UNIMORE Dipartimento di Economia Marco Biagi
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Fondazione Marco Biagi

Intelligenza Artificiale e protezione dei dati personali

Avv. Chiara Ciccia Romito
Dottoranda di ricerca Lavoro, Sviluppo e Innovazione

I punti che vedremo

1. Cos'è l'Intelligenza Artificiale?
2. Le Strategie delle Istituzioni
3. Funzionamento e rischi dell'I.A.
4. Le norme del GDPR e l'I.A.

1

Cos’è l’Intelligenza Artificiale?

Definizione

L’I.A. è una scienza e un insieme di tecnologie informatiche che si ispirano - ma in genere operano in modo molto diverso - al modo in cui le persone usano il loro sistema nervoso e il loro corpo per percepire, imparare, ragionare e agire.

S.J. RUSSEL, P. NORVIG, Artificial Intelligence: A Modern Approach

Definizione

La definizione dovrebbe essere basata sulle principali caratteristiche funzionali del software, in particolare sulla capacità, per una determinata serie di obiettivi definiti dall'uomo, di generare output quali contenuti, previsioni, raccomandazioni o decisioni che influenzano l'ambiente con cui il sistema interagisce, tanto in una dimensione fisica quanto in una dimensione digitale.

PROPOSTA DI REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE STABILISCE REGOLE ARMONIZZATE SULL'INTELLIGENZA ARTIFICIALE (LEGGE SULL'INTELLIGENZA ARTIFICIALE) E MODIFICA ALCUNI ATTI LEGISLATIVI DELL'UNIONE.

Commissione europea

Quello che dicono i media

CORRIERE DELLA SERA

CORRIERE INNOVAZIONE / NEWS

INTELLIGENZA ARTIFICIALE

Intelligenza artificiale (tra rischi e opportunità): i 4 pericoli per l'uomo

Discriminazione, invasione della privacy, propaganda politica, armi autonome. Ecco i pericoli che corre l'umanità, mentre sviluppa applicazioni basate sull'intelligenza artificiale

Avvenire.it

Home · Economia · Lavoro Bes | Lavoro | Motori | Risparmio | Svilup

Il dibattito. L'intelligenza artificiale sostituirà completamente il lavoro umano?

L'arma dell'intelligenza artificiale per ridurre sprechi e liste d'attesa

Il Sole 24 ORE Italia Mondo Economia Finanza Mercati Risparmio Norme & Tributi Al

Interventi

L'Intelligenza Artificiale rivoluzionerà l'apprendimento nel prossimo decennio?

Quello che non vediamo

Quello che vediamo

2

Le Strategie delle Istituzioni

Cosa ci dicono le Istituzioni?

- L'Europa può combinare i suoi punti di forza industriali e tecnologici con **un'infrastruttura digitale di elevata qualità** e un quadro normativo basato sui suoi valori fondamentali per diventare un **leader mondiale nell'innovazione nell'economia dei dati e nelle sue applicazioni.**

- L'Europa dovrebbe sfruttare i propri punti di forza per far crescere la propria posizione negli ecosistemi e lungo la catena del valore, da determinati settori della produzione di hardware al software e ai servizi.

Libro Bianco della Commissione Europea Sull'Intelligenza Artificiale

La Strategia europea

- **Mobilitare risorse per conseguire un «ecosistema di eccellenza»** lungo l'intera catena del valore, a cominciare dalla ricerca e dall'innovazione, e creare i giusti incentivi per accelerare l'adozione di soluzioni basate sull'IA, **anche da parte delle piccole e medie imprese (PMI)**;

- Creazione di un **«ecosistema di fiducia»** unico. A tal fine, deve garantire il rispetto delle norme dell'UE, comprese le norme a tutela dei diritti fondamentali e dei diritti dei consumatori, in particolare per i sistemi di IA ad alto rischio gestiti nell'UE.

La Strategia italiana

- Un potenziale enorme che necessita di direzione
- Il Gruppo di esperti è convinto che la strategia italiana debba avere una visione antropocentrica:

1. L' A.I. deve essere in linea con la legislazione esistente;
2. Incentivare forme di A.I. che aumentano l'intelligenza, la produttività e la creatività umana, anziché sostituirle, investendo sull'educazione;
3. Che si provveda ad introdurre forme di responsabilità civile per alcune tipi di applicazioni includendo sempre l'intervento umano;

Funzionamento e rischi dell’I.A.

Come funziona l’Intelligenza artificiale:

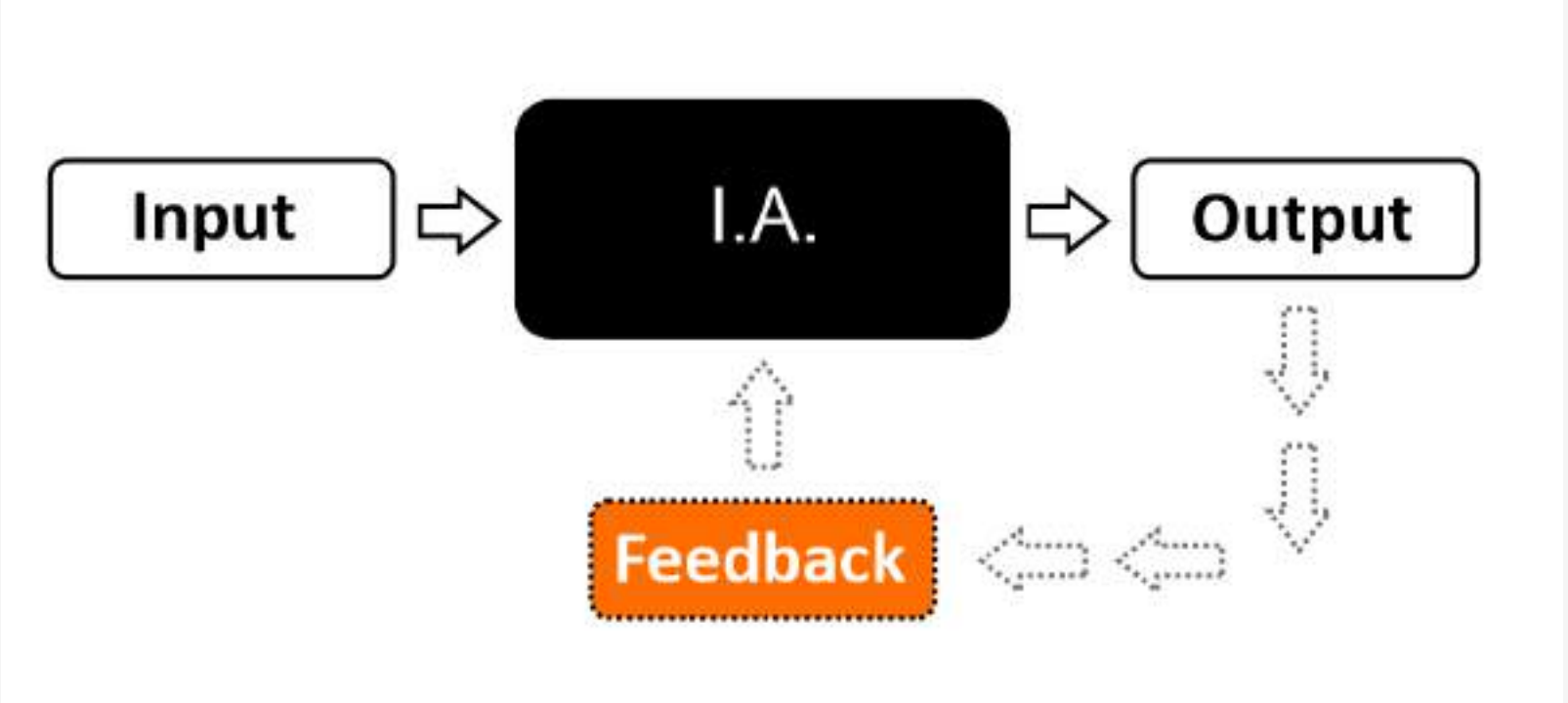
Esempio

1 - Input

2 - Rete neurale

3 - Output

4 - Feedback



Machine Learning e Deep Learning

Machine Learning

- È un processo di apprendimento automatico che permette il riconoscimento di modelli dopo un addestramento basato su campioni

Deep Learning

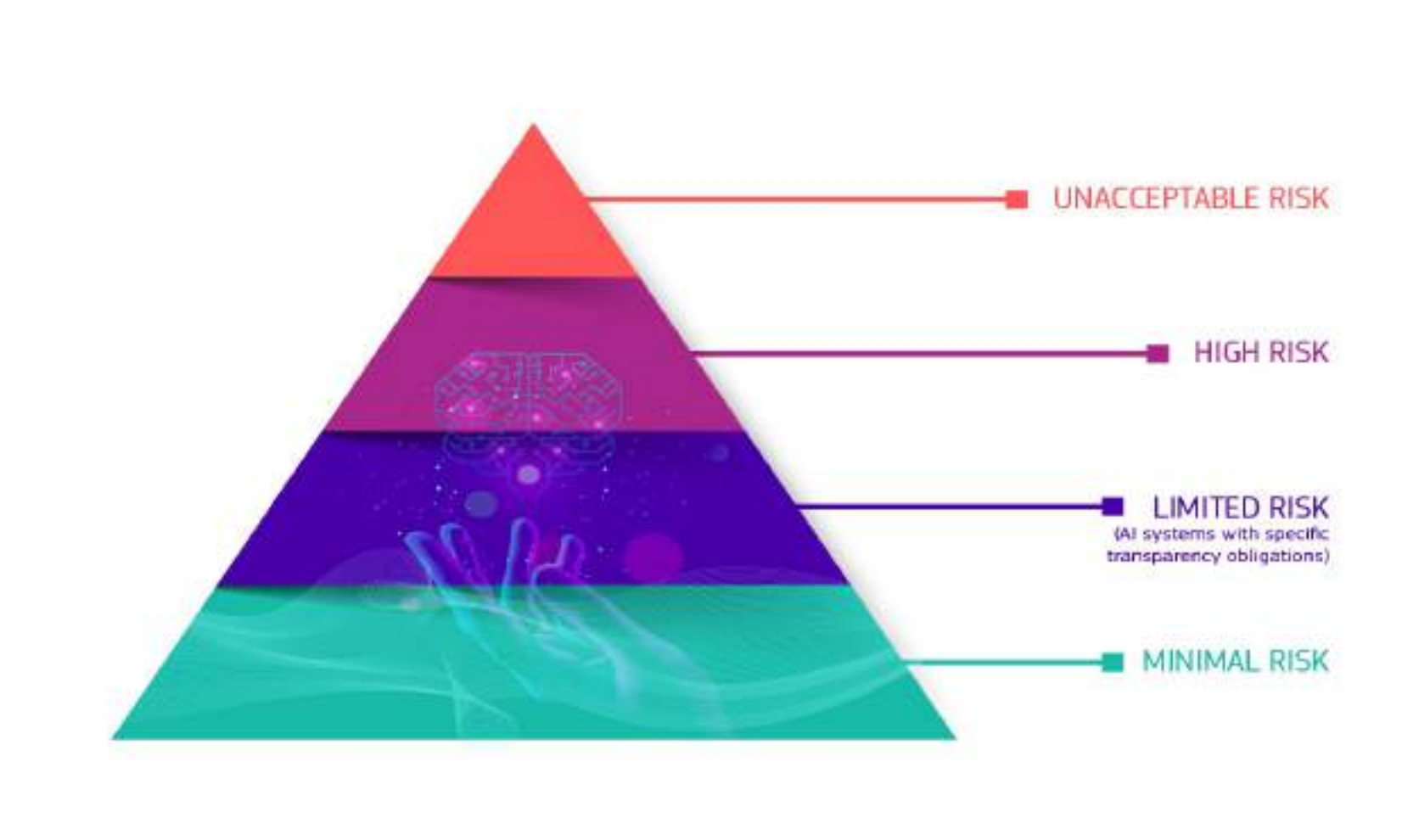
- È un insieme di tecniche basate su rete neurali artificiali organizzate in diversi strati, dove ogni strato calcola i valori su quello successivo affinché l'informazione venga elaborata in maniera sempre più completa.

Proposta di regolamentazione europea

La Commissione propone nuove norme per garantire che i sistemi di IA utilizzati nell'UE siano sicuri, trasparenti, etici, imparziali e sotto il controllo umano.

1. Uso dell'I.A. solo negli ambiti in cui il suo utilizzo può comportare un miglioramento;
2. vietare l'uso non controllato che potrebbe danneggiare gli individui;
3. Rispetto dei diritti fondamentali della dignità umana
4. Garantire l'autodeterminazione dell'individuo

Approccio basato sul rischio



I rischi dell'I.A

1. Primo gruppo si annoverano i rischi legati a finalità illecite contrarie all'ordinamento
2. Nel secondo gruppo rientrano quelli di discriminazione e di bias
3. Rischi legati alla sicurezza informatica
4. Black boxes - ad. es. TESLA

Rischi specifici nel mondo del lavoro

L’avvento dell’IA e l’utilizzo di tecniche c.d. di machine learning che elaborano decisioni sulla base dei dati raccolti potrebbero determinare un rischio non solo per l’imprevedibilità delle conseguenze, ma anche dal punto di vista della sorveglianza e della profilazione del lavoratore.

Il rischio riguarda anche l'imprenditore

- Da un punto di vista legale non potrebbero avere accesso, ad esempio, ai codici algoritmici, utili a gestire le proprie risorse aziendali, di cui però non sono proprietari e che hanno soltanto in uso.
-
- Dal punto di vista tecnico, invece, gli imprenditori al pari dei lavoratori potrebbero non conoscere la chiave per aprire la scatola nera di algoritmi troppo intelligenti che possono risultare indecifrabili.

Una questione etica

1. Intervento e sorveglianza umana
2. Robustezza tecnica e sicurezza
3. Riservatezza e Governance dei dati
4. Trasparenza
5. Diversità, non discriminazione ed equità
6. Benessere sociale e ambientale
7. Accountability

L’esigenza di formazione

1. Preparare i nuovi talenti
2. Investire sul personale aziendale già presente
3. Una formazione specifica per l’impresa al fine di comprendere come funziona l’A.I., le opportunità e i rischi.

Le norme del GDPR e l'I.A.

Analisi delle norme più significative

Il principio di esattezza e aggiornamento

Art. 5 GDPR

Il raccordo tra valutazione della correttezza e della qualità dei dati, e le finalità perseguite è essenziale perché non è possibile sapere se un dato che si intende utilizzare sia corretto, aggiornato o esatto senza conoscere per quale scopi lo si vuole utilizzare.

Nell'ambito dell'I.A. questo principio assurge ad elemento fondamentale per impedire alla macchina di usare dati sbagliati che portano ad output sbagliati.

La macchina si nutre di dati ha bisogno di dati di qualità

La classificazione delle esigenze di raccolta del dato è il primo passo da muovere.

Per consentire all'intelligenza artificiale di realizzare le sue premesse occorre promuovere un'**ecologia dei dati** ossia stabilire norme che indichino chiaramente quali dati possono essere trattati, con quali finalità e per quanto tempo.

Il principio di minimizzazione

I dati devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità perseguite.

Meno dati si utilizzano, meno rischi corre l'interessato.

Se i dati sono «minimizzati» il titolare ha chiare le finalità che tende a raggiungere tramite il trattamento e quali sono i dati indispensabili a tal fine.

Privacy by design

Privacy by design è un «concetto aperto» destinato ad essere attivato in maniera dinamica man mano che le tecnologie si svilupperanno.

La conferma arriva dal Considerando 78 il quale sottolinea che il Titolare deve «assicurare trasparenza per quanto riguarda le funzioni e il trattamento dei dati, consentire all'interessato di controllare il trattamento e creare e migliorare le misure di sicurezza».

Un sistema sicuro di intelligenza artificiale

Se i processi sono automatizzati la mera connessione ad una rete rappresenta potenzialmente un rischio per le imprese, e conseguentemente, per i dati di cui la stessa è titolare.

Non a caso, **ENISA** è intervenuta di recente con un corposo documento relativo alla cybersecurity nei sistemi di Intelligenza Artificiale.

Il rapporto di ENISA ha analizzato le maggiori minacce per l'IA attraverso una classificazione dettagliata dei maggiori rischi e nel contesto delle diverse fasi del ciclo di vita dell'IA.

Il quadro dovrà essere aggiornato al passo con l'evoluzione tecnologica.

Art. 88 GDPR

L’art. 88 riconosce agli Stati membri la facoltà di dettare norme più specifiche a tutela della dignità dei lavoratori.

Art. 22 GDPR

Processo decisionale automatizzato relativo alle persone fisiche (compresa la profilazione)

1.L’interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Elementi fondamentali dei processi decisionali automatizzati

Gli elementi chiave sono due:

a. Il trattamento automatizzato
b. La successiva decisione sia basata unicamente su di esso

L'art. 22 par. 1 vieta quindi l'adozione di decisioni prese senza il coinvolgimento di un essere umano che possa influenzare e modificare la sua autorità o competenza.

Cosa si intende per profilazione?

Secondo il WP251 la raccolta di informazioni su un individuo o un gruppo di individui per analizzare le caratteristiche al fine di inserirli in categorie, gruppi o poterne fare delle valutazioni o delle previsioni.

La profilazione si compone di tre elementi:

1. Trattamento deve essere automatizzato
2. Condotto su dati personali
3. Deve conseguire l'obiettivo di valutare il comportamento della persona

Condizioni

Ai fini dell'applicazione è necessario che la decisione basata unicamente sul trattamento automatizzato di dati personali, produca effetti sulla sfera giuridica dell'interessato o incida in modo analogo significativamente sulla sua persona.

Effetti giuridici

Un'attività o un'elaborazione che abbia impatto sui diritti legali dell'individuo (come ad esempio, la libertà di associarsi, di votare, o intraprendere un'azione legale)

Effetti analoghi a quelli giuridici

Quando la decisione che coinvolge un individuo non influisca sui diritti, ma influisca sui suoi interessi (esempio diniego di richiesta di finanziamento)

Eccezioni

- Contratto

- Obbligo di legge

- Consenso dell'interessato

Esclusione dei dati particolari dai processi decisionali automatizzati.

Risulta significativo come il Legislatore abbia escluso da tali processi i dati particolari dell'interessato di cui all'art. 9 GDPR se non in presenza del **consenso esplicito** dell'interessato o **per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione** o degli Stati membri che tuttavia deve essere ai sensi dell'art. 9 par 2 lett. g) proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dati e prevedere misure appropriate e specifiche per tutelare i diritti degli interessati.

Simili ipotesi, non sono riconducibili al rapporto di lavoro.

Adozione di misure appropriate

Nell'ipotesi di deroga dell'art. 22 par 2) lett. a) e c) il GDPR richiede un livello minimo di tutela all'interessato che consiste nel diritto **di ottenere l'intervento umano da parte del titolare del trattamento**, e di esprimere la propria opinione o contestare la decisione.

Il Considerando 71 integra i predetti diritti con quello di ottenere una **specifica spiegazione della decisione conseguita.**

Informativa rafforzata

Per esercitare il diritto in parola, si presuppone che l'interessato abbia la piena conoscenza dei trattamenti.

L'informativa è importante tanto nella parte relativa all'art. 13, par.2 lett.f (l'esistenza di un processo decisionale automatizzato, compresa la profilazione, di cui all'art. 22 par. 2,) *informazioni aggiuntive sulla logica utilizzata,* quanto in sede di accesso par. 1 lett. h) art. 15.

Diritto alla leggibilità?

- Il Regolamento impone al titolare del trattamento di fornire **informazioni significative sulla logica utilizzata**, ma non necessariamente una spiegazione complessa degli algoritmi utilizzati o la divulgazione dell'algoritmo completo.

- L'interessato è in grado di comprendere la logica utilizzata nel processo decisionale automatizzato?

Ulteriori problematiche

ART. 4 ST. LAV. CO 3

Informazione sull'utilizzo dello strumento e sulle modalità di controllo

TUTELA DEL LAVORATORE E DELL'IMPRESA

Le RSA riescono a comprendere le esigenze di tutela?

Per concludere: Cosa serve?

RAFFORZAMENTO DELLE TUTELE

Occorrerà chiarire se il principio di trasparenza possa essere esercitato come diritto alla leggibilità dell'algoritmo.

Ed in ogni caso, aumento delle tutele dei lavoratori.

Centralità delle procedure e policy.

GOVERNANCE DEI DATI

Corretto governo dei dati

INCLUSIVITÀ

Lavoratori e PMI

Necessario equilibrio tra le nuove garanzie e i nuovi adempimenti da parte delle imprese che rischiano di essere appesantite.

Fattore di disincentivazione agli investimenti.

Per salutarvi

Se il concetto di competenza è destinato a cambiare, solo la capacità di adattamento, di creatività e di organizzazione consentiranno di rispondere alle nuove esigenze del mercato.

Avv. Chiara Ciccia Romito

chiara.cicciaromito@unimore.it