UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI DIRITTO PUBBLICO ITALIANO E SOVRANAZIONALE

PoliS Lombardia | Regione Lombardia

AI NEWS

Newsletter sull'Intelligenza Artificiale
a cura di PoliS-Lombardia

Anno I – n. 6/2024

In questo numero

Quello che state leggendo è un **numero speciale di AI News**: la prima parte è **dedicata per intero all'AI Act**, il regolamento europeo che entrerà in vigore nei prossimi mesi. Per iniziare a renderci conto delle prospettive che

apre e dell'impatto che avrà anche nel settore pubblico, abbiamo chiesto al professor **Marco Bassini**, che insegna Fundamental Rights and Artificial Intelligence all'università di Tilburg (Paesi Bassi), di tracciare una **sintesi ragionata del documento**. Segue una "pillola" formativa sull'**addestramento degli algoritmi**. Poi, la consueta rassegna di best practice applicate alla Pubblica amministrazione. E una panoramica di notizie, commenti, segnalazioni di incontri, pubblicazioni… Buona lettura!

IN EVIDENZA

Speciale AI Act: Così il Regolamento cambierà l'uso dell'AI (non solo) in Europa

a cura di Marco Bassini, docente di diritti fondamentali e intelligenza artificiale, Tilburg University

Come noto, lo scorso 13 marzo il Parlamento europeo ha approvato il regolamento dell'Unione europea che definisce norme armonizzate sull'intelligenza artificiale, il cosiddetto "AI Act". Il voto è arrivato dopo un percorso in salita, che ha visto susseguirsi proposte diverse maturate nel contesto di un dibattito assai partecipato, non soltanto a livello delle istituzioni europee. Un fattore di complicazione che ha influenzato l'iter legislativo- iniziato nel 2021 con la proposta di regolamento formulata dalla Commissione- è certamente legato alla rapidissima evoluzione tecnologica che si è registrata nel corso degli ultimi mesi, ben rappresentata dall'avvento su larga scala di sistemi di Intelligenza artificiale con capacità generative. Queste innovazioni testimoniano l'elevato rischio di obsolescenza cui è esposto ogni tentativo di regolamentazione e riflettono la complessità del compito affidato al legislatore europeo. Il regolamento conoscerà ora alcuni raffinamenti linguistici nelle diverse versioni, prima della sua pubblicazione sulla Gazzetta Ufficiale e della successiva entrata in vigore.
Tra le grandi potenze tecnologiche, l'Ue è la prima a dotarsi di un quadro normativo sulla materia. In letteratura si è discusso **se questo disegno condurrà, come auspicato, a un effettivo rafforzamento della certezza giuridica e della tutela dei diritti**, così da promuovere l'innovazione tecnologica, **oppure a un rischio (anche geopolitico) di isolamento dell'Unione europea**, in ragione della provenienza perlopiù extraeuropea dei principali attori di mercato. Solo l'esperienza applicativa potrà confermare se l'Unione europea sarà riuscita nei suoi intenti, ma un punto di partenza di una tale analisi non potrà che essere la **natura di compromesso dell'accordo**, che **concilia le istanze di innovazione con la tutela dei diritti fondamentali**.
In quanto regolamento, l'atto approvato nei giorni scorsi **avrà efficacia generale** e sarà direttamente **applicabile in tutti gli Stati** membri. Non occorrerà, pertanto, un recepimento formale da parte degli ordinamenti nazionali, sebbene questi ultimi dovranno disciplinare alcuni ambiti particolari di competenza statale per espressa previsione del regolamento.

La definizione e il campo di applicazione

L'AI Act fornisce, anzitutto, una **definizione di sistema di AI**: si tratta di un sistema **automatizzato** progettato per funzionare con **livelli di autonomia variabili** e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare **output quali previsioni, contenuti, raccomandazioni o decisioni** che possono influenzare ambienti fisici o virtuali. Ciò che distingue i sistemi di intelligenza artificiale dai sistemi software o dagli approcci di programmazione tradizionali è la loro **capacità inferenziale**: non si tratta di sistemi basati su regole definite unicamente da persone fisiche, bensì di sistemi che possono fondare la propria capacità di inferenza su tecniche diverse (come gli approcci di apprendimento automatico e gli approcci basati sulla logica e sulla conoscenza).
L'ambito di applicazione del regolamento include varie categorie di soggetti, tra cui in particolare i fornitori (*provider*) e gli utilizzatori (*deployer*) di sistemi di AI, ma anche gli importatori e i distributori. Sotto il profilo territoriale, l'AI Act si applica ai fornitori che immettono sul mercato sistemi di intelligenza artificiale nell'Unione,

a prescindere dal loro luogo di stabilimento, e agli utilizzatori stabiliti nell'Ue o anche situati in Paese terzo (nel caso l'output prodotto dai sistemi sia utilizzato nell'Unione).

L'approccio fondato sul rischio: le pratiche vietate

La disciplina dettata dal regolamento è conforme all'approccio fondato sul rischio, comune ad altri atti normativi dell'Unione europea, tra cui il regolamento generale sulla protezione dei dati personali (GDPR) e il *Digital Services Act*. Tale regime prevede **l'individuazione di varie categorie di rischio** alle quali sono ascrivibili i sistemi di AI e che comportano l'applicazione di regole progressivamente più restrittive all'incremento del livello di rischio. L'AI Act definisce, in particolare, quattro tipologie di rischio: rischio **inaccettabile**, rischio **elevato**, rischio **limitato**, rischio **minimo**.

Per quanto riguarda i sistemi che pongono **un rischio inaccettabile**, l'AI Act ne vieta l'immissione sul mercato, la messa in servizio o l'uso. Tali pratiche comprendono:

- **l'utilizzo di tecniche subliminali o volutamente manipolative o ingannevoli**, aventi lo scopo o l'effetto di distorcere il comportamento di una persona o di un gruppo di persone, pregiudicando in modo considerevole la capacità di adottare una decisione informata;
- **i sistemi che sfruttano le vulnerabilità** di una persona o di un gruppo di persone in ragione dell'età, della disabilità o della situazione socioeconomica, al fine di distorcere il comportamento in modo da provocare un danno significativo;
- **la valutazione o la classificazione delle persone** fisiche o di gruppi di persone **sulla base del loro comportamento sociale** o di caratteristiche personali o della personalità note, inferite o previste, in cui il punteggio sociale così ottenuto comporti un trattamento pregiudizievole o sfavorevole in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti e/o un trattamento pregiudizievole o sfavorevole che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità;
- **la valutazione del rischio relativo a persone fisiche per valutare o prevedere la probabilità di commissione di un reato**, unicamente sulla base della profilazione o della valutazione dei tratti e delle caratteristiche della personalità, con l'eccezione dei sistemi utilizzati a sostegno di valutazioni umane del coinvolgimento di una persona in attività criminose, basato su fatti oggettivi e verificabili;
- **la creazione o l'ampliamento di banche dati di riconoscimento facciale mediante *scraping*** non mirato di immagini facciali da internet o da filmati di telecamere a circuito chiuso;
- **il riconoscimento degli stati emotivi di una persona** fisica nell'ambito del luogo di lavoro e degli istituti di istruzione, salvo ricorrano motivi medici o di sicurezza;
- **la categorizzazione biometrica per la classificazione individuale di persone** fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale;
- **l'identificazione biometrica remota "in tempo reale" in spazi accessibili al pubblico a fini di attività di polizia.** Tale ultimo divieto non opera in tre fattispecie: a) la ricerca mirata di specifiche vittime di rapimento, tratta o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; b) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche, o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; c) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per una serie di reati specifici, punibili nello Stato membro interessato con una pena o una misura privativa della libertà della durata massima di almeno quattro anni.

L'approccio fondato sul rischio: i sistemi di intelligenza artificiale ad alto rischio

Il livello di rischio immediatamente successivo è quello cui appartengono i sistemi **ad alto rischio**, che sono destinatari della maggior parte delle disposizioni stabilite dall'AI Act.

La qualificazione di sistemi di AI come sistemi a rischio elevato può dipendere da due circostanze: nel primo caso, il fatto che il sistema sia **destinato a essere utilizzato come componente di sicurezza di un prodotto** ovvero costituisca esso stesso un prodotto disciplinato dalla normativa europea di armonizzazione elencata in un

apposito allegato (allegato I), ai sensi della quale il prodotto è soggetto a una valutazione di conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio; nel secondo caso, la collocazione di un sistema in un **apposito elenco** formato all'interno dell'allegato III.
L'allegato III dell'AI Act individua per ciascuno settore "critico" una serie di sistemi qualificati come ad alto rischio, ossia:

- **biometria** (laddove consentita): sistemi di identificazione biometrica remota (con l'esclusione dei sistemi per la verifica biometrica la cui unica finalità è confermare che una determinata persona fisica è la persona che dice di essere); sistemi per la categorizzazione biometrica in base ad attributi o caratteristiche sensibili protetti basati sulla deduzione di tali attributi o caratteristiche; sistemi destinati a essere utilizzati per il riconoscimento delle emozioni;
- **infrastrutture critiche**: sistemi destinati a essere utilizzati come componenti di sicurezza nella gestione e nel funzionamento delle infrastrutture digitali critiche, del traffico stradale o nella fornitura di acqua, gas, riscaldamento o elettricità;
- **istruzione e formazione professionale:** sistemi per determinare l'accesso, l'ammissione o
- l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli; sistemi per valutare i risultati dell'apprendimento; sistemi per valutare il livello di istruzione adeguato che una persona riceverà o a cui potrà accedere; sistemi per monitorare e rilevare comportamenti vietati degli studenti durante le prove;
- **occupazione, gestione dei lavoratori e accesso al lavoro autonomo**: sistemi per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati; sistemi per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro;
- **accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione**
- **degli stessi:** sistemi utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria; sistemi per valutare l'affidabilità creditizia delle persone fisiche o per stabilire il loro merito di credito; sistemi per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie; sistemi per valutare e classificare le chiamate di emergenza o per stabilire priorità in merito all'invio di polizia, vigili del fuoco e assistenza medica;
- **attività di polizia**: sistemi per determinare il rischio per una persona fisica di diventare vittima di reati; poligrafi e strumenti analoghi; sistemi per valutare l'affidabilità degli elementi probatori nel corso delle indagini o del perseguimento di reati; sistemi per determinare il rischio di reato o recidiva in relazione a una persona fisica; sistemi per effettuare la profilazione delle persone fisiche nel corso dell'indagine, dell'accertamento e del perseguimento di reati;
- **migrazione, asilo e gestione del controllo delle frontiere**: poligrafi e strumenti analoghi; sistemi per valutare un rischio posto da una persona fisica che intende entrare o è entrata nel territorio di uno Stato membro; sistemi per assistere le autorità pubbliche competenti nell'esame delle domande di asilo, di visto o di permesso di soggiorno; sistemi per individuare, riconoscere o identificare persone fisiche, a eccezione della verifica dei documenti di viaggio;
- **amministrazione della giustizia e processi democratici**: sistemi per assistere un'autorità giudiziaria nella ricerca e nell'interpretazione dei fatti; sistemi utilizzati per influenzare l'esito di un'elezione o di un referendum o il comportamento di voto delle persone.

La qualificazione dei sistemi elencati nell'allegato III quali ad alto rischio è però meramente presuntiva, in quanto l'AI Act riconosce la possibilità di derogare a tale status qualora l'utilizzo in concreto del sistema considerato non presenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali.
In relazione ai sistemi ad alto rischio, l'AI Act individua una serie di requisiti, che comprendono:

- la definizione di un **sistema di gestione del rischio** per tutto il ciclo di vita del sistema;

- la definizione di una **governance dei dati** volta ad assicurare che i dataset utilizzati per l'addestramento, la convalida e il test di sistemi ad alto rischio siano pertinenti, sufficientemente rappresentativi e, per quanto possibile, privi di errori e completi;
- la redazione di una **documentazione tecnica** idonea a dimostrare la conformità prima dell'immissione nel mercato o della messa in servizio;
- la conservazione delle registrazioni degli eventi rilevanti ("log");
- la fornitura di **informazioni e istruzioni d'uso** agli utilizzatori per consentire a questi ultimi di utilizzare adeguatamente un sistema;
- la progettazione e lo sviluppo dei sistemi ad alto rischio in modo da consentire la **supervisione umana** nella fase di utilizzo;
- la progettazione e lo sviluppo dei sistemi ad alto rischio in modo da garantire un adeguato livello di **precisione, robustezza e sicurezza informatica.**

Sono inoltre previsti degli obblighi per i fornitori di sistemi ad altro rischio, che al ricorrere di alcune condizioni si applicano altresì agli utilizzatori (*deployer*). I fornitori devono, ad esempio, garantire che i loro sistemi di IA ad alto rischio siano **conformi ai requisiti previsti dall'AI Act**, mettere in atto un **sistema di gestione della qualità**, conservare la **documentazione tecnica** di cui è richiesta la redazione e via dicendo.
Infine, il regolamento stabilisce l'obbligo di condurre una **valutazione di impatto sui diritti fondamentali** come requisito preliminare all'utilizzo di alcuni sistemi ad alto rischio. Tale obbligo fa capo agli utilizzatori (*deployer*) che sono organismi di diritto pubblico o enti privati che forniscono servizi pubblici, nonché agli utilizzatori di sistemi ad alto rischio particolari. La valutazione di impatto dovrà svolgersi in occasione del primo uso del sistema e dovrà comprendere una serie di elementi (descrizione dei processi di utilizzo; periodo e frequenza di utilizzo; categorie di persone fisiche e gruppi interessati dal suo uso; rischi specifici di danno; misure di sorveglianza umana; misure da adottare in caso di concretizzazione dei rischi).

L'approccio fondato sul rischio: i sistemi a rischio limitato

Da ultimo, il regolamento dedica ai sistemi di intelligenza artificiale che presentano rischio limitato la previsione di **meri obblighi di trasparenza**. Si stabilisce, in particolare, che i sistemi destinati a interagire direttamente con le persone fisiche siano progettati e sviluppati in modo che queste ultime, ove interessate, siano informate del fatto di interagire con un sistema di AI. Tale obbligo non si applica ai sistemi autorizzati per legge per accertare, prevenire, indagare o perseguire reati, a meno che non siano a disposizione del pubblico per segnalare un reato.
Un **obbligo di trasparenza particolare si impone poi ai sistemi di AI generativa**, i quali devono garantire che i rispettivi output siano marcati in un formato leggibile e rilevabili come generati o manipolati artificialmente. Inoltre, gli utilizzatori di sistemi che generano o manipolano immagini o contenuti audio o video che costituiscono un "*deep fake*" nonché di sistemi che generano o manipolano testo pubblicato allo scopo di informare il pubblico devono **rendere noto che il contenuto è stato generato o manipolato artificialmente**.
Regole specifiche sono poi dettate per i sistemi di intelligenza artificiale c.d. "*general purpose*".

Governance

L'AI Act si occupa anche della *governance* dell'intelligenza artificiale*,* declinata sia a livello europeo che a livello nazionale. A livello europeo, l'AI Act istituisce sia un **AI Office**, con compiti promozionali, sia un **Comitato europeo per l'intelligenza artificiale**, con compiti di coordinamento e armonizzazione. A livello nazionale, invece, ciascuno Stato membro dovrà istituire o designare come **autorità nazionali competenti** almeno un'autorità di notifica e almeno un'autorità di vigilanza del mercato.

Sanzioni

Infine, l'AI Act individua le sanzioni applicabili, modulate sulla base della tipologia di violazioni. La violazione del divieto di pratiche vietate è assoggettata a **sanzioni amministrative pecuniarie fino a 35 milioni di euro**, o, se l'autore del reato è un'impresa, **fino al 7% del fatturato mondiale**, se superiore. La violazione degli obblighi e requisiti inerenti ai sistemi a rischio elevato può comportare l'applicazione di sanzioni amministrative pecuniarie fino a 15 milioni di euro o, se l'autore del reato è un'impresa, fino al 3% del fatturato. Infine, la fornitura di informazioni inesatte, incomplete o fuorvianti agli organismi notificati o alle autorità nazionali competenti è

soggetta a sanzioni amministrative pecuniarie fino a 7,5 milioni di euro o, se l'autore del reato è un'impresa, fino all'1% del fatturato.

Entrata in vigore

L'entrata in vigore dell'AI Act avverrà secondo una logica scalare, in cui le disposizioni troveranno applicazione nei 24 mesi successivi, salvo che per alcune previsioni per le quali sono definite soglie diverse, rispettivamente di 6 mesi (quanto alle pratiche vietate), 12 mesi (i sistemi *general purpose*) e 36 mesi (per i sistemi ad alto rischio, che richiedono un adeguamento più complesso).

Per consultare il testo nell'ultima versione disponibile, clicca qui

Per consultare la pagina dedicata della Commissione europea

Normativa

Stati Uniti

Vermont: Bill for Data Privacy Act passes Legislature
12 maggio 2024

Applicazioni alla Pubblica amministrazione

ITALIA

Intelligenza artificiale e robotica

Casi di studio utilizzati al fine di agevolare la collaborazione tra enti pubblici, aziende, atenei e organizzazioni non governative, in vista degli obiettivi dell'Agenda 2030
Robotica e IA per gli obiettivi di sviluppo sostenibile: esempi e casi di studio- Agenda Digitale

***

Med-Gemini: l'IA di Google per la Sanità

I modelli come Med-Gemini potrebbero aprire nuove frontiere nel campo della medicina, offrendo strumenti avanzati per potenziare la ricerca e supportare il settore
Med-Gemini: l'IA di Google per la Sanità promette meraviglie | Agenda Digitale

UNIONE EUROPEA

ESCO

Un'iniziativa della Commissione Europea che mira a standardizzare la classificazione delle abilità, competenze, qualifiche e occupazioni attraverso l'Ue.
Esco: cos'è e a cosa serve la classificazione di abilità e occupazioni dell'UE | Agenda Digitale

MONDO

Cina / L'AI nella Pubblica amministrazione e la responsabilità dei dipendenti pubblici

Uno dei settori dove l'intelligenza artificiale può sortire decisivi risultati di efficienza e di qualità dell'output, secondo lo studio cinese, sono i servizi pubblici. Poiché non sono esposti alla concorrenza, la

***

Trasformazione digitale della Pubblica amministrazione

L'information management suite di Opentext
Trasformazione digitale della PA, come migliora i servizi ai cittadini (agendadigitale.eu)

***

PA e Open innovation

Due nuovi strumenti usati dalle Camere di Commercio: l'Internal Process Automation, per riconfigurare le procedure meno fluide, e l'Intelligent Data Analysis & Management, con cui, grazie all'impiego dell'AI, vengono sviluppate le potenzialità del patrimonio informativo gestito dalle Camere di commercio.
PA: come sfruttare bene l'open innovation | Agenda digitale

responsabilità e motivazione dei lavoratori è il principale stimolo alla qualità delle prestazioni.
AI technology applicatin and employee responsibility | Humanities and Social Sciences Communications (nature.com)

AI in pillole

AI training: ovvero, come ti alleno l'algoritmo

Che cos'è l'AI training?

L'AI training (addestramento dell'intelligenza artificiale) consiste nell'insegnare all'AI a comprendere gli input degli utenti e a prendere decisioni basate su di essi. Senza la fase di addestramento, l'AI non sarebbe in grado di operare in quanto non saprebbe come interpretare i dati che le vengono sottoposti.
Due numeri fa *(cfr AI News n. 4)* abbiamo parlato della **distinzione tra Machine Learning e Deep Learning.** Il primo (il cosiddetto "apprendimento automatico") permette al sistema di apprendere **autonomamente attraverso l'esperienza, senza che sia stato specificamente programmato.** Questo sistema si avvale di statistiche per delineare un modello all'interno di una grande quantità di dati, costituiti da numeri, parole, immagini o qualsiasi altra cosa possa essere archiviata digitalmente. L'addestramento di un sistema di Machine Learning consiste quindi nella sua **esposizione a una grande quantità di dati**, che lo aiuteranno a identificare pattern con una maggiore "sicurezza" e a fornire output sempre più accurati. Il Deep Learning ("l'apprendimento profondo") è una sottocategoria di Machine Learning. Si tratta di un tipo di sistemi che cerca di **imitare la struttura base e il funzionamento del cervello umano attraverso la creazione di reti neurali artificiali (artificial neural networks).** In questo secondo caso, **la fase di apprendimento è svolta interamente dalla rete neurale cui vengono sottoposti i dati di interesse.** Questa procederà all'estrazione delle caratteristiche e classificherà gli input, dando a ogni dato un peso differente e facendo passare le informazioni al livello neurale successivo. Se la rilevanza associata a un dato risultasse a posteriori male attribuita, il sistema tornerà indietro ad aggiornarla per determinare output appropriati.

Quali sono i dati su cui viene addestrata l'AI?

L'addestramento di un modello di IA è il processo mediante il quale il modello "impara" da un insieme di dati, detto "**dataset**". Questo insieme è diviso generalmente in due sottoinsiemi: uno per l'addestramento e uno per il test.

Il modello utilizza il **dataset di addestramento** per fare previsioni e migliorare le proprie prestazioni attraverso un processo iterativo. Durante questo processo un algoritmo di ottimizzazione cerca di minimizzare la differenza tra le previsioni del modello e i dati reali, la cosiddetta "funzione di perdita". Questa funzione aiuta il modello a cercare, tra le possibili soluzioni, quella più efficiente.

Il **dataset di test** viene invece utilizzato per valutare le prestazioni del modello in un contesto "sconosciuto", cioè con dati che non sono stati utilizzati durante l'apprendimento, permettendo di verificare quanto il modello sia in grado di generalizzare ciò che ha appreso a nuovi dati, fornendo un'indicazione di come potrebbe comportarsi in un ambiente reale.

Da chi viene addestrata l'AI?

È necessario che il training della AI sia basato su un dataset completo e – almeno tendenzialmente – privo di bias, ovvero di "pregiudizi" che potrebbero minarne il funzionamento. È qui che operano i cosiddetti **AI trainer**, professionisti che si occupano di insegnare all'intelligenza artificiale a interpretare le informazioni fornitele e ad agire di conseguenza.

I compiti svolti dagli AI trainer possono essere raggruppati in:

- Sintetizzazione di dati grezzi e non filtrati per la **creazione di dataset** ben organizzati e privi di bias;
- **Annotazione** meticolosa **dei dati** secondo precise linee guida, verifica e validazione delle annotazioni ed eventuale ri-annotazione dei dati qualora l'AI non dovesse leggerli correttamente;
- **Addestramento dei sistemi** di AI attraverso l'utilizzo di training dataset d'esempio al fine di verificare che l'output sia corretto.

Una volta creato un programma di intelligenza artificiale apparentemente funzionante, **l'addestratore di AI continua comunque a testare i sistemi per assicurarsi che operino efficientemente, con una costante** supervisione dei programmi, necessaria per verificare che non commettano errori.

Qui di seguito alcuni materiali di approfondimento:

Come vengono addestrati i modelli di Intelligenza Artificiale | esa-automation.com
Cosa è l'apprendimento supervisionato? | IBM

Dati per addestrare i robot: il nuovo oro del settore | Agenda Digitale
The robot race is fueling a fight for training data | MIT Technology Review

Gli AI trainer e l'addestramento dell'intelligenza artificiale | AI news
Le differenze tra machine learning e deep learning | AI news

Notizie

E. Mullin, *Cina, i chip cerebrali per "potenziare" gli esseri umani* | Wired Italia, 13 maggio 2024

C. Galletti, *Come riconoscere i video fatti con intelligenza artificiale? Su TikTok arrivano le etichette «AI-generated»* I Corriere della Sera, 11 maggio 2024

E. Frasso, *Francia e Cina insieme per ridurre i rischi dell'intelligenza artificiale* I AI news, 7 maggio 2024

A.D. Signorelli, *Leggere la mente: la nuova frontiera delle big tech* | Wired Italia, 6 maggio 2024

G. Vergine, *L'IA accelera anche in Italia: ecco le startup più promettenti* I Agenda Digitale, 6 maggio 2024

Redazione ANSA, *L'Ucraina avrà una portavoce generata dall'intelligenza artificiale* I Ansa, 3 maggio 2024

A.Patella, *Intelligenza artificiale, un nuovo modello italiano | Wired Italia*, 29 aprile 2024

Commenti

R. Forsi, *PA digitale, tornare indietro è impossibile: i piani* I Agenda Digitale, 13 maggio 2024

A. Corrado, *Intelligenza artificiale, regole e cautele* I Corriere della Sera, 12 maggio 2024

I. Trovato, *L'AI non è un rischio per i posti di lavoro Ma serve formazione* I Corriere della Sera, 12 maggio 2024

D. Conforti, *Formazione e scuola, così l'AI gen aiuta HR manager e insegnanti* I Agenda Digitale, 10 maggio 2024

F. Sanna, *Intelligenza artificiale e copyright: l'infinito braccio di ferro* | Wired Italia, 10 maggio 2024

F. Del Castillo – A. Tironi, *Elogio all'interoperabilità nella PA: dieci consigli per migliorarla* I Agenda Digitale, 6 maggio 2024

Intelligenza artificiale: i limiti, i controlli biometrici e le multe introdotte dalle nuove regole europee I Ansa, 3 maggio 2024

Fra sentenze e ricorsi, l'IA che aiuta i magistrati I Ansa, 2 maggio 2024

E. Frasso, *L'AI è uno dei presupposti per iniziare di nuovo a pensare di essere umani*, intervista a Matteo Ciastellardi | AI Talks #10- AI news

M. Corradino, *Intelligenza artificiale e pubblica amministrazione: sfide concrete e prospettive future* I Diritto Amministrativo | Ildirittoamministrativo.it, maggio 2024

Corsi, convegni e pubblicazioni

Corsi

Master in intelligenza artificiale per la pubblica amministrazione ! Polimi Gsom

Eventi e convegni

Intelligenza artificiale e professione forense: le novità introdotte dall'AI Act | Unione Forense per la tutela dei diritti umani e Ordine degli Avvocati di Lecco

L'opportunità dell'intelligenza artificiale per gli enti locali, 22 maggio 2024 | Acb – associazione comuni bresciani

L'intelligenza artificiale negli appalti pubblici | Omologhia

I corsi per trasformare la Pubblica amministrazione attraverso l'intelligenza artificiale | Unige.life

La cura ai tempi delle nuove tecnologie e dell'intelligenza artificiale. La sfida dell'ipercomplessità, 30-31 maggio 2024 | Ordine Regionale dei Chimici e dei Fisici della Toscana

Forum PA 2024: a maggio l'evento sull'innovazione dell'AI nella pubblica amministrazione | Economyup

Valore PA: Corsi di formazione 2024 | ilPersonale.it

Da rivedere:

City Vision Milano 2024 | City Vision (city-vision.it)

Il workshop di Ernesto Belisario al Think Festival 2024 | E-lex.it

Pubblicazioni

Shaping the Future of Learning: The Role of AI in Education 4.0 | World Economic Forum (weforum.org)

Link attivi al 16 maggio 2024

Prodotto da: PoliS-Lombardia

Coordinamento editoriale a cura di **Davide Perillo**

Comitato Scientifico: **Marco Sica, Marco Bassini, Annalisa Negrelli**