagini e testi, a partire da quelli del dataset di addestramento.

In particolare, questa nuova tecnologia è impiegata nella creazione di nuovi contenuti visivi. Infatti, mediante l'utilizzo di strumenti avanzati come ChatGPT4 e DALL-E, è possibile creare delle opere originali che sfidano i confini della creatività umana. Inoltre, come si è potuto evincere dalle analisi effettuate sulle opere della mostra "01-IO: il punto di vista dell'Intelligenza Artificiale attraverso la sua arte", le immagini prodotte sono di altissima qualità e assolutamente originali.

Anche se sono state utilizzate tecnologie molto avanzate, le immagini risultanti presentano degli errori significativi, come, ad esempio, nel quadro "Le Mani della Creazione", in cui alcune mani sono deformi e altre presentano un numero di dita inferiore o superiori rispetto alla normalità.

Questi errori possono presentare origini diverse. Alcuni di questi possono originarsi a causa dei bias presenti nel dataset, i quali riflettono pregiudizi e opinioni sociali esistenti. Ciò può condurre alla produzione di output che presentano informazioni del tutto inopportune. Un altro motivo di errore può essere causato dalla presenza di errori negli algoritmi, che non riescono a processare il dataset in maniera efficace. Come si può notare, molte di queste cause derivano dalla scorretta costruzione del dataset. Infatti, è molto importante che le informazioni vengano raccolte ed elaborate in maniera accurata e opportuna, per consentire una corretta analisi. Uno dei problemi più rilevanti riguarda la quantità di dati raccolti. Inoltre, se questi sono insufficienti si può verificare l'underfitting, producendo un vuoto nelle informazioni da processare; in caso contrario, si verifica l'overfitting, il quale può causare l'aggiunta di rumore indesiderato sul risultato prodotto.

Nonostante le enormi potenzialità, l'utilizzo dell'IA Generativa nella creazione di immagini solleva importanti questioni etiche, proprio a causa degli errori che può produrre. Una delle principali preoccupazioni riguarda la proprietà intellettuale. Le immagini generate dall'IA sono spesso basate su grandi dataset che includono opere d'arte e fotografie esistenti, sollevando il problema della paternità e dei diritti d'autore.

Un'altra questione etica cruciale riguarda il potenziale uso improprio delle immagini generate dall'IA. La capacità di creare immagini su richiesta può essere sfruttata per produrre deepfake, immagini false o ingannevoli che possono essere utilizzate per diffondere disinformazione, manipolare opinioni pubbliche o compromettere la reputazione di individui. Questo rischio richiede un'attenta regolamentazione e la creazione di strumenti di verifica dell'autenticità delle immagini.

Infatti, per garantire la sicurezza dei cittadini e per far sì che questa nuova tecnologia venga utilizzata in modo corretto, diverse organizzazioni internazionali hanno introdotto numerose leggi che regolamentano questo nuovo mondo legato all'IA Generativa.

Nel corso di questa tesi è stata condotta un'analisi approfondita sull'Intelligenza Artificiale e sulle sue implicazioni in vari settori. Inizialmente, è stata esplorata la natura dell'IA, partendo dalla sua definizione, passando attraverso il Test di Turing e fornendo una prima distinzione tra Intelligenza Artificiale debole e forte. È stata, poi, tracciata la storia dell'IA, dai primi cenni sulla nascita della disciplina, passando per i primi successi per arrivare fino ai primi fallimenti. È stata, inoltre, esaminata l'evoluzione delle tecnologie di Machine Learning e Deep Learning, con un focus particolare sulle reti neurali artificiali, le quali sono alla base del funzionamento dell'Intelligenza Artificiale. Sono state, poi, trattate le principali applicazioni pratiche dell'IA in vari ambiti, come la Data Science e la robotica.

Successivamente, è stato introdotto Amazon Web Services, il principale strumento impiegato nelle analisi svolte in questa tesi, evidenziando la storia e l'evoluzione della piattaforma, i principali servizi offerti e il ruolo di AWS nella collaborazione industriale. Un'analisi dettagliata dell'infrastruttura ha evidenziato la presenza di diverse tipologie di Cloud Computing proposte da AWS e l'impatto che questo servizio ha nell'ambito dell'IA, con un'attenzione particolare alle reti neurali e alle soluzioni implementative impiegate.

La tesi ha dedicato una sezione all'Intelligenza Artificiale Generativa, illustrando la sua storia e le sue applicazioni principali. Sono stati esaminati modelli come i Variational AutoEncoder, le Generative Adversarial Network, i Transformer e i Diffusion model, oltre a discutere le principali sfide digitali riscontrate, come quella dei deepfake.

Le analisi svolte in questa tesi si sono concentrate sull'attività di riconoscimento di immagini, mediante l'utilizzo di Amazon Rekognition, e sulla traduzione automatica, grazie all'impiego di Amazon Translate e DeepL. Grazie alle analisi svolte, è stato possibile comprendere le potenzialità e i limiti dell'IA. Infine, è stato approfondito il rapporto che vi è tra il mondo dell'arte e l'IA Generativa, esaminando ulteriormente i limiti e le implicazioni etiche e legali dell'IA.

I futuri sviluppi dell'Intelligenza Artificiale promettono di ridefinire profondamente la società, toccando aspetti fondamentali della vita quotidiana. L'integrazione sempre più avanzata dell'IA nei processi decisionali e operativi renderà i sistemi più autonomi e capaci di apprendere e adattarsi in modo dinamico a contesti mutevoli.

Una delle direzioni più promettenti è il miglioramento delle capacità di apprendimento non supervisionato e di trasferimento, che permetterà alle IA di apprendere da una quantità di dati limitata e di applicare le conoscenze acquisite da un contesto a nuovi domini, riducendo la necessità di costosi processi di training. Questa evoluzione aprirà la strada a un utilizzo più diffuso dell'IA in situazioni reali e complesse, come la gestione delle emergenze e la pianificazione strategica. Inoltre, si prevede un significativo progresso nell'interazione



uomo-macchina, grazie allo sviluppo di interfacce sempre più intuitive. Tecnologie come il riconoscimento vocale e facciale, la realtà aumentata e virtuale, e i sistemi di dialogo avanzati renderanno l'interazione con le macchine più fluida e accessibile, consentendo a un pubblico più ampio di sfruttare i benefici dell'IA senza barriere tecniche.

Tuttavia, questi sviluppi richiedono una gestione etica e regolatoria accurata. La crescente autonomia delle IA solleva questioni cruciali riguardo alla responsabilità, alla trasparenza e alla protezione dei dati. Sarà fondamentale sviluppare normative che garantiscano l'uso sicuro ed equo delle tecnologie IA, prevenendo abusi e discriminazioni.

Gli sviluppi futuri dell'Intelligenza Artificiale rappresentano una straordinaria opportunità per migliorare molteplici aspetti della nostra esistenza, ma necessitano di un approccio responsabile e olistico per assicurare che i benefici siano equamente distribuiti e che le sfide etiche e sociali vengano affrontate in modo opportuno.

- ALIGHIERI, D. (1982), *La Divina Commedia, Vol. I, Inferno*, La Nuova Italia Editrice, Firenze.
- ANTONIOU, A., STORKEY, A. e EDWARDS, H. (2017), «Data augmentation generative adversarial networks», *arXiv preprint arXiv:1711.04340*.
- BANK, D., KOENIGSTEIN, N. e GIRYES, R. (2023), «Autoencoders», *Machine learning for data science handbook: data mining and knowledge discovery handbook*, p. 353–374.
- BATTIATO, S., GIUDICE, O. e PARATORE, A. (2016), «Multimedia forensics: discovering the history of multimedia contents», in «Proceedings of the 17th International Conference on Computer Systems and Technologies 2016», p. 5–16.
- BRADEŠKO, L. e MLADENIĆ, D. (2012), «A survey of chatbot systems through a loebner prize competition», in «Proceedings of Slovenian language technologies society eighth conference of language technologies», vol. 2, p. 34–37, sn.
- CELLAN-JONES, R. (2014), «Stephen Hawking warns artificial intelligence could end mankind», *BBC news*, vol. 2 (10), p. 2014.
- DUBEY, S. R. e SINGH, S. K. (2023), «Transformer-based generative adversarial networks in computer vision: A comprehensive survey», *arXiv preprint arXiv:2302.08641*.
- FAIRCLOUGH, H. R., BROWN, S. L. e OTHERS (1914), *Virgil's Aeneid*, BH Sanborn.
- FEUERRIEGEL, S., HARTMANN, J., JANIESCH, C. e ZSCHECH, P. (2024), «Generative ai», *Business & Information Systems Engineering*, vol. 66 (1), p. 111–126.
- GHOSHAL, A. (2023), «Amazon Q, la respuesta de AWS a Copilot de Microsoft.», *Computerworld Spain*, p. NA–NA.
- GOODFELLOW, I., BENGIO, Y. e COURVILLE, A. (2016), *Deep learning*, MIT press.
- GOODFELLOW, I., POUGET-ABADIE, J., MIRZA, M., XU, B., WARDE-FARLEY, D., OZAIR, S., COURVILLE, A. e BENGIO, Y. (2014), «Generative adversarial nets», *Advances in neural information processing systems*, vol. 27.
- GREWAL, D. S. (2014), «A critical conceptual analysis of definitions of artificial intelligence as applicable to computer engineering», *IOSR Journal of Computer Engineering*, vol. 16 (2), p. 9–13.

- HOCHREITER, S. e SCHMIDHUBER, J. (1997), «Long Short-Term Memory», *Neural Computation*, vol. 9 (8), p. 1735–1780.
- KEWATE, N., RAUT, A., DUBEKAR, M., RAUT, Y. e PATIL, A. (2022), «A review on AWS-cloud computing technology», *International Journal for Research in Applied Science and Engineering Technology*, vol. 10 (1), p. 258–263.
- MATHEW, S. e VARIA, J. (2014), «Overview of amazon web services», *Amazon Whitepapers*, vol. 105 (1), p. 22.
- MURTHY, C. V. N. U. B., SHRI, M. L., KADRY, S. e LIM, S. (2020), «Blockchain Based Cloud Computing: Architecture and Research Challenges», *IEEE Access*, vol. 8, p. 205 190–205 205.
- ONESTI, R. C. (2014), *Eneide*, Einaudi.
- PERMISSION, S. (2005), «Generative and discriminative classifiers: Naive bayes and logistic regression», .
- RADFORD, A., METZ, L. e CHINTALA, S. (2015), «Unsupervised representation learning with deep convolutional generative adversarial networks», *arXiv preprint arXiv:1511.06434*.
- RUSSELL, S. J. e NORVIG, P. (2021), *Artificial intelligence: a modern approach*, Pearson.
- SEARLE, J. R. (1980), «Minds, brains, and programs», *Behavioral and brain sciences*.
- SINHA, P. (2020), «Cloud computing using AWS: an analysis», .
- TAN, Z., WANG, S., YANG, Z., CHEN, G., HUANG, X., SUN, M. e LIU, Y. (2020), «Neural machine translation: A review of methods, resources, and tools», *AI Open*, vol. 1, p. 5–21.
- TURING, A. M. (2009), *Computing machinery and intelligence*, Springer.
- WESTERLUND, M. (2019), «The emergence of deepfake technology: A review», *Technology innovation management review*, vol. 9 (11).
- YANG, L., ZHANG, Z., SONG, Y., HONG, S., XU, R., ZHAO, Y., ZHANG, W., CUI, B. e YANG, M.-H. (2023), «Diffusion models: A comprehensive survey of methods and applications», *ACM Computing Surveys*, vol. 56 (4), p. 1–39.
- ZHONG, G., GAO, W., LIU, Y., YANG, Y., WANG, D.-H. e HUANG, K. (2020), «Generative adversarial networks with decoder–encoder output noises», *Neural Networks*, vol. 127, p. 19–28.

- Amazon Web Services — [www.aws.amazon.com](http://www.aws.amazon.com)
- DeepL — [www.deepl.com](http://www.deepl.com)
- LinkedIn — [www.linkedin.com](http://www.linkedin.com)
- IBM — [www.ibm.com](http://www.ibm.com)
- MathWorks — [www.mathworks.com](http://www.mathworks.com)
- Microsoft — [www.microsoft.com](http://www.microsoft.com)
- Oracle — [www.oracle.com](http://www.oracle.com)
- OpenAI — [www.openai.com](http://www.openai.com)
- Osservatori Digital Innovation — [www.osservatori.net](http://www.osservatori.net)
- Parlamento Europeo — [www.europarl.europa.eu](http://www.europarl.europa.eu)
- Treccani — [www.treccani.it](http://www.treccani.it)

---

## Ringraziamenti

---

Ringrazio il professore *Domenico Ursino*, che con grande disponibilità mi ha accompagnato nell'elaborazione di questa tesi, trasmettendomi la sua professionalità e il suo entusiasmo verso il mondo dell'ingegneria.

Ringrazio *Loris*, il mio ragazzo, che ha creduto sempre in me e che, con il suo amore, mi ha supportata nei momenti più difficili e ha gioito con me in quelli più felici, dandomi una forza incredibile.

Ringrazio i miei compagni di studio *Angelo* e *Leonardo*, che sono stati compagni formidabili di viaggio, di scleri e di risate, durante le lunghe giornate in università.

Ringrazio *Elena*, tanto più di una semplice amica, ma la sorella che avrei voluto avere. Grazie per essermi stata vicina in tutti questi anni, per le lunghe chiacchierate, per le risate e per avermi compresa.

Ringrazio i miei amici pendolari, che durante i lunghi momenti trascorsi in treno insieme hanno reso più leggere le mie giornate con il loro supporto e le loro risate.

Ringrazio tutti coloro che mi hanno affiancata in questa avventura tra Fano e Ancona, arricchendo il mio percorso. Grazie per avermi permesso di vivere delle esperienze così preziose.

Infine, questa tesi è dedicata alla mia famiglia. A mia madre *Loretta* che è stata la mia roccia in questo viaggio, dandomi sempre fiducia anche nei momenti più difficili. Grazie per il tuo coraggio e per i tuoi sacrifici. A mia nonna *Maria*, che con la sua forza, intraprendenza e genialità, è stata una seconda mamma e una migliore amica in questi anni. A mio padre *Francesco*, il mio angelo custode, che dall'alto mi dà tutti i giorni il coraggio per credere nei miei sogni.