IT4LIA, a Bologna il supercomputer per spingere l’AI tra le imprese e rafforzare l’autonomia europea nell’HPC



Il supercomputer IT4LIA arriva al Dama Tecnopolo di Bologna

Promuovere e accelerare l’adozione dell’intelligenza artificiale (AI) in comparti strategici come l’agroalimentare, la cybersecurity, le scienze della terra e il manifatturiero. Questo l’obiettivo di **E4 Computer Engineering**, l’azienda emiliana con sede in provincia di Reggio Emilia, che si è aggiudicata la realizzazione di **IT4LIA AI Factory**, l’AI Factory italiana promossa da **EuroHPC Joint Undertaking (EuroHPC JU)**,co-finanziata dal **Ministero dell’Università e**

della Ricerca e gestita da **CINECA**.

E4 diventa il primo system integrator italiano a vincere una gara nell'ambito delle AI Factories europee e avrà il coordinamento tecnico del progetto, con presidio fisso al **Dama Tecnopolo di Bologna**, a cu partecipano diversi partner di livello come Dell Techologies, NVIDIA, Alma Mater Studiorum – Università di Bologna, Università degli Studi di Torino, VAST Data, Axelera AI, SiPearl e Rittal.

E4 diventa Il primo system integrator italiano a vincere una gara delle AI Factories

Nascerà così un nuovo ecosistema in cui industria, ricerca e università collaboreranno per costruire un'infrastruttura all'altezza delle sfide globali, con un investimento complessivo che ammonta a circa 420 milioni di euro, sostenuto dalla Commissione europea tramite EuroHPC JU e dal Governo italiano.

Il supercalcolatore IT4LIA fa parte dell'omonima **AI Factory** europea, selezionata nel dicembre 2024 e coordinata da Cineca, rientrando nel **network delle 19 infrastrutture che EuroHPC** sta implementando in Europa per offrire accesso al calcolo avanzato a startup, Pmi e comunità di ricerca, nel rispetto degli standard europei di sovranità dei dati.

"*L'aggiudicazione ad E4, primi italiani nel contesto delle AI Factory EuroHPC, è per noi un traguardo fondamentale, un riconoscimento che ci consente di portare le nostre competenze ai massimi livelli internazionali. Siamo orgogliosi di essere protagonisti insieme ai nostri partner di IT4LIA, una infrastruttura sovrana che rappresenta una opportunità incredibile per la diffusione dell'AI e per la competitività del nostro paese. Continueremo a lavorare con i nostri partner*

con cui siamo riusciti a creare una proposizione vincente e continueremo ad investire in ricerca ed innovazione per essere sempre – come in questo caso – sulla frontiera delle tecnologie europee", ha dichiarato **Cosimo Damiano Gianfreda**, CEO di E4 Computer Engineering.

Aggiudicandosi la commessa, **E4 diventa il primo system integrator italiano a vincere una gara nell'ambito delle AI Factories europee**.

Che cos'è IT4LIA

Il DAMA Tecnopolo di Bologna, già punto di riferimento europeo per il supercalcolo, i big data, l'intelligenza artificiale e il calcolo quantistico, accoglie al suo interno il nuovo supercalcolatore di nuova generazione IT4LIA. Il sistema sarà **4 volte più potente per le applicazioni standard** e fino a **40 volte più potente per i carichi di lavoro specifici per l'AI**.

E4, è spiegato sul sito dell'azienda, si occuperà dell'integrazione di un sistema *AI liquid-cooled* ad alta efficienza energetica, composto da oltre 2.000 nodi e 8.000 GPU, realizzato con tecnologie completamente europee nell'ambito del programma NextGen EU.
Il perimetro di intervento include inoltre lo sviluppo dello *stack software* per facilitare l'implementazione e la diffusione dell'AI, nonché il supporto e la manutenzione del sistema in produzione.

"*Una pietra miliare per l'ecosistema europeo dell'IA e un passo significativo nel rafforzamento del ruolo dell'Italia nel panorama tecnologico globale. Con il sostegno del Ministero dell'Università e della Ricerca e attraverso una stretta collaborazione con EuroHPC Joint Undertaking ed E4 Computer Engineering, stiamo costruendo un ambiente sicuro, sovrano e ad alte prestazioni in cui l'innovazione europea possa prosperare, pienamente in linea con i valori europei in materia di privacy dei dati e autonomia tecnologica*", ha

spiegato **Gabriella Scipione**, HPC Director di CINECA.

È l'**evoluzione del supercalcolatore LEONARDO** verso una **infrastruttura AI-ottimizzata** di prima classe, concepita come uno sportello unico, user-friendly e altamente competitivo. L'obiettivo è costruire un ecosistema coeso capace **di connettere ricercatori, sviluppatori, startup e PMI**, colmando il divario tra i fornitori di soluzioni AI e i potenziali utilizzatori: **pubblica amministrazione**, università, imprese e studenti.

AI, supercalcolo e sovranità digitale nazionale ed europea

Il progetto è entrato nella sua fase operativa il 5 settembre 2025 al DAMA Tecnopolo di Bologna, alla presenza della Vicepresidente della Commissione Europea, **Henna Virkkunen**, e del Ministro dell'Università e della Ricerca, **Anna Maria Bernini**.

Dal punto di vista settoriale, il supercomputer si concentrerà sull'adozione dell'AI in comparti strategici come l'agroalimentare, la cybersecurity, le scienze della terra e il manifatturiero, attraverso l'accesso a repository di dati e servizi specifici per ciascun dominio, insieme a iniziative di formazione per qualificare l'intero ecosistema.

Con **14 supercomputer** e il **7,2% della potenza di calcolo globale**, l'Italia è oggi il **terzo Paese al mondo per capacità computazionale**, dietro solo a colossi come Stati Uniti e Giappone.

IT4LIA è parte del più ampio programma europeo di AI Factories gestite da EuroHPC/JU, che punta a creare un ecosistema sovrano di AI e calcolo ad alte prestazioni sul suolo UE. Posizionando l'Italia come hub centrale (Bologna) di questo ecosistema, il Paese aumenta il suo peso nelle decisioni su

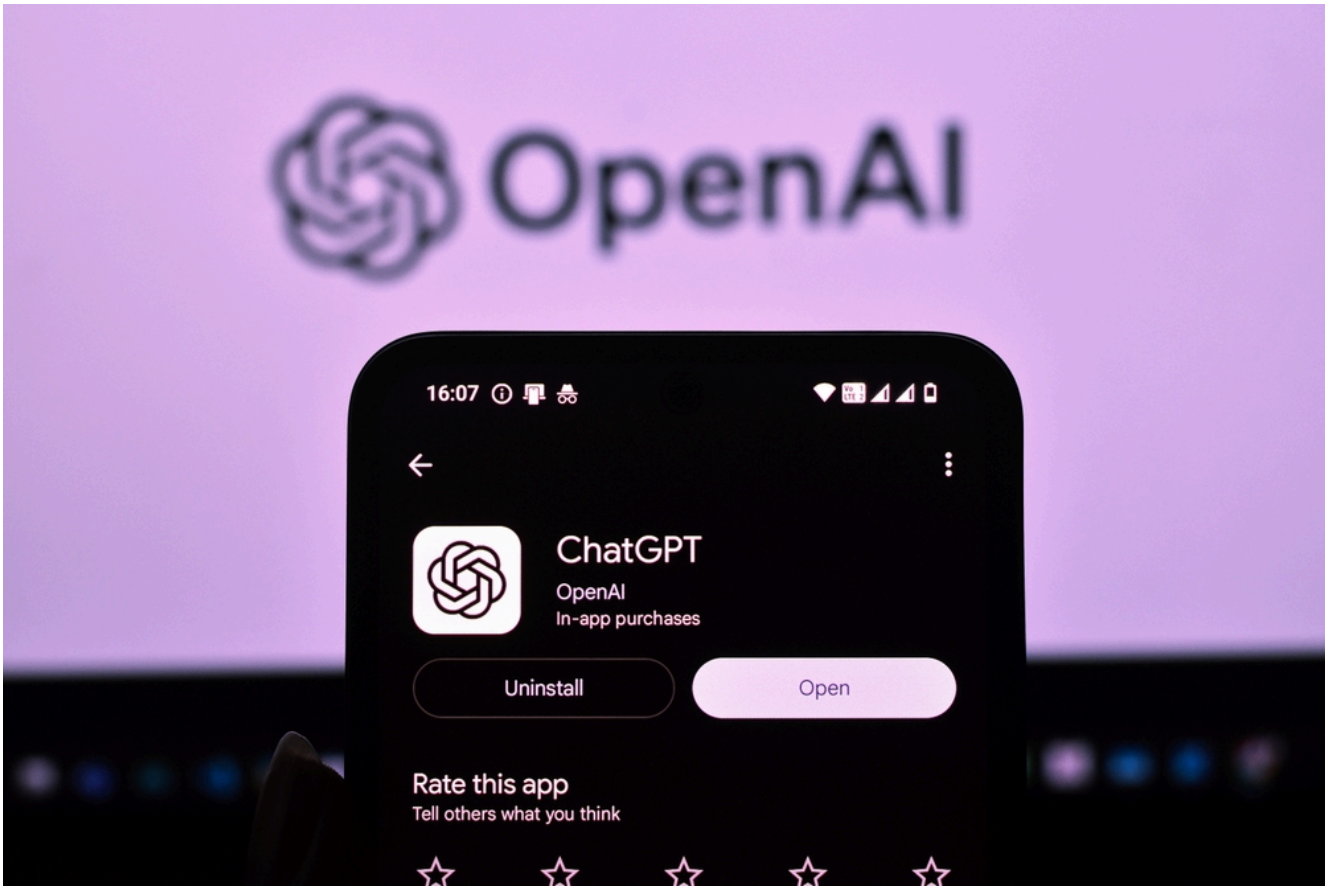
standard, governance dei dati, e architetture cloud-AI, consolidando una sovranità digitale collettiva europea a cui l’Italia contribuisce in modo strutturale.

Il progetto rafforza la strategia italiana di sovranità digitale perché colloca sul territorio nazionale un’infrastruttura di supercalcolo e AI ad alto livello, controllata tramite enti pubblici e sovranazionali europei, e aperta a PA, ricerca e imprese italiane, riducendo dipendenze da infrastrutture cloud e AI proprietarie straniere.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/it4lia-a-bologna-il-supercomputer-per-spingere-lai-tra-le-imprese-e-rafforzare-lautonomia-europea-nellhpc/570892/

OpenAI presenta GPT-5.4-Cyber a governi e alleati Five Eyes



OpenAI ha avviato negli ultimi giorni una serie di briefing con agenzie federali statunitensi, governi locali e Paesi dell'alleanza **Five Eyes** per presentare le capacità del suo nuovo prodotto di cybersecurity: **GPT-5.4-Cyber**.

La notizia, riportata da Axios segnala l'interesse crescente delle istituzioni per strumenti AI avanzati applicati alla sicurezza.

GPT-5.4-Cyber: un nuovo modello per la difesa

La sicurezza informatica sta diventando uno dei principali terreni di confronto tra laboratori di AI come OpenAI e Anthropic. I modelli più avanzati, infatti, rappresentano un doppio elemento: da un lato possono introdurre nuovi rischi, dall'altro offrono capacità sempre più sofisticate per la difesa.

OpenAI ha presentato la scorsa settimana, una variante del suo

modello di punta ottimizzata per attività di cybersecurity difensiva. Il sistema è stato mostrato a circa 50 professionisti della difesa informatica durante un evento a Washington, con dimostrazioni pratiche delle sue capacità.

Accesso controllato e alleanza Five Eyes

L’azienda ha avviato briefing anche con i Paesi membri dei Five Eyes – Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda – con l’obiettivo di selezionare e abilitare i primi utilizzatori del modello.

GPT-5.4-Cyber sarà inizialmente distribuito in modo limitato, solo a fornitori di sicurezza, organizzazioni e ricercatori verificati. La scelta riflette la natura più permissiva del sistema, che richiede controlli rigorosi per evitare utilizzi impropri.

La sfida tra OpenAI e Anthropic

La mossa arriva a breve distanza dal lancio di Mythos da parte di Anthropic, un modello con caratteristiche simili ma orientato anche alla capacità di sfruttare le vulnerabilità individuate. Anche in quel caso, la distribuzione è stata limitata a pochi partner selezionati, tra cui **Amazon, Apple e Microsoft,** a conferma di un approccio prudente verso tecnologie ad alto potenziale dual use.

Il confronto tra OpenAI e Anthropic segna l’avvio di una nuova fase: la competizione non riguarda più solo modelli generativi, ma sistemi in grado di operare direttamente su codice e infrastrutture critiche. Si tratta di strumenti progettati per un uso professionale, con applicazioni immediate nella sicurezza informatica, dal vulnerability assessment all’analisi delle superfici di attacco.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/openai-presenta-gpt-5-4-cyber-a-governi-e-alleati-five-eyes/570853/

L’inganno dell’intelligenza artificiale



- Pubblicato: 17/03/2026
- Pagine: 324
- ISBN: 9791259678447
- Prezzo: 20,00
- Fazi editore

Le tecnologie vendute come “**intelligenza artificiale**” sono spesso presentate come una magia capace di risolvere ogni problema. Emily M. Bender e Alex Hanna, due delle voci più influenti nel dibattito sull’IA, spiegano perché non è così. In questo saggio illuminante smontano l’esaltazione mediatica alimentata dalle **Big Tech**: l’IA di oggi è fatta di sistemi

statistici su larga scala, che producono linguaggio e immagini senza comprenderli – non un'intelligenza pensante ma «pappagalli stocastici», secondo la definizione resa popolare da Bender per descrivere rischi e limiti dei **modelli linguistici di grandi dimensioni** (LLM) come ChatGPT e Gemini.

Le autrici ripercorrono le radici del **tecno-ottimismo contemporaneo**, spiegano con chiarezza che cos'è l'IA e come funzionano davvero questi sistemi. Ne sfatano i falsi miti (neutralità delle macchine, automazione "inevitabile") e mettono in luce le insidie del loro impiego in ambiti chiave – lavoro, sanità, giustizia, istruzione, scienza, arte e giornalismo. Dietro la **retorica dell'innovazione** emergono dati raccolti senza consenso, lavoro nascosto e sottopagato, un impatto ambientale crescente e un marketing che propone illusioni come possibilità concrete.

Bender e Hanna sollevano domande chiave: **l'IA ci renderà più competenti o più dipendenti? Creerà una società più equa o più diseguale? Chi ne risponde quando un algoritmo sbaglia?**

Una riflessione lucida, brillante e accessibile sulle sfide poste dall'intelligenza artificiale: per riportare il dibattito sulle questioni essenziali – diritti, trasparenza, responsabilità –, scegliere consapevolmente quali tecnologie adottare e costruire un futuro in cui l'innovazione torni al servizio delle persone.

Emily M. Bender, è linguista computazionale e professoressa all'Università di Washington, dirige il master in Computational Linguistics. Tra le studiose di riferimento internazionali su linguaggio e IA, nel 2023 è stata inclusa da «Time» nella lista delle 100 persone più influenti nel campo dell'intelligenza artificiale.

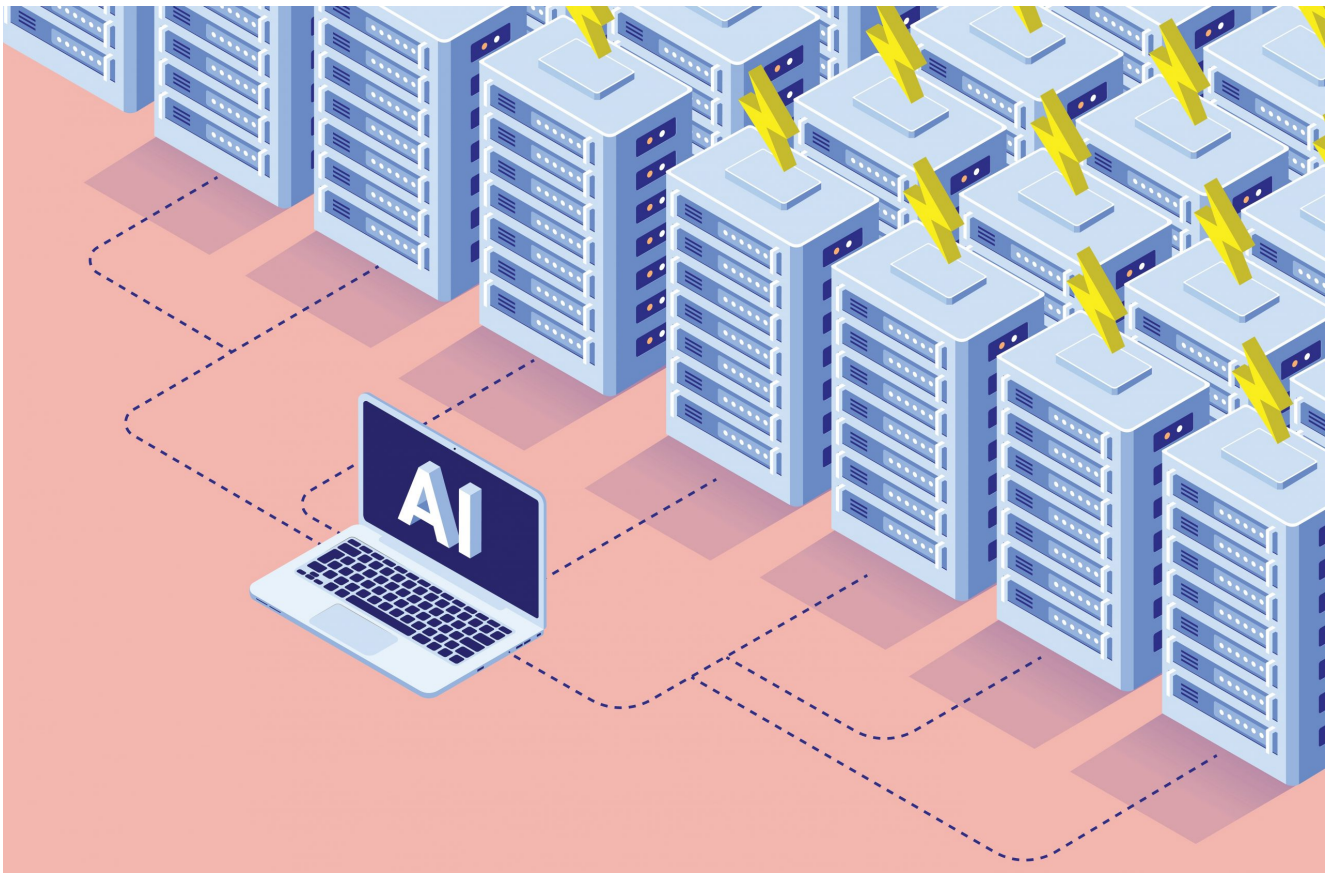
Alex Hanna, sociologa, già ricercatrice in Google, oggi è direttrice della ricerca al Distributed ai Research Institute (DAIR) e docente alla School of Information dell'Università

della California, Berkeley. È tra le voci più ascoltate sui risvolti sociali dell'IA. Le sue analisi compaiono su «The Washington Post», «Financial Times», «Time» e altre testate.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/linganno-dellintelligenza-artificiale/570843/

L'impresa corre con l'AI: la produttività sale del 5,2%



Truenumbers *è l'appuntamento settimanale con la rubrica curata dal portale www.truenumbers.it, il più importante sito editoriale di Data Journalism in Italia, fondato da* ***Marco Cobianchi****. Una rubrica utile per saperne di più, per*

approfondire, per soddisfare ogni curiosità, ma sempre con la precisione che solo i numeri sanno dare. Per leggere tutti gli articoli della rubrica Truenumbers su ***Key4biz*** *clicca qui.*.

Efficienza e redditività in aumento, ma la diffusione resta ferma all'11,2%

Nelle imprese che adottano l'intelligenza artificiale, **il valore aggiunto generato da ogni lavoratore aumenta del +5,2% e il margine operativo lordo (EBITDA) per addetto cresce dell'11,9%**. È quanto emerge da un'analisi di *Banca d'Italia* sull'impatto economico dell'AI nelle imprese italiane. Non è fantascienza, non è propaganda tech: sono numeri, e vengono da una delle istituzioni più serie e prudenti del paese. In termini concreti, ogni dipendente contribuisce a produrre più valore e più margine per l'azienda – e no, non a scapito di nessuno: questo avviene senza variazioni significative nell'occupazione complessiva e senza un aumento del costo del lavoro per unità di prodotto.

L'aumento della produttività dipende soprattutto da processi più efficienti. L'intelligenza artificiale viene utilizzata per automatizzare le attività ripetitive, ridurre i tempi e usare meglio le risorse. Questo libera tempo che viene spostato su compiti a maggiore valore aggiunto, con un effetto diretto sulla produttività media. Il risultato è semplice: le imprese riescono a produrre di più e a generare più margini con le stesse risorse, senza aumentare gli input. In questo senso, l'AI non sostituisce il lavoro, ma ne migliora l'efficacia.

AI, diffusione lenta tra le imprese italiane

In Italia la diffusione dell'intelligenza artificiale resta ancora contenuta. **Sulla base di dati raccolti nel 2024 su imprese con almeno 50 addetti, l'11,2% utilizza già queste tecnologie**, mentre il 28,4% prevede di adottarle entro i due anni successivi. Accanto a queste, il 33,4% le considera non rilevanti per la propria attività e il 26,9% non esprime una valutazione, segno di una diffusione ancora incerta e disomogenea. **Il confronto europeo conferma il ritardo: secondo Eurostat, solo l'8,2% delle imprese italiane con almeno 10 addetti utilizza l'AI, contro una media UE del 13,5%.**

La tecnologia resta quindi concentrata in una parte limitata del sistema produttivo, soprattutto tra le imprese più grandi e nei settori a maggiore intensità di conoscenza. Questo limita, almeno in questa fase, l'impatto sull'economia nel suo complesso: i miglioramenti in termini di produttività e margini emergono già a livello aziendale, ma non sono ancora abbastanza diffusi da incidere in modo significativo sugli aggregati macroeconomici.

Con l'AI le imprese hanno più profitti

L'adozione dell'intelligenza artificiale si traduce in un miglioramento diretto dei margini. Nelle imprese che la utilizzano, il **ROA aumenta di circa +0,5 punti percentuali**, il **rapporto tra EBITDA e ricavi cresce di +2,0 punti percentuali** e il **cash flow in rapporto agli attivi sale di +0,6 punti percentuali**. In concreto, significa che le aziende non solo producono valore, ma riescono anche a trasformarne una quota maggiore in margine e liquidità. Il ROA misura il rendimento delle risorse impiegate, quindi quanto l'azienda è efficiente nell'utilizzare capitale e asset, mentre il cash

flow indica la capacità di generare cassa dall'attività operativa.

Il punto centrale è proprio questo: **l'AI non incide solo sui volumi, ma sulla qualità economica della produzione**. Riducendo inefficienze, tempi e sprechi, consente alle imprese di trattenere una parte più ampia del valore generato. I ricavi diventano più "profittevoli" e l'attività operativa più solida dal punto di vista finanziario. È in questo senso che si parla di margini in aumento: non perché le imprese vendono necessariamente di più, ma perché guadagnano di più su ciò che producono.

AI, lavoro stabile ma più qualificato

L'introduzione dell'intelligenza artificiale non modifica in modo significativo il numero complessivo di occupati nelle imprese che la adottano: i dati non evidenziano variazioni rilevanti nei livelli totali di occupazione. Cambia però la composizione della forza lavoro. In particolare, aumenta la quota di lavoratori **white collar** – impiegati e figure con mansioni amministrative, tecniche o gestionali – di **+0,7 punti percentuali**, mentre diminuisce quella dei **blue collar**, legati ad attività manuali o ripetitive, di **–1,1 punti percentuali**. L'effetto principale è quindi una riallocazione interna del lavoro verso profili più qualificati, più che una riduzione o un aumento dell'occupazione complessiva.

Il cambiamento riguarda soprattutto la qualità del lavoro, più che la sua quantità. L'intelligenza artificiale viene impiegata per automatizzare attività operative e ripetitive, mentre cresce il peso delle funzioni che richiedono competenze analitiche, organizzative e decisionali. Ne deriva una riorganizzazione interna di processi e ruoli, senza effetti evidenti sul numero complessivo degli occupati. Questa lettura è coerente anche con le aspettative delle imprese: **circa il**

70% non prevede alcun impatto sull’occupazione, mentre il 17% si attende una riduzione e solo il 2% un aumento.

Più efficienza nei processi che innovazione

Nelle imprese l’intelligenza artificiale entra ovviamente più nei processi che nei prodotti. **Nel 54% dei casi viene utilizzata per rendere più efficienti le attività produttive e organizzative, mentre nel 24,8% serve a automatizzare compiti ripetitivi e standardizzati**. Solo in una quota più limitata, pari al 13,9%, contribuisce a migliorare la qualità di prodotti e servizi, e in appena il 3,6% dei casi viene impiegata per sviluppare nuove offerte o applicazioni più innovative. Il quadro che emerge è quello di un utilizzo ancora pragmatico: l’AI viene adottata prima di tutto per far funzionare meglio ciò che già esiste, più che per cambiare in modo radicale il modello di business.

Con l’AI, prezzi stabili e rincari più contenuti

Nel breve periodo l’intelligenza artificiale non cambia i prezzi praticati dalle imprese: i listini restano sostanzialmente invariati e non emergono effetti significativi sui prezzi applicati. La differenza si vede guardando avanti. Le aziende che adottano l’AI si aspettano aumenti più contenuti, inferiori di circa **0,4 punti percentuali** rispetto a chi non la utilizza. In altre parole, prevedono di ritoccare i prezzi meno del resto del mercato.

Alla base ci sono i guadagni di efficienza. Processi più veloci, meno errori e un uso più efficace delle risorse riducono i costi operativi nel tempo. Questi benefici non si trasferiscono subito sui prezzi, ma iniziano a entrare nelle strategie future delle imprese. L’effetto è graduale e si

riflette soprattutto nelle aspettative: una minore pressione ad aumentare i listini negli anni successivi.

L’AI non cambia l’inflazione oggi, ma domani sì

Le imprese che adottano l’intelligenza artificiale si aspettano **un’inflazione più bassa nel medio periodo: –0,25 punti percentuali a due anni e –0,33 a quattro anni**. In questo caso, per inflazione si intendono **le aspettative delle aziende sull’aumento generale dei prezzi nell’economia**. Nel breve termine, infatti, non emergono differenze: tra i 6 e i 12 mesi le previsioni restano sostanzialmente invariate. Il cambiamento riguarda l’orizzonte più lungo, dove i guadagni di efficienza legati all’AI iniziano a essere incorporati nelle aspettative. In altre parole, le imprese si attendono che, nel tempo, produrre costi meno e questo contribuisca a ridurre la pressione sui prezzi.

Diffusione diseguale: l’AI resta per pochi

L’intelligenza artificiale non sta avanzando in modo uniforme nel sistema produttivo. Si concentra soprattutto nelle imprese più grandi e nei settori ad alta intensità di conoscenza, dove competenze tecniche, investimenti digitali e strutture organizzative più complesse rendono più facile integrare queste tecnologie nei processi. È qui che l’AI trova terreno fertile e produce effetti più evidenti in termini di produttività e margini.

Al di fuori di questo perimetro, la diffusione è ancora limitata. Le imprese più piccole e meno strutturate faticano ad adottarla, sia per mancanza di risorse sia per competenze. Ne deriva un quadro ancora parziale: i benefici esistono, ma restano concentrati. Il rischio, in questa fase, è che si

allarghi la distanza tra le aziende che riescono a sfruttare l'AI e quelle che restano indietro.

Fonte: *Banca d'Italia*

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/limpresa-corre-con-lai-la-produttivita-sale-del-52/570834/

L'analisi di ASviS. Vespignani (Northeastern University): "Umani e AI sono ormai un unico sistema"



Anche se molti non se ne rendono conto, l'**intelligenza artificiale** (AI) fa ormai parte delle nostre vite: "un processo dinamico nel quale le nostre scelte alimentano gli

algoritmi e gli algoritmi, a loro volta, orientano preferenze, comportamenti e visioni del mondo. Dai sistemi di raccomandazione agli assistenti digitali, fino alle piattaforme social e ai modelli generativi, si attiva un 'circolo di feedback' continuo che trasforma dati in decisioni e decisioni in nuovi dati. Questo intreccio produce effetti sociali complessi, talvolta inattesi, che riguardano informazione, polarizzazione, consumi, partecipazione democratica. Comprendere le dinamiche di questa interazione è decisivo per governare l'intelligenza artificiale con responsabilità, sviluppando strumenti teorici e normativi capaci di affrontare le sfide tecniche, etiche e politiche poste da un ecosistema sempre più interconnesso, e promuovendo consapevolezza critica nei cittadini".

Così si presentava sul sito della Biennale Tecnologia – Soluzioni, la *lectio magistralis* di **Alessandro Vespignani** al Politecnico di Torino, che il 15 aprile ha dato il via alla manifestazione, parlando sul tema: "**La co-evoluzione di esseri umani e intelligenza artificiale".**

[embedded content]
Alessandro Vespignani è presidente della Fondazione Isi di Torino ed è Sternberg family distinguished university professor presso la Northeastern University, dove dirige il Network Science Institute. La sua ricerca si colloca all'intersezione tra modellistica computazionale, scienza dei dati e sistemi complessi, con un focus sui fenomeni di contagio come le epidemie, la diffusione dell'informazione e i comportamenti collettivi. Ma è anche autore di libri di divulgazione scientifica, tra cui *L'algoritmo e l'oracolo* e *I piani del nemico*.

Ecco il video integrale dell'evento di apertura della Biennale Tecnologia. Dopo l'introduzione di **Luca Antonio Graziani**, professional roject anager per le manifestazioni culturali dell'Ateneo, è intervenuto per un saluto il rettore del Politecnico **Stefano Paolo Corgnati.** Si è poi entrati nel vivo

del tema con l'intervento di **Guido Saracco**, ex rettore del Politecnico e curatore di Biennale Tecnologia (dal minuto 10.30) e la conferenza di Vespignani (dal minuto 19). Ne riportiamo le conclusioni.

"*Dobbiamo reinventare completamente come facciamo formazione, educazione, università. Pensare che il sistema universitario nel mondo, non in Italia, nel mondo, possa continuare tra cinque anni a essere quello che è ora è ingenuo, non può essere. Noi dobbiamo reinventarlo completamente. È inutile che vietiamo l'uso dell'intelligenza artificiale o diciamo no 'usiamo tutti l'intelligenza artificiale', non funziona così. Noi dobbiamo creare un sistema formativo che tenga conto del tasso di velocità di questa macchina è alla quale non siamo preparati. (…) Noi non dobbiamo solo rispondere alle domande di oggi; quando noi pensiamo all'Agi, quando pensiamo a queste macchine, sono domande che valgono oggi e probabilmente non varranno tra quattro anni. E quando facciamo insegnamento, non possiamo insegnare cose che sono già vecchie nel momento in cui ne stiamo parlando; cioè il nostro sistema formativo, il nostro sistema di comunicazione deve cominciare a parlare di cose che vedono il futuro, altrimenti saremo sempre indietro. Una volta si diceva: le università devono insegnare quello di cui poi l'industria e il mondo del lavoro ha bisogno. Il problema è che noi adesso dobbiamo insegnare quello di cui forse il mondo del lavoro avrà bisogno tra cinque anni perché gli studenti poi escono tra cinque anni e tra cinque anni quello che insegniamo ora probabilmente sarà già un'altra cosa. Quali sono gli strumenti per chi ha una formazione universitaria, per essere pronto a ingaggiare il mondo in cinque anni? È giusto partire dalle domande giuste. Questa è la mia conclusione: abbiamo realmente costruito il sistema complesso più sofisticato della storia umana ed è ora di iniziare a studiarlo come un sistema complesso*".

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/lanalisi-di-asvis-vespignani-northeaste

rn-university-umani-e-ai-sono-ormai-un-unico-sistema/570816/

L’AI entra nei licei italiani. Mim: “L’obiettivo è formare una coscienza digitale”



L’intelligenza artificiale nelle nuove Indicazioni per i licei italiani volute dal ministro Valditara

L’**intelligenza artificiale** (AI) entra ufficialmente e di fatto nei **licei italiani**, non come oggetto di fascinazione tecnologica, ma “*come territorio critico da governare*”. È

quanto si legge sul sito del ministero dell'Istruzione e del merito (Mim) in attuazione delle nuove "Indicazioni Nazionali per i Licei", fortemente volute dal ministro dell'Istruzione, **Giuseppe Valditara**.

Indicazioni che il ministero invierà anche ai rappresentanti delle Consulte studentesche e altri stakeholders e che saranno adottate "*solo al termine del percorso di ascolto della comunità scolastica*". Il testo è alla base di un progetto di riforma del secondo ciclo di istruzione che ripensa a livello strutturale l'intera funzione formativa della scuola superiore, in particolare il rapporto tra le discipline scolastiche e i cambiamenti profondi che stanno interessando la nostra società.

AI e coscienza digitale al tempo dell'epistemia

Tornando all'**AI**, in attuazione della Legge 132/2025 e dell'AI Act europeo, il suo inserimento a livello disciplinare segue una logica ben precisa e un obiettivo chiave: "***formare una coscienza digitale*** *capace di distinguere tra la simulazione algoritmica* – la *doxa* – *e il sapere validato* – l'*epistéme*", è chiarito nel comunicato ministeriale.

In greco antico *epistémē* indicava "*la conoscenza vera, certa e giustificata*", diversa dalla semplice "*opinione*" (*doxa*).

Oggi, soprattutto in Italia, il termine *epistémē* è stato ripreso per descrivere un fenomeno psicologico e culturale su cui molto di dibatte: l'**epistemia**. Ci si sente "più istruiti" o "più competenti" solo perché un chatbot AI produce testi ben formulati, anche se non si sono verificati i dati o i ragionamenti che li hanno prodotti. Di fatto, sempre più spesso, la plausibilità del discorso, la buona estetica (come di dice, qualcosa che 'suona bene') sostituisce la verifica della conoscenza, creando l'illusione di possedere sapere

reale.

“*Viviamo in un’epoca in cui la fluidità del linguaggio viene scambiata per profondità. In cui la plausibilità sintattica di una frase basta a conferirle autorevolezza. È qui che prende forma una nuova condizione cognitiva, che possiamo chiamare epistemia: l’incapacità di distinguere ciò che suona come conoscenza da ciò che è conoscenza*“, scrive uno dei massimi esperti di questo argomento, **Walter Quattrociocchi**, professore ordinario di Informatica all’Università di Roma “La Sapienza” e alla guida del Center of data science and complexity for society (da leggere lo studio “*The simulation of judgment in LLMs*“, pubblicato su PNAS).

Un problema enorme, che intacca i processi conoscitivi, cognitivi e decisionali. Fidarsi di un testo ‘che suona bene’ genera approssimazione, ignoranza, disinformazione e cattiva coscienza di sé e dell’ambiente in cui si vive.

Governare la tecnologia con consapevolezza

Probabilmente Valditara e il suo ministero non si preoccupano (ancora) di questo aspetto, invece così presente nella nostra esperienza quotidiana con l’AI e con le sue simulazioni di realtà (che ormai stanno sempre più caratterizzando il nostro mondo e il nostro modo di stare al mondo). L’intento del Mim è fare in modo che gli studenti imparino ad usare l’AI consapevolmente, ma anche a interrogarla, “*a riconoscerne i limiti, a tutelarne i confini rispetto alla propria libertà intellettuale*”.

Insomma, “*l’obiettivo non è addestrare studenti all’uso degli strumenti digitali: è formarli a governarli con consapevolezza*”.

Una missione di grande importanza, anche perchè oggi un

giovane su due in Italia proprio in età scolastica usa ormai chatbot AI.

Capire l'AI, con la matematica

Altra novità importante è proporre la **matematica** come "*esperienza intellettuale*", cioè fare in modo che le tecniche alla base di questa disciplina scolastica così importante diventino "*strumenti per comprendere concetti, modelli e decisioni – ovvero per esercitare quella cittadinanza attiva e critica che è l'obiettivo ultimo del percorso liceale*".

Alla matematica, poi, è affidato "*il compito di fornire i concetti e il linguaggio che stanno alla base dei sistemi di AI*".

Via la Geostoria, un posto al sole per italiano e filosofia

Tra le altre Indicazioni per i licei annunciate del ministero, c'è il rilancio della lettura come pratica identitaria, la fine della geostoria e il ritorno come discipline autonome di storia e geografia. La filosofia, invece, troverà un nuovo posto a scuola come "*pratica concreta (esercizio di riflessione, interrogazione, giudizio, argomentazione)*" e come "*sapere storico e teorico, tradizione di autori e testi da conoscere e approfondire*".

Non ultimo un ritrovato ruolo dei licei nel migliorare le relazioni umane e quindi la società nel suo insieme. Una specie di missione etica in cui "*i licei dedicano ampio spazio all'educazione emotiva e relazionale così come al contrasto di ogni forma di violenza e di discriminazione*", dove "*il rispetto è riconosciuto come presupposto etico che precede e fonda l'agire civile: non una norma da rispettare, ma una disposizione da coltivare*". Strumenti utili a costruire i fondamenti della convivenza pluralistica, "*dove l'inclusione*

non è concessione ma architrave della cultura occidentale moderna”.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/lai-entra-nei-licei-italiani-mim-lobiettivo-e-formare-una-coscienza-digitale/570733/

Intelligenza artificiale e criminalità Informatica: quando lo stesso strumento difende e attacca

L’AI ridisegna i confini della digital forensics e apre interrogativi inediti per magistratura e forze dell’ordine

C’è un momento preciso in cui una tecnologia smette di essere neutrale. Non è quando viene usata per fare del male, perché quella è una storia antica quanto il fuoco. È quando diventa così pervasiva, così duttile, così integrata nella catena causa-effetto del crimine da rendere irriconoscibile la distinzione tra arma e scudo. Con l’intelligenza artificiale applicata alla cybersecurity, quel momento è adesso.

Un paper depositato su arXiv il 16 ottobre 2025, dopo essere stato presentato all’APWG-EU Tech Summit and Researchers Forum di Cagliari nel giugno dello stesso anno, mette a fuoco con rara lucidità questa doppia natura dell’AI applicata alla criminalità informatica.

I suoi autori, Silvia Lucia Sanna, Leonardo Regano, Davide

Maiorca e Giorgio Giacinto, lavorano tutti all'Università di Cagliari, nell'ambito del progetto SERICS finanziato dal PNRR europeo. Il titolo, sobrio e tecnico, non tradisce l'ambizione dell'analisi: *Improving Cybercrime Detection and Digital Forensics Investigations with Artificial Intelligence*. Ma quello che il paper contiene è molto più di un inventario di tecniche. È una mappa concettuale di un territorio in rapida trasformazione, con implicazioni che si estendono ben oltre i laboratori universitari, fino alle aule dei tribunali.

Il doppio volto dell'AI nella criminalità informatica e nelle indagini digitali

La premessa da cui muovono i ricercatori cagliaritani è scomoda ma ineludibile: i modelli linguistici di grandi dimensioni, Gemini, Copilot e ChatGPT, che oggi assistono gli analisti forensi nell'elaborazione di enormi volumi di evidenze digitali, sono gli stessi strumenti che i criminali informatici possono impiegare per nascondere le proprie tracce, automatizzare attacchi e generare contenuti sintetici difficili da attribuire.

Non si tratta di un paradosso astratto. È la descrizione operativa di un ecosistema in cui l'AI agisce simultaneamente come lente d'ingrandimento per gli investigatori e come nebbia artificiale per chi vuole sottrarsi all'indagine. Il riferimento esplicito nel paper è a un recente rapporto Europol sul cybercrime in Europa, che conferma la persistenza e la crescente complessità del fenomeno, richiedendo strumenti di contrasto all'altezza.

Sul versante difensivo, il contributo dell'AI alla forensics digitale è già consistente e documentato. I sistemi di machine learning permettono di analizzare in tempo reale flussi di dati di rete alla ricerca di pattern anomali, di classificare

malware con una granularità che gli approcci *signature-based* non possono raggiungere, di correlare eventi distribuiti su infrastrutture eterogenee ricostruendo catene di attacco che altrimenti rimarrebbero invisibili.

I Large Language Model, in particolare, stanno emergendo come strumenti di supporto cognitivo per gli analisti: capaci di supportare la fase di *reporting*, producendo bozze di documenti, definendo glossari tecnici e sintetizzando le evidenze in linguaggio comprensibile anche per i non specialisti, e di accelerare il *triage* su volumi di prove che nessun team umano potrebbe processare nei tempi richiesti da un'indagine.

Ma è sull'altro versante, quello offensivo e anti-forense, che il paper introduce gli elementi più perturbanti.

Il caso studio: steganografia LSB generata da tre chatbot

Il contributo più originale della ricerca riguarda un caso studio condotto direttamente dai ricercatori, che vale la pena esaminare nella sua specificità tecnica. Sanna e colleghi hanno testato Gemini, Copilot e ChatGPT su due capacità distinte: la generazione di immagini con contenuto steganografico tramite tecnica LSB (*Least Significant Bit*) e la produzione di codice Python funzionante per la codifica e decodifica di immagini steganografiche.

La steganografia digitale applicata sulle immagini è una delle tecniche di occultamento dati più consolidate: consiste nel modificare i bit meno significativi dei pixel di un'immagine per nascondervi informazioni, in modo percettivamente invisibile all'occhio umano. L'immagine di input usata nel test è un file PNG bianco prelevato da Wikimedia, nel quale è stato incorporato il messaggio segreto *"This is a secret message APWG."* Le immagini generate e i contenuti nascosti

sono stati poi verificati con **zsteg**, un tool Linux specializzato in analisi steganografica, e con uno script esterno disponibile su GitHub.

I risultati sono significativi: tra i tre modelli testati, **Copilot si è dimostrato il più performante** nell'esecuzione di entrambi i compiti. Un dato che non è un dettaglio minore: emerge da un test controllato e comparativo, con implicazioni dirette sulla valutazione del rischio nei diversi ecosistemi di AI generativa.

È fondamentale riportare una precisazione che i ricercatori stessi formulano in modo esplicito: la presenza di questi chatbot in un contesto digitale non è di per sé un indicatore di criminalità o attività malevola. La tecnica steganografica, se impiegata da un criminale informatico, diventa uno strumento anti-forense, ma la stessa tecnica ha usi legittimi nella protezione delle comunicazioni. Questa distinzione, che il paper enuncia con chiarezza, è essenziale per evitare letture fuorvianti del lavoro.

La sfida per gli investigatori: quando il codice viene scritto dall'AI

Il dato che rende la ricerca particolarmente rilevante per chi lavora nelle investigazioni non è tanto la tecnica in sé, ma la democratizzazione del suo accesso. Un soggetto privo di competenze di programmazione avanzata può chiedere a un modello linguistico di generare uno script steganografico, personalizzarlo e incorporarlo in un flusso operativo d'attacco. La barriera tecnica all'ingresso si abbassa in modo radicale. La rilevabilità del contenuto nascosto, già difficile per sua natura, non peggiora sul piano tecnico, ma si moltiplica su scala: più attori potenziali, più artefatti, più rumore di fondo per gli investigatori.

Si pone poi un problema ulteriore, che il paper apre pur senza pretendere di risolverlo: come si documenta e si attribuisce, in sede processuale, un contenuto generato tramite AI? Quando il codice che nasconde le prove è stato scritto da un chatbot su richiesta dell'indagato, la catena causale che collega soggetto e artefatto diventa più complessa da dimostrare. Non si tratta ancora di un tema affrontato esplicitamente dal sistema giudiziario italiano, ma è la traiettoria logica di ciò che questo tipo di ricerca rende oggi tecnicamente possibile.

Il paper anticipa infine una visione ancora più radicale per il futuro: gli autori prevedono che l'AI sarà usata in modo sempre più pervasivo tanto nel cybercrime quanto nella digital forensics, fino a configurare scenari di **AI-vs-AI interamente autonomi**, in cui sistemi di attacco e sistemi di difesa si fronteggiano senza intermediazione umana diretta.

Implicazioni operative per gli investigatori

Per chi lavora sul campo, unità di cybercrime, CERT, team SOC e magistratura specializzata, il paper suggerisce alcune linee di riflessione immediate.

La prima riguarda la **formazione**. Se gli LLM sono strumenti già usati sia dagli analisti sia dagli attaccanti, le competenze necessarie per valutarne l'*output*, comprenderne i limiti e riconoscerne i pattern, devono entrare nei programmi di aggiornamento delle forze dell'ordine in modo strutturale, non episodico.

La seconda riguarda la **catena di custodia digitale**. In un contesto in cui contenuti generati da AI si moltiplicano, la documentazione del processo di raccolta e analisi delle evidenze deve includere procedure specifiche per l'identificazione di artefatti potenzialmente prodotti o

modificati tramite AI. Non è più sufficiente certificare che un file “esiste”: occorre certificare con quale grado di confidenza si possa classificare la sua origine.

La terza, la più delicata, riguarda il **valore probatorio** delle analisi AI-assistite in sede processuale. Come approfondito anche nel dibattito sulla digital forensics e il diritto, gli strumenti di rilevazione automatica sono accurati ma non infallibili, e la loro accuratezza varia in funzione del modello che ha generato il contenuto e delle eventuali tecniche di offuscamento applicate. Utilizzarli come prova diretta senza un adeguato *framework* di riferimento e senza perizia tecnica qualificata rischia di introdurre nel processo una forma di errore sistematico difficile da contestare.

Vale la pena segnalare, infine, un ulteriore problema di contesto: l’uso di *Private AI* in ambito forense sta emergendo come requisito operativo nelle indagini più sensibili, proprio perché l’invio di evidenze digitali a servizi AI in cloud introduce criticità di controllo dei dati incompatibili con la catena di custodia.

Un contributo italiano al dibattito globale

Vale la pena sottolineare la provenienza istituzionale di questo lavoro, non per campanilismo, ma per una ragione sostanziale. Il paper nasce all’interno del progetto SERICS (*Security and Rights in CyberSpace*), uno dei *spoke* del PNRR dedicati alla cybersecurity, che coinvolge decine di atenei e centri di ricerca italiani. Il fatto che Silvia Lucia Sanna conduca questa ricerca nell’ambito del Dottorato Nazionale in Intelligenza Artificiale (Sapienza Università di Roma in collaborazione con l’Università di Cagliari) segnala una continuità di investimento sistemico che va ben al di là del singolo paper.

L’Italia è uno dei paesi europei in cui il dibattito sull’uso processuale dell’AI è più vivo, sia per la tradizione di dottrina giuridica in materia di prova digitale, sia per la presenza di strutture investigative specializzate con sensibilità tecnica crescente. Un lavoro come quello di Sanna e colleghi non è solo un contributo alla letteratura accademica: è un documento che può e dovrebbe alimentare la formazione delle procure specializzate e informare le linee guida che le istituzioni competenti stanno costruendo attorno all’uso investigativo dell’intelligenza artificiale.

Conclusione: la neutralità non è un’opzione

L’intelligenza artificiale non ha alleanze. Ottimizza obiettivi. Se l’obiettivo è rilevare una comunicazione criminale nascosta in un’immagine, l’AI può farlo. Se l’obiettivo è nascondere quella comunicazione in modo da complicarne l’individuazione e l’attribuzione, l’AI può farlo con la stessa competenza e, come dimostra il caso di Copilot nel test dei ricercatori cagliaritani, con una certa efficacia.

Questa simmetria non è una ragione per limitare l’uso dell’AI nella forensics. È invece una ragione per sviluppare, con urgenza e rigore, i *framework* tecnici, legali e procedurali che permettano di usare questi strumenti in modo robusto, verificabile e giuridicamente sostenibile.

Il paper di Sanna, Regano, Maiorca e Giacinto non offre risposte definitive. Offre qualcosa di più prezioso: dati sperimentali concreti e le domande giuste. In un campo che cambia a questa velocità, è già un contributo straordinario.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/ai-criminalita-informatica/

AI, ultimi in Europa. Secondo l’Istat usata dal 20% degli italiani, contro media Ue del 33%



L’AI utilizzata da un giovane su due in Italia

Spesso, purtroppo, l’Italia fa notizia per record poco invidiabili, soprattutto nel settore tecnologico e in termini di utilizzo di nuovi strumenti tra la popolazione. Secondo la ricerca “***Cittadini e ICT***” per l’anno 2025 dell’Istat, gli italiani conoscono l’**intelligenza artificiale** (AI), ma non la usano.

Stando ai nuovi dati statistici, “***a livello europeo, il 32,7%***

della popolazione tra i 16 e i 74 anni ha utilizzato strumenti di AI, mentre in Italia la quota è pari al 19,9%”. Questo risultato colloca il nostro Paese al penultimo posto nella graduatoria europea, davanti alla sola Romania (17,8%).

Se si usa la lente e ci si concentra sulla fascia di età che va da 14 a 19 anni, il dato migliora nettamente: **l’AI è usata dal 51,2% dei giovani e dal 43,1% di chi ha tra i 20 ed i 24 anni**. Con una differenza significativa in termini di genere: l’AI piace ed è utilizzata dal 53,3% delle ragazze, contro il 49,1% dei ragazzi.

La differenza la fa il titolo di studio e dove abiti, ma in tanti affermano di non avere bisogno dell’AI

Prendendo in considerazione, invece, il titolo di studio: la quota di utilizzatori di 25 anni e più raggiunge il 32% tra le persone con titolo di studio elevato, si riduce al 14,6% tra chi possiede un diploma di scuola secondaria superiore e si attesta al 3,6% tra coloro che hanno al massimo la licenza media.

A livello regionale, l’utilizzo dell’AI è più diffuso nel Nord (19,7%) e nel Centro (18,8%), rispetto al Mezzogiorno (14,6%).

Tra chi non utilizza l’AI, il 59,9% degli italiani ha dichiarato che il motivo risiede nella mancanza di necessità, seguito dal 21,6% che ha indicato di non saperli utilizzare. Il 5,5% ha sollevato, invece, preoccupazioni relative alla sicurezza o alla protezione dei dati personali, mentre il 4,8% ha precisato di non essere a conoscenza dell’esistenza di tali strumenti.

Raddoppia il numero di imprese che fa uso di AI

L’intelligenza artificiale sta trasformando il lavoro e l’organizzazione dei processi produttivi nelle imprese italiane. Nel 2025, secondo le stime **Anitec-Assinform**, il mercato italiano vale già 1,24 miliardi di euro, in crescita del 33% rispetto ai 935 milioni del 2024 e con proiezioni da oltre 2,5 miliardi entro il 2028. Parimenti, gli ultimi dati **ISTAT**, mostrano un’accelerazione senza precedenti nell’adozione nelle imprese: la quota di queste ultime ad utilizzare almeno una soluzione di IA è più che raddoppiata tra 2024 e 2025 passando dall’8 al 16,4%.

Aumentano però le competenze digitali

Nel 2025 **l’87,3% delle famiglie dispone di un accesso a internet** (+1,1% rispetto all’anno precedente). L’analisi territoriale evidenzia un persistente ritardo del Mezzogiorno, pari circa 5 punti percentuali in meno rispetto al Centro-Nord.

Internet è il mezzo principale ancora oggi per migliorare le proprie competenze digitali. **54,3% è la quota di chi, tra 16 e 74 anni, dichiara di avere competenze digitali almeno di base, +8,4% in più** rispetto all’anno precedente. Resta però lontano l’obiettivo europeo che punta, entro il 2030, a una quota dell’80%.

In Italia, come in altri Paesi europei, spiega l’Istat, le competenze digitali sono caratterizzate da forti divari associati a specifiche caratteristiche socio-culturali della popolazione. Nel 2025, il 71,7% dei ragazzi di 20-24 anni, che hanno usato Internet, afferma di avere competenze digitali almeno di base. Una quota che scende rapidamente con l’età,

per arrivare al 49,1% tra i 55-59enni e attestarsi al 27,4% tra le persone di 65-74 anni.

Eppure**, il 63,9% delle famiglie composte esclusivamente da anziani (65 anni e più) dispone di un accesso a internet da casa**. Una quota, questa, che registra un incremento di 3,3 punti percentuali rispetto al 2024, attenuando la distanza, per quanto ancora notevole, dalle famiglie con almeno un minore (98,7%).

Un italiano su due usa Spid e Cie

Più di metà degli italiani utilizza Spid o Cie. Lo indica l'Istat nel Report Cittadini e Itc nel 2025. Nel 2025 il 53,2% della popolazione tra 16 e 74 anni che ha utilizzato Internet negli ultimi 12 mesi ha utilizzato il Sistema Pubblico di Identità Digitale (Spid) o la Carta d'Identità Elettronica (Cie) nei 12 mesi precedenti l'intervista per accedere a servizi online della Pa o dei gestori dei servizi pubblici (es. servizi sanitari o fiscali) o ai servizi di aziende, imprese o organizzazioni non profit (es. trasporto), valore di poco superiore alla media Ue (52,3% delle persone tra 16 e 74enni).

Come per l'accesso a Internet, anche per l'utilizzo di Spid o Cie esiste un forte divario territoriale. Nel 2025 le persone residenti nel Nord hanno utilizzato nel 52,3% dei casi l'identità digitale nei 12 mesi precedenti l'intervista, a fronte di un 38,3% delle persone del Mezzogiorno.

Per l'accesso a internet domina lo smartphone, poi il pc

Il 79,1% delle persone di 6 anni e più accede a internet tramite lo **smartphone**, secondo l'Istati, il 54% tramite **pc fisso o portatile**, il 38,2% tramite **smart TV**, altoparlanti, **smartwatch** o consolle per video giochi, il 27,8% si avvale del

tablet.

Il numero di dispositivi utilizzati e la loro combinazione evidenziano marcate differenze generazionali. I giovani di 11-24 anni risultano i più orientati a un utilizzo multi-device: quasi il 30% impiega tutti i dispositivi considerati, a fronte del 17,7% nella media della popolazione.

Tra gli adulti di 25-34 anni si osserva una maggiore propensione all'uso combinato di PC, smartphone, smart TV incluso altoparlanti, smart watch o consolle per video giochi (27,1% contro il 17,9% del totale). Le persone di 65 anni e più presentano invece la quota più elevata di utenti che accedono alla Rete esclusivamente tramite smartphone (quasi il 40% a fronte del 20,5% della media).

Crescono gli acquisti online

Quasi metà della popolazione italiana over 14 anni acquista su internet tramite siti di **ecommerce**. Nel 2025, il 49% della popolazione di 14 anni e più ha fatto acquisti online nei 12 mesi precedenti l'intervista, con un aumento di 2,3 punti percentuali rispetto all'anno precedente.

Più di un terzo di queste persone (38%, +1,6 punti percentuali rispetto al 2024) ha ordinato o comprato merci o servizi nei tre mesi precedenti l'intervista, l'11% nel corso dell'anno e il 5,8% più di un anno fa.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/ai-ultimi-in-europa-secondo-listat-usata-dal-20-degli-italiani-contro-media-ue-del-33/570651/

Sentenza Tribunale di Siracusa 338/2026: colpa grave per uso non verificato dell’IA negli atti processuali



Il Tribunale di Siracusa, con la sentenza n. 338 del 20 febbraio 2026, traccia per la prima volta in Italia uno standard di diligenza esigibile dagli operatori del diritto che usano sistemi di intelligenza artificiale generativa. La decisione si inserisce in un filone giurisprudenziale che si sta consolidando e interroga, ben oltre l’avvocatura, chiunque produca output professionali con strumenti di generative AI.

Sentenza Siracusa 338/2026: quattro precedenti di Cassazione inventati dall’IA

Alla prima lettura sembravano tutte al loro posto. Quattro precedenti della Corte di Cassazione, gli estremi completi, la sezione, l’anno, persino il numero di ruolo. Per ognuna un passaggio tra virgolette che avrebbe dovuto dare la stoccata finale e demolire l’eccezione di decadenza che l’avvocato della controparte aveva costruito con cura. Una memoria difensiva costruita con il mestiere, sostenuta da pronunce pertinenti, apparentemente inoppugnabile.

Il Giudice Unico di Siracusa, davanti a quella memoria, ha fatto quello che ogni magistrato fa quando un argomento poggia così nettamente sui precedenti: è andato a leggerli. Le banche dati in uso alla magistratura italiana restituiscono

provvedimenti autentici, con il testo integrale delle motivazioni. Di quei passaggi virgolettati, però, non c'era traccia. Alcune delle sentenze richiamate esistevano davvero, ma trattavano materie diverse, in qualche caso lontanissime dalla questione in discussione; altre non risultavano affatto. I brani riportati tra virgolette, in ogni singolo caso, non figuravano in nessuna pronuncia reale. Non erano imprecisioni né errori di trascrizione: erano testi inesistenti, costruiti *ex novo*.

A quel punto il giudice, prima di pronunciarsi, ha provato a mettersi nei panni di chi aveva firmato quella memoria. Poteva trattarsi di un cortocircuito delle banche dati professionali? No, perché quegli strumenti indicizzano materiale autentico, non lo generano. Un errore mnemonico? Nemmeno, perché non si trattava di un numero sbagliato o di una sezione male attribuita, ma di quattro massime inventate dal nulla. Una falsificazione deliberata? Implausibile, perché nessun professionista esperto si esporrebbe a una conseguenza disciplinare così grave per un vantaggio difensivo tanto modesto.

Restava una sola spiegazione coerente con i fatti: il difensore si era affidato a uno strumento di intelligenza artificiale generativa e aveva riportato negli atti ciò che il sistema gli aveva restituito, senza verificarlo sulle fonti primarie.

Il giudizio riguardava, in origine, tutt'altro. Una società in liquidazione chiedeva oltre centosessantacinquemila euro di risarcimento a chi aveva sottoscritto, in nome di un'associazione non riconosciuta, un contratto di sublocazione poi risolto per morosità. La questione tecnica era l'applicabilità del termine di decadenza semestrale di cui all'art. 1957 c.c. alla responsabilità personale prevista dall'art. 38 c.c., un punto su cui la Cassazione si è espressa più volte in modo univoco. Proprio per superare quell'orientamento, la difesa attorea aveva bisogno di

precedenti che spingessero nella direzione opposta. Ma quei precedenti non esistevano.

La sentenza n. 338/2026 rigetta integralmente la domanda e condanna l'attrice a 14.103 euro di spese legali, ad altrettanti 14.103 euro *ex* art. 96, comma 3, c.p.c. e a ulteriori 2.000 euro in favore della Cassa delle ammende *ex* art. 96, comma 4, c.p.c. Ma il cuore della decisione non è nella cifra: è nel fatto che, per la prima volta in modo così esplicito in Italia, un giudice scrive in motivazione che cosa ci si può aspettare, nel 2026, da chi fa il suo mestiere usando un *Large Language Model*.

Colpa grave per uso acritico dell'IA: la nuova diligenza professionale

Il passaggio motivazionale che rende la decisione un punto di svolta è la qualificazione giuridica dell'errore. Il giudice afferma che costituisce ormai *fatto notorio*, acquisito alla generalità dei consociati e certamente esigibile da un operatore professionale del diritto, che i modelli di IA generativa non sono banche dati giurisprudenziali da cui estrarre precedenti, bensì strumenti di generazione automatica del linguaggio fondati su meccanismi inferenziali di natura statistica e probabilistica.

Tali sistemi, ricorda la sentenza, non *sanno* né *ricordano* alcunché, ma producono sequenze di testo statisticamente plausibili sulla base di miliardi di parametri di addestramento, senza avere accesso, ordinariamente, ad alcuna base di conoscenza verificata o verificabile. È proprio per questo che sono soggetti al fenomeno delle c.d. *hallucinations*, ossia alla generazione di contenuti formalmente plausibili ma sostanzialmente falsi o inesistenti.

Da questa premessa tecnica discende la qualificazione giuridica. L'utilizzo acritico di tali strumenti, senza la doverosa verifica dell'attendibilità degli *output* mediante

consultazione delle fonti primarie, integra gli estremi della colpa grave. Il passaggio è decisivo perché sposta l'asticella della diligenza professionale: non basta più scusarsi con un malfunzionamento tecnico, perché il rischio di *hallucination* è, nel 2026, parte della conoscenza ordinaria che ci si attende da chi esercita una professione regolamentata.

Da Firenze a Milano: la giurisprudenza italiana sulle allucinazioni dell'IA

La decisione siracusana non nasce nel vuoto. Il primo precedente italiano conosciuto è l'ordinanza del 14 marzo 2025 del Tribunale delle Imprese di Firenze, che affrontò una comparsa di costituzione contenente alcune sentenze di Cassazione inesistenti, prodotte da una collaboratrice di studio tramite ChatGPT e non verificate prima del deposito. In quel caso il collegio fiorentino escluse la responsabilità aggravata *ex* art. 96 c.p.c., ritenendo assenti il dolo e il danno concreto, ma riconobbe espressamente il disvalore dell'omessa verifica.

Nei mesi successivi la giurisprudenza di merito si è fatta più rigorosa. Il Tribunale di Torino, Sezione Lavoro, con sentenza n. 2120 del 16 settembre 2025, ha censurato un ricorso redatto "col supporto dell'intelligenza artificiale" e costruito, nelle parole del giudice, su "un coacervo di citazioni normative e giurisprudenziali astratte, prive di ordine logico e in larga parte inconferenti", riconoscendo la responsabilità aggravata *ex* art. 96, commi 3 e 4, c.p.c. A pochi giorni di distanza, il Tribunale di Latina con sentenza n. 1037 del 23 settembre 2025 ha deciso in senso analogo, in una serie di pronunce gemelle che hanno colpito ricorsi seriali redatti "a stampone".

In ambito amministrativo, la sentenza n. 3348 del 21 ottobre 2025 del TAR Lombardia, Sezione V, ha affrontato un ricorso contro la bocciatura di una studentessa di liceo: nell'atto introduttivo, tutte le citazioni giurisprudenziali a sostegno

dell’illegittimità dei provvedimenti impugnati risultavano inesistenti o riferite a orientamenti non noti. Il difensore, messo davanti all’evidenza in udienza, ha ammesso di essersi avvalso di strumenti di ricerca basati su IA. Il TAR ha respinto il ricorso, condannato alle spese e, soprattutto, disposto la trasmissione della sentenza all’Ordine degli Avvocati di Milano per le valutazioni disciplinari di competenza, aprendo un fronte deontologico ulteriore rispetto a quello processuale.

Vale la pena notare che anche la Terza Sezione Penale della Corte di Cassazione, con sentenza n. 25455/2025, ha annullato con rinvio una pronuncia della Corte d’Appello di Torino in materia di reati tributari, rilevando che la motivazione faceva riferimento “a principi di legittimità non affermati o a sentenze di questa Corte inesatte nel numero riportato”: un segnale che il fenomeno comincia a riguardare anche la funzione giudicante.

La pronuncia di Siracusa, dunque, si innesta su questa linea e la porta a un nuovo grado di chiarezza: la colpa grave non è un giudizio di valore, ma la conseguenza della violazione di un obbligo di verifica tecnicamente definito.

Allucinazioni IA in tribunale: oltre 1.300 casi documentati nel mondo

Che il caso siracusano non sia un episodio locale è confermato dai numeri. Il database di Damien Charlotin, ricercatore presso lo Smart Law Hub di HEC Paris, nel maggio 2025 registrava 116 casi in dodici Paesi (Stati Uniti, Israele, Regno Unito, Canada, Australia, Brasile, Paesi Bassi, Italia, Irlanda, Spagna, Sudafrica, Trinidad e Tobago); ad aprile 2026 i casi documentati superano quota 1.300, di cui circa 800 negli Stati Uniti, con rilevazioni che registrano fino a 17

decisioni statunitensi in un singolo giorno.

Le sanzioni crescono in proporzione: un tribunale federale in Oregon ha disposto 109.700 dollari di sanzioni e spese complessive a carico di un singolo avvocato in un caso di citazioni generate dall'IA, cifra riportata come record aggregato negli Stati Uniti. Un'analisi condotta dal Center for Internet and Society di Stanford su 114 casi statunitensi, sulla base degli stessi dati, mostra che il 90% degli studi coinvolti sono *solo practice* o piccoli studi, e che, nei casi in cui è stato possibile identificare il sistema usato, la metà riguarda una versione di ChatGPT.

Il caso fondativo resta Mata v. Avianca (S.D.N.Y., 22 giugno 2023), nel quale il giudice P. Kevin Castel sanzionò con 5.000 dollari in solido due avvocati e il loro studio per aver depositato sei precedenti inesistenti generati da ChatGPT, ritenendo che il comportamento integrasse *subjective bad faith* soprattutto per aver insistito sulle citazioni anche dopo che la controparte ne aveva contestato l'esistenza. È lo stesso schema che si ritrova, con variazioni, in quasi tutti i casi successivi.

Legge 132/2025 art. 13: gli obblighi per i professionisti che usano l'IA

La sentenza siracusana arriva pochi mesi dopo l'entrata in vigore della Legge 23 settembre 2025, n. 132, il primo intervento organico italiano in materia di intelligenza artificiale, che si affianca al Regolamento (UE) 2024/1689 (*AI Act*). L'articolo 13 della legge introduce due principi che incidono direttamente sul tema. Il primo stabilisce che l'uso dei sistemi di IA nelle professioni intellettuali è finalizzato al solo esercizio delle attività strumentali e di supporto, con prevalenza del lavoro intellettuale oggetto della prestazione d'opera. Il secondo impone al professionista di comunicare al destinatario della prestazione, con linguaggio chiaro, semplice ed esaustivo, le informazioni

relative ai sistemi di IA utilizzati.

Non si tratta di un obbligo meramente formale. La disposizione, letta insieme alla giurisprudenza che si sta consolidando, disegna un modello in cui l'avvocato (ma lo stesso vale per il consulente, l'ingegnere, il commercialista) resta titolare pieno della prestazione intellettuale, e la firma sull'atto vale come assunzione di responsabilità per tutto ciò che è stato prodotto, a prescindere dal fatto che il testo sia stato redatto personalmente, da un collaboratore o da un *Large Language Model*.

Il Consiglio Nazionale Forense ha diffuso un modello di informativa tipo da consegnare al cliente all'atto del mandato, mentre l'Ordine degli Avvocati di Milano aveva anticipato il tema già a dicembre 2024 con la *Carta dei principi per un uso consapevole dei sistemi di intelligenza artificiale in ambito forense* (progetto "Horos"), richiamata per la prima volta in una sentenza proprio dal TAR Lombardia nella pronuncia n. 3348/2025.

A completare il quadro, la Guida del Consiglio degli Ordini Forensi Europei (CCBE, 2 ottobre 2025) ribadisce i doveri di riservatezza, competenza e lealtà, con particolare attenzione al rischio che l'inserimento di dati dei clienti in piattaforme di IA pubbliche violi il segreto professionale.

Shadow AI in azienda: tre livelli di rischio per CISO e compliance

Per chi si occupa di *information security* e *governance* aziendale, la vicenda siracusana è un caso da manuale di *shadow AI*, ossia l'uso di sistemi di intelligenza artificiale al di fuori di qualsiasi policy, autorizzazione o supervisione organizzativa. Il fenomeno presenta tre livelli di rischio concorrenti che la vicenda siracusana illustra perfettamente.

Il primo è il rischio di *output* inaffidabile. Gli *LLM* non consultano una base di conoscenza verificata: producono testo

probabilisticamente plausibile. Ciò vale per le citazioni giurisprudenziali come per le citazioni bibliografiche, i riferimenti normativi, i dati numerici, gli standard tecnici, gli articoli di contratto. In un contesto professionale in cui la sottoscrizione vale come assunzione di paternità, utilizzare un *output* non verificato significa trasferire il rischio di *hallucination* dal modello al professionista.

Il secondo è il rischio di *data leakage*. L'inserimento di dati personali, segreti commerciali, atti processuali, pareri legali, documentazione classificata o credenziali nei *prompt* di sistemi *consumer* comporta, in assenza di garanzie contrattuali adeguate, un potenziale trasferimento illecito *ex* GDPR, un'erosione del segreto professionale e una perdita di controllo sul ciclo di vita dell'informazione (*retention*, *training*, accesso di terzi). Non è un rischio teorico: il Garante italiano ha già avviato procedimenti in materia, e le sanzioni del GDPR possono raggiungere il 4% del fatturato mondiale annuo.

Il terzo è il rischio di *compliance* e *audit trail*. Se un'organizzazione non sa quali strumenti di IA sono usati dai propri professionisti, con quali dati e per quali decisioni, non è in condizione di documentare la formazione del personale, le misure di sicurezza adottate, i processi decisionali. In caso di ispezione, di contenzioso, di *due diligence* M&A, l'assenza di governance sull'IA è un segnale che può compromettere l'operazione e, negli scenari peggiori, aggravare la posizione dell'ente rispetto ai rischi sopra citati.

Governance dell'IA generativa: tre lezioni per studi legali e imprese

Il caso siracusano, letto da una prospettiva di *cybersecurity* e *risk management*, suggerisce tre considerazioni di metodo che valgono ben oltre l'avvocatura.

In primo luogo, il perimetro dell'obbligo di verifica si sta definendo in concreto attraverso la giurisprudenza, non solo attraverso la normativa. Il principio di prevalenza del lavoro intellettuale dell'art. 13 della L. 132/2025 è un'enunciazione programmatica; è nelle pronunce di merito che sta emergendo il contenuto operativo di quell'obbligo. Lo standard minimo, oggi, è: conoscere i limiti degli *LLM*, verificare ogni citazione sulle fonti primarie, tracciare l'uso dell'IA in forma documentabile. L'ignoranza di questo standard non è un'attenuante ma, secondo il Tribunale di Siracusa, un indicatore di colpa grave.

In secondo luogo, la distinzione fra uso individuale e uso organizzativo dell'IA si sta dissolvendo sul piano della responsabilità. Un singolo professionista che usi ChatGPT nel suo studio espone sé stesso, il proprio cliente e, potenzialmente, anche l'organizzazione in cui opera. Per uno studio legale, un ente pubblico, un'impresa regolata, la *shadow AI* non è più un problema IT da delegare al tecnico di fiducia: è un tema di *board*, che coinvolge *legal*, *compliance*, *privacy*, *security*, *procurement*, *HR*, *internal audit*.

In terzo luogo, le misure di mitigazione sono note e non particolarmente esotiche. Censimento degli strumenti effettivamente in uso, classificazione degli usi consentiti e vietati, regole esplicite sui dati che non possono entrare nei *prompt*, valutazione dei fornitori di IA come *critical third parties*, *logging* delle interazioni con sistemi di IA, formazione differenziata per ruoli, gestione degli incidenti *AI-related* come potenziali *data breach*, responsabilizzazione del *management*. Il tutto integrato nei processi già esistenti di sicurezza, protezione dati e conformità NIS2.

La vera lezione della sentenza di Siracusa non riguarda il singolo caso e nemmeno solo l'avvocatura. Riguarda il fatto che, in un ordinamento che sta imparando a qualificare giuridicamente il rischio di *hallucination*, il costo dell'assenza di governance sull'IA generativa sta rapidamente

superando il costo di implementarla. È un passaggio che i *CISO* e i *compliance officer* stanno già osservando in altri settori regolati: la regola ricorrente è che, quando un rischio tecnologico diventa *fatto notorio*, chi non lo ha presidiato paga di più di chi ci aveva investito per tempo.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/sentenza-siracusa-338-2026-ai/

L'AI fatta in Italia, aperta e trasparente di Engineering apprezzata da Ronzulli, Butti, Barachini e Nobile

"AI Italia. L'AI tra innovazione e sovranità digitale", l'iniziativa della Sen. Ronzulli con Engineering al Senato

In un mondo sempre più interconnesso, l'**intelligenza artificiale** (AI) non è solo uno strumento di innovazione, ma il pilastro per una crescita autonoma e competitiva del nostro Paese. Per coglierne appieno il potenziale, però, l'Italia deve puntare con decisione sulla sovranità digitale: sviluppare infrastrutture, talenti e soluzioni proprietarie significa rompere la dipendenza da giganti esteri, garantendo sicurezza, controllo e un vantaggio strategico a livello

competitivo.
A questo è stato dedicato l'evento "***AI Italia. L'AI tra innovazione e sovranità digitale***" che si è tenuto presso la Sala Zuccari di Palazzo Giustiniani a Roma, oggi sede di rappresentanza della presidenza del Senato della Repubblica. Un incontro organizzato su iniziativa della Senatrice **Licia Ronzulli**, in collaborazione con **Engineering**, per dare vita ad un momento di confronto istituzionale e industriale, allargato al mondo accademico, dedicato al ruolo strategico dell'intelligenza artificiale (AI) nello sviluppo del Paese, con un focus sui temi dell'innovazione tecnologica, della competitività del sistema economico e della sovranità digitale, ma soprattutto sulla necessità di sviluppare un modello di intelligenza artificiale tutto italiano.

Tantissimi gli interventi di rappresentanti politici di tutti gli schieramenti, del mondo imprenditoriale e universitario, moderati da **Michelangelo Suigo**, Chief Public Affairs, Corporate Communication & Sustainability Officer di Engineering Group, che hanno affrontato il tema delle condizioni necessarie per costruire una reale sovranità tecnologica, ma anche argomenti chiave come lo sviluppo di infrastrutture nazionali di calcolo e data center, la riduzione della dipendenza da provider extra-europei e il ruolo dell'AI Act e quindi della regolamentazione. L'incontro è stata anche l'occasione per presentare **IS-IA – *Italy's Sovereign Intelligence Architecture***, un approccio architetturale basato sul concetto di Intelligenza Artificiale italiana, governabile e sicura, basato su **EngGPT 2**, piattaforma italiana di *Private Generative AI* sviluppata da Engineering.



Sen. Ronzulli: “Dobbiamo favorire investimenti nazionali, lavorare ad una regolamentazione europea più smart e accelerare sulla formazione”

Ad aprire l’incontro è stata proprio la Vicepresidente del Senato della Repubblica, **Licia Ronzulli**, che ha affermato: “*Una tecnologia che non possiamo subire ma che dobbiamo governare. Questa tecnologia non è neutrale, può salvare vite o minacciare la libertà, creare lavoro o generare esclusione, sta a noi decidere come usarla al meglio. Per questo oggi è fondamentale parlare di AI tra innovazione e sovranità digitale. Dobbiamo sfruttare questa tecnologia senza perdere il controllo e la sovranità. Non dobbiamo diventare dipendenti*

da chi fornisce questa tecnologia. Può ridurre disuguaglianze tra Nord e Sud del Paese, può migliorare i servizi sanitari, ma il controllo dei dati è fondamentale".

"L'AI può ridurre gli sprechi delle fabbriche intelligenti, ma gli algoritmi che controllano i processi sono sviluppati altrove. Si stima che sia in grado di generare 15 trilioni di dollari di PIL fino al 2030, ma oggi il 90% die modelli di AI sono dominati da Stati Uniti e Cina, motivo per cui Europa e Italia rischiano di diventare una colonia digitale. La sovranità non è un lusso, ma una necessità strategica. Dobbiamo agire su 3 pilastri – ha precisato Ronzulli – *il primo sono gli investimenti nazionali, potenziando il supercomputer Leonardo, il Gaia di Bologna e il supercalcolatore di Napoli. L'Italia ha bisogno di implementare il Polo strategico nazionale per creare un'IA al 100% made in Italy, addestrata sui nostri dati sanitari, aziendali e culturali, che pensi in italiano e sia ospitata in data center nazionali per evitare fughe di dati sensibili all'estero. Il secondo pilastro è l'Europa, che necessita di una regolamentazione smart. Da una parte abbiamo l'AI Act con oltre 300 pagine, un mattone burocratico che rischia di frenare ogni reazione rapida, dall'altra paesi come il Giappone, dove l'autoregolamentazione delle aziende fa volare l'innovazione. Regolamentare è giusto, ma la burocrazia europea non può essere la zavorra che affonda il futuro dell'Italia. Il terzo pilastro è la formazione e il lavoro. Molti temono che l'AI porti via il lavoro, in alcune professioni purtroppo sarà così, ma allo stesso tempo incrementerà tantissimo la produttività, generando si stima 97 milioni di nuovi lavori globali entro il 2027. Fondamentale* – ha sottolineato Ronzulli – *è che l'essere umano sia sempre al centro, con le sue competenze e la sua intelligenza. Dobbiamo trattenere i cervelli italiani, altrimenti non ci sarà né innovazione, né crescita. E oggi la vera competizione globale non è solo sulle tecnologie, ma sulle persone. Per questo serve un cambio di passo: investire seriamente in formazione,*

creare condizioni di lavoro competitive, sostenere ricerca e università e costruire un ecosistema in cui i giovani possano scegliere di restare e crescere in Italia”.



Barachini: “Più saremo sovrani dei nostri dati, più saremo liberi”

“*Siamo allo stesso tempo potentissimi e fragilissimi. Sono stati bombardati dei data center nel Bahrein e negli Emirati Arabi, ci sono stati problemi per alcune Big Tech. Con la vicepresidente del Senato Licia Ronzulli eravamo a Valencia nel momento del blackout e tanti servizi non erano più disponibili. C’è stato un giudice della Corte penale internazionale la cui presenza digitale è stata spenta dagli Stati Uniti. Stiamo pattinando su un ghiaccio sottile, che è la nostra democrazia*”, ha dichiarato **Alberto Barachini**, Sottosegretario alla Presidenza del Consiglio dei

Ministri all'Informazione e all'Editoria. "*Più saremo liberi e indipendenti dal possesso dei dati, più saremo liberi da punto di vista democratico. Ci sono state diverse iniziative, come la legge sull'intelligenza artificiale, ed è stato positivo l'intervento della presidente della Commissione europea, Ursula von der Leyen, sulle gigafactory* – ha aggiunto Barachini – *ma abbiamo bisogno che gli studiosi vengano supportati perché le loro invenzioni abbiano sviluppo sul mercato. L'indipendenza digitale è un tema esponenziale, più saremo sovrani dei nostri dati, più saremo liberi democraticamente. I tentativi tedeschi e francesi sono positivi, in questo senso, ma dobbiamo evitare l'iper-regolamentazione e allo stesso tempo ridurre la tecno-dipendenza*".

L'ammiraglio **Andrea Billet,** capo del Servizio Certificazione e Vigilanza dell'Agenzia per la cybersicurezza nazionale (Acn), ha approfondito il legame sempre più stretto tra intelligenza artificiale e cybersecurity. L'attenzione è stata posta sulla necessità di integrare tecnologie avanzate con una solida cultura digitale, in grado di sostenere cittadini e organizzazioni: "*La sovranità digitale passa innanzitutto dalla riduzione della dipendenza da forniture estere. Parliamo di data center, chip, terre rare per quanto riguarda le infrastrutture; ma anche di servizi, come il cloud, che raggiungono gli utenti attraverso le reti di comunicazione. A questo si aggiungono le applicazioni di intelligenza artificiale, dove la scala è un fattore determinante: non avere la capacità di sviluppare modelli propri comporta inevitabilmente dei costi e delle vulnerabilità. Non si può parlare di sovranità tecnologica senza conoscere e presidiare l'intera pila tecnologica, cercando di costruire una reale autonomia. È un tema che riguarda anche l'energia. La scala, infatti, è fondamentale, e per affrontare questa sfida sono necessari partenariati molto ampi, coinvolgendo anche il settore privato. Un esempio concreto arriva dal nuovo modello Mythos* – ha proseguito Billet – *che ha individuato*

vulnerabilità sconosciute anche in sistemi ritenuti sicuri, generando una forte preoccupazione a livello globale, inclusi gli Stati Uniti, tanto che il prodotto non è stato immediatamente immesso sul mercato. Secondo Anthropic, entro 18 mesi altri operatori raggiungeranno le stesse capacità, con il rischio che questi strumenti possano finire nelle mani sbagliate. In questo contesto si inserisce il progetto Glasswing, avviato da Anthropic per individuare vulnerabilità nei software critici, con l'obiettivo di prevenire scenari peggiori. L'iniziativa punta a mettere insieme i principali operatori del settore, insieme anche a grandi istituzioni finanziarie americane, particolarmente esposte alle minacce cyber. Oggi si registra uno sbilanciamento a favore delle capacità offensive dell'intelligenza artificiale rispetto a quelle difensive. La domanda è quindi come muoversi in questo scenario. Per contrastare queste minacce servono soluzioni controllabili e governabili. Le dipendenze da fornitori esteri, in questo senso, possono rappresentare un ulteriore elemento di rischio. L'Agenzia sta lavorando per reclutare esperti di intelligenza artificiale entro l'estate, con l'obiettivo di metterli subito al lavoro nello sviluppo di soluzioni avanzate basate sull'AI. Parallelamente, stiamo sostenendo la candidatura italiana per ospitare una gigafactory avanzata".



Bisio (Engineering): “Un’AI sovrana dichiara su quali dati è stata addestrata ed è ispezionabile, anche dai cittadini”

Nel suo intervento dal titolo “*Sovereign AI Architecture*“, il CEO di Engineering Group, **Aldo Bisio**, ha spiegato che “*un sistema AI sovrano dichiara su quali dati è stato addestrato e i parametri che determinano i comportamenti, e può essere ispezionato, anche dai cittadini*”.
Riguardo l’intelligenza artificiale sovrana, Bisio ha illustrato le tre condizioni fondamentali: “*chiarezza e piena trasparenza sui dati, dati di addestramento e capacità di essere trasparente*”.

“*L’intelligenza sovrana è, in sostanza, un’intelligenza artificiale governata* – ha aggiunto Bisio – *mira a evitare la dispersione del patrimonio cognitivo di aziende o istituzioni.*

In termini semplici: l'intelligenza artificiale assorbe dati e apprende da questi. Se qualcun altro, dopo di voi, accede allo stesso modello, finisce per nutrirsi e arricchirsi del vostro know-how e del vostro patrimonio cognitivo. È quindi fondamentale che l'AI riesca a mantenere al proprio interno il nucleo informativo di un'azienda o di un'istituzione, senza condividerlo con concorrenti o soggetti non desiderati. Questo rappresenta un vantaggio competitivo rilevante. L'altro tema che stiamo affrontando è quello della trasparenza, ciò che tecnicamente viene definito "open weights". I pesi sono i parametri numerici attraverso cui funziona questa gigantesca funzione dell'intelligenza artificiale. Il problema è che, tipicamente, i grandi modelli sono delle scatole nere: si conoscono gli input, si conoscono gli output, ma non è chiaro perché venga presa una determinata decisione o fornita una certa risposta. Avere "open weights" significa disporre di un controllo completo su tutti i dati, rispondendo così a questa seconda grande esigenza. C'è poi una questione di proporzionalità nell'uso dell'intelligenza rispetto alla dimensione e alla complessità dei problemi da affrontare. I modelli molto grandi consumano molta energia – ha precisato il CEO di Engineering – *alcuni possono essere utilizzati per risolvere determinate problematiche, altri invece dovrebbero essere impiegati per compiti molto più specializzati, con un consumo energetico e un'intensità decisamente inferiori. Non significa che non sia opportuno utilizzare modelli di grandi dimensioni, ma che questi vadano impiegati solo quando necessario. Ad esempio, quando non vi è un patrimonio cognitivo o una proprietà intellettuale da difendere. Se invece il know-how di un'azienda o di un'istituzione, oppure i dati di clienti e cittadini sono a rischio, è meglio adottare un approccio più prudente*".

"*Non voglio dire che non sia opportuno usare i grandi modelli, ma che bisogna usarli solo quando è il caso, quindi, ad esempio, quando non c'è un patrimonio cognitivo o un intellectual property da difendere, se è a rischio il know how*

di un’azienda, di un’istituzione, i dati di clienti o di cittadini è meglio fare attenzione. La nuova architettura lanciata dal progetto – ha spiegato Bisio – *riempie il bisogno delle imprese di dare risposta a quelle sfide di cui vi stiamo parlando. Crediamo di aver sviluppato tramite questa progettazione un large model, e su questa base abbiamo poi costruito tutta una struttura che in qualche modo aiuta le aziende o le istituzioni a costruire gli agenti, a dare perfetta visibilità sulla compliance, per cui il modello e tutta l’architettura è nativamente compliant con il Gen Ai Act europeo, intendiamo in questo modo dare una risposta a tutte queste esigenze*”.

“*Sicuramente l’attenzione deve ricadere sul tema legato alla protezione della proprietà intellettuale* – ha infine sottolineato Bisio – *e sull’evoluzione, per esempio, della normativa sui data leaks, sia per quanto riguarda l’accesso ai modelli di Ai sia per la protezione; un secondo tema riguarda chi fa le regole. I modelli devono essere perfettamente ispezionabili in hand to hand quindi non devono essere solo chiari i parametri del modello stesso, ma devono essere chiari e aperti anche i dati di training su cui è stato allenato quel modello perché in funzione dei dati acquisisce determinati modi di pensare certi comportamenti”. “Non si tratta solo di governare la meccanica del modello ma anche il suo tipo di comportamento. Bisogna definire questo set di regole e confortare chi le utilizzerà e chi sarà oggetto delle decisioni di queste macchine*”.



Pastorella: “Non bastano le regole, è necessario creare le condizioni affinché queste tecnologie vengano effettivamente utilizzate”

La Capogruppo di Azione alla Commissione Trasporti, Poste e TLC Camera dei Deputati, On. **Giulia Pastorella**, ha aperto la prima tavola rotonda dal titolo “*AI sovrana, sicura e sostenibile*“, sostenendo che “*lo sviluppo di un LLM italiano rappresenta uno dei pilastri della strategia nazionale sull’intelligenza artificiale, e il modello che viene presentato si inserisce pienamente in questa direzione, contribuendo all’attuazione di un obiettivo chiave: favorire l’adozione e la diffusione della tecnologia, stimolando al tempo stesso sia l’offerta sia la domanda. Non bastano le*

regole: è necessario creare le condizioni affinché queste tecnologie vengano effettivamente utilizzate. L'iniziativa è infatti orientata sia alla pubblica amministrazione sia al tessuto produttivo, con un approccio che si allontana dalla logica dei grandi modelli generativi, spesso critici sotto il profilo della privacy e della sicurezza. In questo scenario, i data center restano un elemento fondamentale, ma assume un ruolo sempre più centrale l'edge cloud, dimensionato in modo coerente con le specificità dei territori e con le reali esigenze delle imprese. Per sostenere questo ecosistema servono infrastrutture adeguate: connettività e disponibilità energetica. La sovranità digitale, inoltre, non può limitarsi alla semplice localizzazione dei dati. È necessario puntare con decisione sulla trasparenza dei sistemi, elemento imprescindibile per costruire fiducia e garantire sicurezza".

"*Il tema dell'energia e dell'autonomia strategica in questo settore sono argomenti chiave che ci fanno ragionare anche sull'AI. dal punto di vista del mercato non possiamo raggiungere gli LLM americani e cinesi, perché investono molto di più e investono ancor prima miliardi sulle loro startup. Modelli come quello di Engineering possono funzionare perché possiamo declinare queste tecnologie sulle nostre filiere, come quella dell'aerospazio, dei servizi, dei software e delle app. capacità computazioni e di calcolo non ci mancano, abbiamo supercomputer sul territorio nazionale. La partita è aperta perché quasi all'inizio, possiamo giocarcela, ma a certe condizioni. C'è chi sta pensando anche agli small language models, una nuova forma, perché possiamo utilizzare quelle tecnologie e declinarle sulle nostre filiere. In Italia, per esempio, abbiamo una filiera dell'aerospazio che è più completa rispetto anche a quella degli altri grossi player europei. Ecco quindi che quelle tecnologie possiamo declinarle qui: possiamo diventare una powerhouse per quanto riguarda la costruzione di servizi, software e applicazioni. L'altro angolo sotto cui possiamo vedere il nostro possibile vantaggio competitivo è la capacità computazionale e di calcolo. Licia*

Ronzulli, in apertura, parlava di supercalcolatori e quantum computing: quello può essere il nostro ambito. Possiamo cominciare a svilupparci da lì, la partita è aperta, è quasi all'inizio e possiamo giocarcela", ha dichiarato l'On. **Giulio Centemero**, Componente Lega della Commissione Finanze Camera dei Deputati. Ù

Basso: "La priorità è la formazione, il vero nodo resta la diffusione capillare delle competenze a livello sociale"

"*Nel libro Il Secolo dell'AI invito i cittadini a sviluppare una maggiore consapevolezza nell'utilizzo di queste tecnologie, con l'obiettivo di migliorare la qualità della vita senza metterla a rischio. È fondamentale comprendere quando e come regolamentare, così come quando e in che modo utilizzare questi strumenti, per salvaguardare le libertà individuali e il know-how delle imprese. Riuscire a spiegare il funzionamento dell'intelligenza artificiale è alla base di un uso proporzionato e responsabile della tecnologia. L'AI ha un impatto su società ed economia persino superiore a quello avuto dall'elettricità e da altre grandi innovazioni del passato, perché rappresenta un abilitatore trasversale dei cambiamenti tecnologici futuri, dalla computazione quantistica alle neuroscienze, fino alla robotica umanoide. La priorità, dunque, è la formazione. Il nostro Paese dispone di eccellenze di primo piano in questo ambito, ma il vero nodo resta la diffusione capillare delle competenze a livello sociale, necessaria per promuovere un uso più responsabile e consapevole dell'intelligenza artificiale*", ha affermato il Sen. **Lorenzo Basso**, Componente PD della Commissione Ambiente Senato della Repubblica.

"*Nelle aree più marginali, dove la presenza dello Stato e dei*

servizi è più debole – dagli ospedali ai trasporti fino alle scuole – si tende a dimenticare che tra le infrastrutture critiche rientrano anche le reti digitali, attraverso cui transitano i flussi informativi. Dobbiamo considerare l'intelligenza artificiale come una grande opportunità, ma è necessario governarla, non subirla. Questo significa, innanzitutto, avere il controllo dei dati, che rappresentano una leva competitiva e al tempo stesso democratica. Lo Stato, quindi, deve essere in grado di proteggere efficacemente il proprio patrimonio informativo", ha ricordato il Sen. **Guido Liris**, Capogruppo FdI nella Commissione Bilancio Senato della Repubblica.



La seconda tavola rotonda dal titolo "*AI everywhere: le applicazioni dell'AI nei verticali di mercato*", è stata aperta dalla Professoressa Ordinaria di Computer Science all'Università Milano-Bicocca, **Stefania Bandini**, che ha detto: "*L'intelligenza artificiale è ormai pervasiva, ma è con l'avvento dell'AI generativa che si è verificato un vero cambio di paradigma. Oggi più che mai è fondamentale*

riconoscere il valore della sperimentazione, che rappresenta il primo passo verso un'adozione consapevole e strategica di queste tecnologie. In Italia esiste già una forma diffusa di sperimentazione "di base", che coinvolge cittadini, imprese e pubbliche amministrazioni. Tuttavia, questa pratica deve essere maggiormente valorizzata e strutturata, trasformandosi in progettualità concreta e in innovazione sistemica. C'è infatti un livello di sperimentazione di cui spesso non si ha piena consapevolezza, un patrimonio diffuso ancora in gran parte inesplorato. È proprio da qui che bisogna partire: riconoscere, mettere a sistema e far crescere queste esperienze, collegandole a una visione più ampia che tenga insieme sviluppo tecnologico, sovranità digitale, sicurezza e sostenibilità. Solo così la sperimentazione potrà diventare un vero motore di innovazione e competitività per il Paese".

Momola (Engineering): "EngGPT 2 assicura una riduzione dei consumi che può arrivare dal 60% all'80% in meno rispetto a un modello su larga scala"

Più tecnico è stato l'intervento di **Fabio Momola**, EVP ENG Digital di Engineering Group, considerato assieme a Bisio l'artefice di EngGPT 2: "*Con IS-IA, l'architettura di intelligenza sovrana italiana, proponiamo un sistema aperto che consente di integrare modelli provenienti da diverse fonti, governando al contempo l'intero flusso di utilizzo delle API associate a tali modelli. Grazie a questo approccio, è possibile raggiungere la redditività in tempi rapidi: entro un massimo di 12-18 mesi. Per quanto riguarda la sostenibilità, si tratta di una questione fondamentale quando si parla di intelligenza artificiale. Se consideriamo che i grandi modelli americani consumano, nella sola fase di*

addestramento, quanto decine di famiglie europee in un anno, comprendiamo quanto sia cruciale affrontare questo problema. Soprattutto quando le fonti energetiche utilizzate provengono dal carbone o, più in generale, da combustibili fossili. In questo contesto, EngGPT2 cerca di offrire una soluzione, essendo basato su un'architettura "Mixture of Experts", capace di garantire consumi molto più bassi nella fase di utilizzo, l'inference, rispetto alla media dei modelli esistenti quando il sistema è chiamato a svolgere un compito. Parliamo di una riduzione dei consumi che può arrivare dal 60% all'80% in meno rispetto a un modello su larga scala. Infine, soffermandosi sugli effetti dell'AI Act, la mia posizione è chiara: la legislazione non ha mai bloccato l'evoluzione; al contrario, rappresenta un ostacolo solo per chi non si mette nelle condizioni di sfruttarla per innovare meglio. Credo che, con la nostra architettura Is-Ia e con EngGPT 2, ci siamo messi nelle condizioni di considerare l'AI Act come un acceleratore dell'innovazione, e non come un freno per noi, per l'Italia e per l'Europa nel suo complesso".

"*L'università opera su più livelli – famiglie, studenti e stakeholder – e si trova oggi ad affrontare una duplice sfida: intervenire sia sui contenuti sia sui metodi, perché è in atto una trasformazione profonda del modo di insegnare e apprendere. Si dice spesso che l'intelligenza artificiale sostituisca il pensiero critico, ma il tema è più complesso. L'AI, in realtà, agisce come un amplificatore per chi ha già sviluppato capacità critiche. È quindi fondamentale distinguere tra performance e apprendimento: nel primo caso l'AI può essere estremamente efficace, mentre nel secondo può rappresentare un rischio, se utilizzata in modo passivo. Una delle sfide principali è stata introdurre l'intelligenza artificiale in tutti i percorsi di studio. La formazione è lenta? Forse, ma va ricordato che si muove all'interno di sistemi regolati e strutturati per discipline. Proprio per questo, la vera sfida è innanzitutto pedagogica. Dobbiamo costruire uno spazio in cui l'essere umano resti centrale.*

L'AI, in ambito universitario, deve diventare soprattutto uno strumento di riflessione, più che di semplice produzione. In questo senso, la sovranità non è solo tecnologica o digitale, ma anche cognitiva: un valore che non può essere disperso né delegato", ha detto invece **Enzo Peruffo**, Pro Rettore e Professore Ordinario di Strategie d'Impresa della Luiss.

Donatella Proto, Direttore Generale Nuove Tecnologie Abilitanti Mimit, ha affermato che "*il vero punto di forza risiede nella differenziazione: nella capacità di valorizzare dati di qualità e la lingua italiana per sostenere concretamente le filiere produttive del Paese, che esprimono esigenze profondamente diverse tra loro. È in questa direzione che devono svilupparsi strumenti di intelligenza artificiale sempre più verticali, capaci di tenere conto delle specificità dei singoli settori e di rispettare l'identità del patrimonio imprenditoriale e industriale italiano*".
"*Servono modelli modulari, trasparenti e scalabili, in grado di generare fiducia e consapevolezza nelle imprese rispetto al loro utilizzo. Oggi, tuttavia* – ha aggiunto Proto – *le PMI non hanno ancora sviluppato appieno le competenze necessarie per affrontare l'adozione di sistemi di AI. Esiste un evidente problema di formazione, ma anche di accompagnamento: non bastano incentivi economici, è necessario supportare le imprese lungo tutto il percorso di integrazione di queste tecnologie. Parallelamente, bisogna lavorare alla costruzione di un vero ecosistema industriale abilitante, capace di accogliere e sviluppare l'innovazione. Un processo che richiede uno sforzo trasversale, che coinvolga università, istituzioni e sistema produttivo, chiamati a comprendere come l'intelligenza artificiale sia ormai uno strumento imprescindibile per la produttività e la resilienza del tessuto economico nazionale. È necessario superare le dipendenze di mercato e compiere un salto culturale, mettendo le imprese nelle condizioni di governare l'innovazione, anziché subirla. In questo senso, la sovranità non è solo una questione tecnologica, ma anche la capacità di affrontare e*

guidare il cambiamento che il nostro tempo impone”.



Nobile: “Un’AI sovrana per far emergere i talenti nazionali”

Mario Nobile, direttore Generale dell’Agenzia per l’Italia Digitale (Agid), ha affrontato il tema delle politiche pubbliche necessarie a sostenere lo sviluppo dell’AI in Italia. Il focus è sull’equilibrio tra regolamentazione e innovazione, con particolare attenzione al rischio di over-regulation e alla frammentazione normativa europea. L’intervento approfondisce la necessità di passare da un approccio prevalentemente prescrittivo a modelli più agili, capaci di accompagnare la crescita tecnologica senza comprometterne la competitività, mantenendo al tempo stesso elevati standard di sicurezza e tutela dei dati.
“*Il modello di LLM sovrano proposto da Eng rappresenta un*

passaggio importante, anche per la sua capacità di far emergere e valorizzare i talenti, un aspetto che ritroviamo chiaramente anche nelle linee guida attualmente in consultazione. Abbiamo parlato di sovranità cognitiva – ha precisato Nobile – *un concetto che si fonda su consapevolezza e competenze. Ma questa riflessione va inserita all'interno dell'intera pila tecnologica, che oggi comprende data center, infrastrutture, applicazioni e servizi. La domanda, quindi, è strategica: qual è la nostra visione in termini di energia, semiconduttori, infrastrutture e servizi? A livello europeo, la politica ha compreso la necessità di intervenire, come dimostra l'AI Act, mentre l'Italia ha promosso una propria iniziativa normativa. Il punto ora è capire come integrare in modo efficace le autorità pubbliche con il mondo delle imprese e quello accademico, costruendo un percorso condiviso. Come AgID faremo la nostra parte per intercettare e coinvolgere l'intero ecosistema. In questo contesto, Eng rappresenta già oggi un passo avanti concreto verso la sovranità cognitiva. L'obiettivo è crescere insieme, individuando le traiettorie più efficaci e contribuendo a orientare le politiche pubbliche verso una strada certamente più lunga e complessa, ma necessaria per ricomporre tutti gli elementi della sovranità tecnologica*".

Butti: "*Uno Stato è tecnologicamente sovrano se fa un uso attento della risorsa più importante che è il dato*"

Le conclusioni sono state affidate al Sen. **Alessio Butti**, Sottosegretario alla Presidenza del Consiglio dei Ministri all'Innovazione Tecnologica e Transizione Digitale. "Sul tema della regolamentazione dell'intelligenza artificiale ritengo che non solo gli hyperscalers e le Big Tech si siano adeguati sostanzialmente al Gdpr, ma si siano adeguati anche

all’AI Act. Tutti, a eccezione di Meta, hanno fatto la fila per siglare i codici di condotta a Bruxelles”, ha dichiarato Butti.

“*È il risultato di un grande lavoro svolto anche dal Governo italiano, ma soprattutto dalla Commissione Europea. A proposito di scenario europeo, l’ingegner Nobile ha ricordato il lavoro dell’Edic, il Consorzio per un’infrastruttura digitale europea. Non solo noi abbiamo indicato l’Edic, ma ne abbiamo scritto anche il programma, raccogliendo l’adesione immediata di alcuni degli Stati e delle imprese più importanti. Esprimiamo la vicepresidenza esecutiva di questo importante contesto tecnico europeo e non ci limitiamo esclusivamente a questo, poiché stiamo lavorando su una serie di altre per noi importanti questioni. L’AI di Eng è un servizio on demand e certamente anche tecnicamente è accessibile e semplice che guarda al futuro. Uno Stato è tecnologicamente sovrano se fa un uso attento della risorsa più importante che è il dato, ma anche se garantisce la sicurezza delle proprie infrastrutture per consentire uno scambio di dati in sicurezza. Un ecosistema intelligente vive di dati calcolo e energia e anche di infrastrutture e filiere produttive, anche in condizioni di scarsa adozione da parte delle piccole imprese. Oggi il dato sta migliorando*”, ha proseguito Butti.



"A proposito di dipendenza quando un Paese usa modelli, strutture e capacità di calcolo progettate altrove, si intravede inevitabilmente un rischio di dipendenza e di lock-in. Questa non è solo una tragedia per il mondo economico del Paese, ma lo è anche per chi, come questo Governo, rivendica fortemente un concetto di sovranità digitale e tecnologica, ed è un rischio per tutta la filiera di imprese che dipendono da questo concetto di sovranità. Noi abbiamo settori assolutamente strategici, come la sanità, i trasporti e la manifattura, che fanno un uso importante dell'IA, e abbiamo voluto consentire loro di avere qualche garanzia in più rispetto a quelle già offerte dall'AI act e dal mercato. Non è stato un atto di presunzione o supponenza: abbiamo voluto dotare il Paese di una legge nazionale sull'IA coerente con i principi tecnici dell'AI Act, ma che dedicasse grande attenzione a quella filiera manifatturiera che non ha eguali a livello europeo. Se continuiamo a ripetere che non ha eguali, dobbiamo valorizzarla, proteggerla e cullarla; è ciò che

stiamo facendo con questa legge, che ha una governance solida. La tecnologia è una questione trasversale alle forze politiche – ha sottolineato Butti – *ma abbiamo voluto raccogliere tutti i contributi dal mondo parlamentare, industriale, universitario e imprenditoriale. Abbiamo messo un miliardo di euro di risorse pubbliche che agisce come volano per gli investimenti privati che sono in aumento. Un altro sviluppo che stiamo impostando prevede una grande attenzione per la valorizzazione del territorio, senza la quale le cose raccontate finora non avrebbero senso. Per questo, abbiamo recentemente promosso Reg4AI e finanziato, come dipartimento per la Trasformazione digitale, 4 grandi progetti che riguardano le filiere della sanità, del turismo, dei trasporti e della pubblica amministrazione. Abbiamo coinvolto le Regioni e le società in house. La settimana scorsa, a un tavolo tecnico di confronto con Assinter, abbiamo colto la positività e la concretezza del nostro lavoro, fondato sulla collaborazione continua e costante con il territorio. L'obiettivo di Reg4AI è creare le migliori pratiche che, in seguito, dovranno essere estese e scalate a livello nazionale*".

"*Nella PA abbiamo 400 progetti di AI previsti per il 2026 previsti dalle Linee guida dell'Agenzia digitale per promuovere l'adozione dell'AI nella Pubblica amministrazione, vuol dire che sta maturando grazie ad una guida politica che ha una visione chiara orientata a modelli di AI ispezionabili e aperti. Questo vale per la Pa e le imprese e la dimostrazione di questa impostazione è proprio il modello di AI lanciato da Engineering. Non c'è solo Leonardo ma c'è molto altro che sta emergendo dalla strategia del Quantum che abbiamo rilasciato assieme all'Europa. Dall'incontro con la Virkkunen, in occasione delle celebrazioni di Alessandro Volta, nasce un centro di sviluppo per AI e quantum che accoglierà anche le imprese, anche europee, dando vita alla Quantum Alliance. La Camera sta discutendo sul disegno di legge delega sull'Energia, che prevede la realizzazione degli*

SMR, che consentano la sostenibilità dei data center e delle infrastrutture tecnologiche avanzate. Entro l'estate avremo il disegno di legge delega sull'energia come ha dichiarato il ministro Pichetto Fratin. L'AI arriverà a svilupparsi anche nello Spazio. C'è chi già ci sta lavorando. La legge che governa lo Spazio è del 1967, un tempo in cui i privati non agivano nello Spazio. Un Paese in raccordo agli altri Stati dovrebbe raggiungere un minimo comun denominatore per capire a chi spetti la gestione di un certo livello dello Spazio, serve l'intervento pubblico in questo settore così strategico", ha concluso Butti.

Per approfondire in modo tecnico: la scheda dell'AI di Engineering

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/lai-italiana-aperta-e-trasparente-di-engineering-apprezzata-da-ronzulli-butti-barachini-e-nobile/570597/