PRIVATE AI

COMPETITIVITÀ, SICUREZZA E SOVRANITÀ PER LE AZIENDE

seeweb | Istituto EuropIA.it
Comprendere per Agire

Private AI: competitività, sicurezza e sovranità per le aziende

I vantaggi dell’efficacia della Private AI per le aziende del Made in Italy nel contesto competitivo globale e come sviluppare competenze e infrastrutture per lo sviluppo industriale

Prefazione

Quale AI per lo sviluppo economico delle aziende italiane e dell'intero Sistema Paese?

L'AI è ormai assodato essere diventato un motore potente per lo sviluppo futuro dell'economia e anche le aziende italiane si stanno muovendo per integrare sistemi di automazione e di gestione dei processi, produttivi e decisionali, governati dall'intelligenza artificiale. Urge sviluppare competenze e infrastrutture a livello nazionale ed europeo in grado di far fronte all'egemonia degli hyperscaler internazionali, le cui AI si alimentano di dati e informazioni per le quali spesso non viene garantita la tutela e la privacy che invece normative locali ed europee esigono. I vantaggi di una Private AI, alimentata con i propri dati, per i propri scopi, i cui benefici vengano unicamente a chi la coltiva e utilizza, che valorizzi le peculiarità di prodotto, di creatività, di contesto di mercato, sono innumerevoli.

Al pari dei pericoli nascosti nell'affidarsi a operatori globali, che vanno dal lock in tecnologico ai costi nascosti, fino alla sicurezza.

In questo documento abbiamo cercato di fornire degli spunti di riflessione su quanto sia necessario e urgente, per le aziende del Made in Italy, appropriarsi di tecnologie basate su AI che vivono grazie ai dati che loro stesse forniscono. E godere dei risultati per fare fronte al contesto competitivo globale.

Gentile Lettore,

l’intelligenza artificiale ha smesso da tempo di essere relegata al dibattito puramente scientifico ed è ormai entrata in molti processi industriali della nostra economia: l’interesse crescente verso tale tecnologia sollecita l’attenzione dei mercati e spinge le aziende a toccarne con mano i benefici.

I rischi nel tempo abbiamo imparato a conoscerli e possiamo dire che c’è una diffusa consapevolezza delle diverse dinamiche che intervengono nella trasformazione digitale dei processi produttivi guidati dall’AI.

Abbiamo ormai compreso che le macchine possono addestrarsi autonomamente e fornire risultati *plausibili* sulla base delle esperienze passate. E questo ha aperto immediatamente la via a fattori di compliance normativa, soprattutto europea, per la protezione dei dati personali e non personali, segnatamente quelli aziendali perché rappresentano un valore distintivo delle imprese nei settori avanzati e per la ricerca.

Ora è chiaro che se abbiamo pensato a uno studio specifico sull’intelligenza artificiale privata, oltre ai molti già esistenti, è perché pensiamo che sia **necessario evidenziare i vantaggi dell'utilizzo della Private AI nelle aziende italiane** rispetto a soluzioni di AI pubblica, offerte su scala globale da operatori extraeuropei. Saranno così individuati i diversi benefici in termini di sicurezza dei dati, per la sovranità digitale e la conformità normativa, soprattutto in relazione al GDPR e all’AI Act.

Ma questo studio propone qualcosa di più al lettore attento, ovvero un percorso per l'implementazione *concreta* di una Private AI che sottolinei **l'importanza di preservare il know-how italiano in diversi settori produttivi,** con due principali vantaggi: la riduzione del rischio di **condivisione involontaria dei dati all’esterno, e l’indipendenza dalle piattaforme globali**, con il risultato di un maggiore controllo dei dati ma anche dei costi dell’adozione e dell’uso dell’AI in azienda.

L’AI ci accompagnerà in questi prossimi tempi, continuando a chiederci dati: la quantità di informazioni disponibili è, infatti, cruciale per i modelli. Spesso, una *quantità* che è ancora più importante della qualità.

Al momento, c’è un delicato equilibrio che lega GDPR e AI Act di cui bisogna tenere conto. Il GDPR, con il suo principio di minimizzazione dei dati, offre **una cornice solida di protezione della privacy**, mentre l'AI Act mira a regolamentare lo sviluppo dell'intelligenza artificiale in base al *livello di rischio*. L’unico modo per conciliare questi due aspetti è permettere alle organizzazioni di *mantenere il controllo sui dati*, personalizzando i modelli di intelligenza artificiale in base alle proprie esigenze e garantendo un elevato livello di sicurezza.

Raccogliere solo i dati necessari e non condividerli con gli operatori globali che propongono le loro soluzioni di Intelligenza Artificiale non equivale a limitare le capacità innovativa delle aziende, bensì a **garantire che i dati utilizzati siano pertinenti e di alta qualità, con risultati più accurati e affidabili** e che il loro valore non sfugga al perimetro dell'impresa che investe capitale di rischio, ricerca e innova. Ci aiuterà fare qualche esempio.

La Private AI può essere utilizzata per analizzare grandi volumi di dati clinici e genetici in modo sicuro, supportando lo sviluppo di nuovi farmaci e trattamenti personalizzati. La capacità di creare modelli di machine learning su misura, ottimizzati per le esigenze specifiche dell'azienda, permette di ottenere risultati più precisi e rilevanti rispetto ai modelli generici offerti dai player globali, proteggendo le proprie scoperte e i dati di ricerca più sensibili, come i risultati delle sperimentazioni ed i modelli di previsione elaborati con l'AI.

Tutto questo è chiaramente importante per preservare e custodire il vantaggio competitivo e il valore dell'innovazione, ma è necessario un impegno più forte e congiunto da parte delle imprese, dei governi e delle istituzioni per **garantire la crescita di un ecosistema nazionale che promuova lo sviluppo di competenze e di infrastrutture cloud di operatori locali** per favorire l'adozione più rapida e diffusa di questa tecnologia.

In questo documento, spieghiamo attraverso vari passaggi come l'intelligenza artificiale privata sia la vera strada per un'innovazione competitiva, sicura e a garanzia della sovranità dei dati aziendali.

Antonio Baldassarra
CEO Seeweb

Indice:

1. La rivoluzione dell’AI e il ruolo centrale per le aziende e la Pubblica Amministrazione

Dalla meccanizzazione alla produzione di massa, dall'elettronica all'intelligenza artificiale: l'umanità ha attraversato quattro grandi rivoluzioni industriali, ognuna segnata da innovazioni tecnologiche che hanno trasformato radicalmente il modo di vivere e lavorare. Oggi l'intelligenza artificiale con la sua capacità di apprendere e adattarsi, sta letteralmente rivoluzionando il modo in cui produciamo, consumiamo e interagiamo e si pone come il motore della prossima rivoluzione, promettendo di ridefinire ancora una volta il nostro mondo. E lo sta facendo a grande velocità.

Siamo, quindi, all'alba di un nuovo grande cambiamento dove, in un contesto in cui ogni bit di informazione può essere trasformato in valore, l'AI sta riscrivendo le regole del gioco per l'industria, la Pubblica Amministrazione, fino ad arrivare al singolo individuo. Non è solo una questione di efficienza o innovazione: è una trasformazione radicale che sta ridefinendo ciò che è possibile fare e ottenere, puntando a obiettivi fino a poco, pochissimo tempo fa, impensabili. Mentre le macchine imparano, prevedono e decidono, siamo testimoni e attori allo stesso tempo della nascita di un nuovo paradigma operativo, dove il confine tra umano e digitale si fa sempre più sottile e le opportunità diventano infinite.

L'intelligenza artificiale sta trasformando radicalmente il modo in cui aziende private e Pubbliche Amministrazioni operano, ridefinendo processi, modelli di business e servizi. La vera rivoluzione che l’AI sta introducendo in questi contesti è caratterizzata da un aumento esponenziale della capacità delle macchine di eseguire compiti complessi che richiedono l’elaborazione di enormi quantità di dati, il riconoscimento di pattern e l’automazione decisionale.

Per le aziende, l'AI rappresenta un’opportunità per innovare prodotti e servizi, ottimizzare le operazioni e migliorare l'esperienza del cliente. Attraverso l’uso di modelli predittivi, le imprese possono, per esempio, anticipare le tendenze del mercato, migliorare la gestione delle catene di approvvigionamento e personalizzare le offerte ai consumatori, mentre l'automazione di alcuni processi consente di ridurre i costi operativi e di migliorare l'efficienza.

Nella Pubblica Amministrazione, l'AI può migliorare l'efficacia e l'efficienza dei servizi pubblici. Attraverso l'automazione di molte pratiche burocratiche e la digitalizzazione dei servizi, le PA possono, infatti, ridurre i tempi di risposta e migliorare la qualità del servizio per i cittadini. Inoltre, l'AI può essere utilizzata per analizzare grandi volumi di dati relativi alla sanità pubblica, alla sicurezza e all’ambiente, permettendo di prendere decisioni più informate e tempestive.

L'impatto dell’intelligenza artificiale è quindi potenzialmente dirompente, ma il suo stesso impiego nasconde una dualità: da un lato, l'AI degli hyperscaler globali, potente e accessibile a tutti, dall'altro, la Private AI, più personalizzata e riservata.

Nasce il dilemma di dove collocare questa risorsa preziosa, se affidarsi ai colossi tech o custodirla gelosamente all'interno dell'azienda, affrontando da un lato il rischio di dipendenza dagli hyperscaler globali e l’esposizione a rischi di lock-in e violazione della privacy, mentre dall’altro la necessità di investimenti e competenze specializzate per la

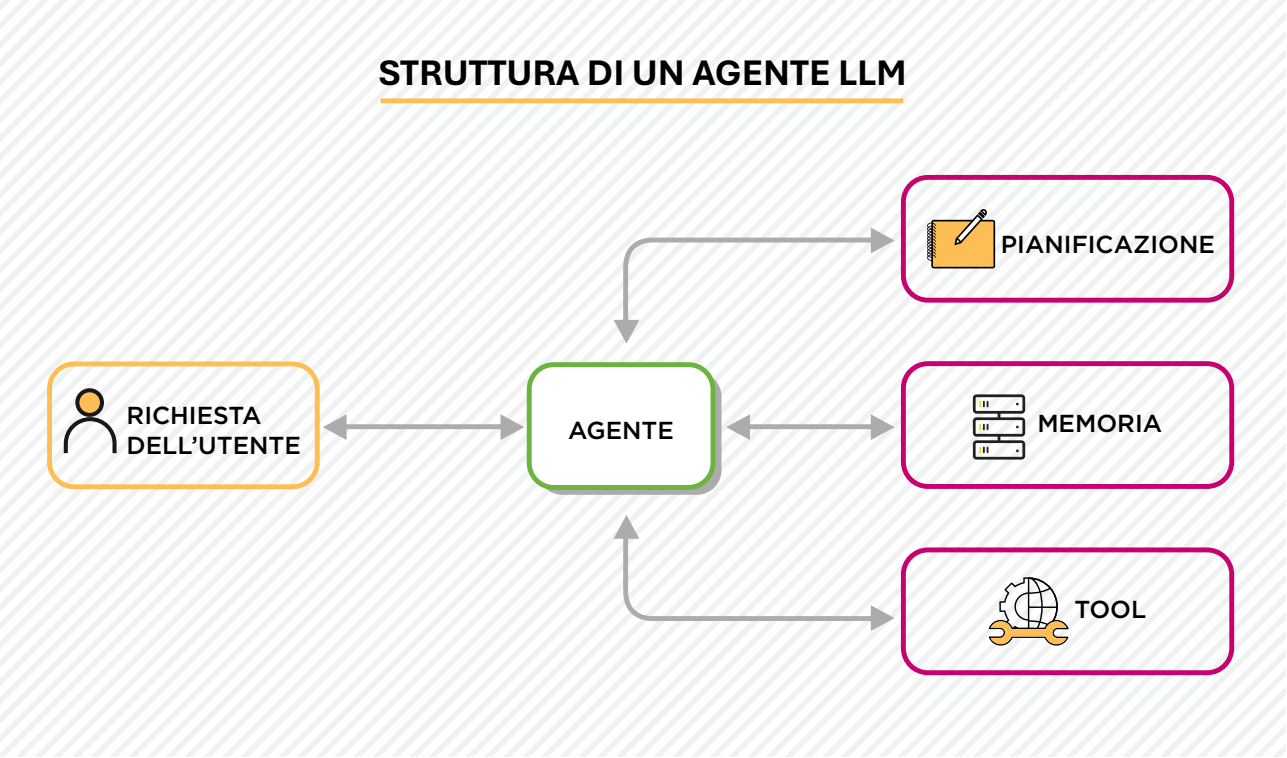
creazione di una Private AI. Competenze che nel nostro Paese scarseggiano e per le quali urge definire un piano per il loro sviluppo.

Due modelli, quindi, con logiche, più che per le tecnologie impiegate, differenti tra di loro, ognuno con caratteristiche che li rendono opzionabili e preferibili rispetto alle singole esigenze.

1.1. Definizione di Private AI: caratteristiche e differenze rispetto ai modelli degli operatori globali extraeuropei

Si intendono come Private AI le soluzioni di intelligenza artificiale che vengono sviluppate e gestite all'interno di un ambiente controllato e privato, in cui un'organizzazione mantiene il pieno controllo su tutte le fasi del ciclo di vita dell'AI, dalla raccolta dei dati, all'istruzione dei modelli e alla loro implementazione.

Questa tipologia di AI è progettata per operare su infrastrutture private, come un data center aziendale o un cloud privato, invece che su piattaforme pubbliche gestite da fornitori di servizi globali, e il suo obiettivo principale è garantire che i dati sensibili e i modelli di IA siano trattati in modo sicuro e conforme alle normative, mantenendo allo stesso tempo un alto grado di personalizzazione e controllo attraverso l'uso di modelli linguistici specifici e verticalizzati in base al dominio di interesse. Tratto differenziante delle Private AI è la possibilità di integrare degli "Agenti"[1] che consentano si usare il motore LLM di intelligenza artificiale nel contesto di usi e processi disparati.



[1] Gli agenti AI "(…) migliorano l'interazione con l'utente, rendendo le operazioni più rapide e meno complesse rispetto ai tradizionali moduli HTML o form. Aggiungono automazione e praticità": https://blog.seeweb.it/perche-gli-agenti-sono-il-primo-vero-caso-duso-dellintelligenza-artificiale/

1.1.1.Caratteristiche distintive della Private AI

La Private AI rappresenta un approccio avanzato per le organizzazioni che intendono mantenere il controllo totale sui propri dati, garantendo allo stesso tempo la massima sicurezza e conformità alle normative vigenti. Questo modello permette di conservare la sovranità sulle informazioni in possesso, evitando che vengano gestite o trasmesse a terze parti, un aspetto particolarmente rilevante per settori come la Finanza, la Sanità e la Pubblica Amministrazione.

Un elemento fondamentale di questa strategia è la **data residency**[2], che non si limita a una questione puramente geografica, ma riguarda soprattutto la giurisdizione di riferimento in cui i dati vengono gestiti. Mantenere i dati all'interno del perimetro giuridico scelto consente alle organizzazioni di rispettare le normative locali e le politiche specifiche in materia di residenza dei dati, evitando il rischio che informazioni sensibili siano soggette a regolamentazioni straniere meno restrittive o a ingerenze di governi esteri. Un approccio che offre una maggiore certezza legale e operativa, riducendo le vulnerabilità legate alla dipendenza da infrastrutture globali e garantendo alle imprese e alle istituzioni pubbliche un livello superiore di protezione e controllo sulle proprie risorse digitali.

Un'ulteriore caratteristica della Private AI è la possibilità di **personalizzare le misure di sicurezza** in base alle specifiche esigenze dell'organizzazione, come la crittografia avanzata, l'accesso controllato e un monitoraggio continuo delle attività, assicurando che la protezione dei dati sia allineata con le normative locali e settoriali, come il GDPR in Europa. La conformità a queste normative non solo evita sanzioni, ma rafforza anche la fiducia degli utenti.

La Private AI consente inoltre **un'alto grado di customizzazione**, permettendo lo sviluppo di modelli di **machine learning su misura**, ottimizzati per le esigenze operative specifiche. Personalizzazioni che, a differenza dei modelli generici offerti dai grandi cloud provider pubblici, possono portare a una maggiore precisione e risultati più rilevanti, in linea con le reali e specifiche esigenze e aspettative della singola azienda.

Un altro vantaggio della Private AI riguarda la **protezione della proprietà intellettuale**. Gestendo internamente gli algoritmi e i dati, le organizzazioni possono proteggere meglio i propri asset strategici, evitando l'esposizione a fornitori esterni. I modelli AI sviluppati internamente restano riservati, riducendo il rischio di compromissione o di utilizzo non autorizzato.

[2] Sulla definizione di Data Residency: https://www.techtarget.com/searchcloudcomputing/definition/data-residency

L’Oligopolio dell’AI non è l’unica opzione

	PRIVATE AI	PUBLIC AI
Scopo e Utilizzo	Usato da una specifica entità che vuole mantenere il controllo sui propri dati.	Usato da tutti con i dati di tutti che però diventano un asset per il fornitore.
Modelli	Aperti o chiusi da terze parti o interni ma ospitati e gestiti su sistemi privati.	Chiusi e di proprietà del fornitore. Le interazioni dell’utente espandono il modello.
Dati per il Training e/o Fine Tuning	Solo set di dati proprietari o di origine nota incluso dati sensibili e strategici.	Dati pubblici o acquistati. Gli utenti aggiungono dati che vanno usati per allenamento
Dati per Inferenza	In genere dati proprietari e riservati che rimangono dell’entità.	Dati proprietari conferiti e dati pubblicamente disponibili. I fornitori accedono e archiviano i dati di inferenza.

Infine, la Private AI garantisce **indipendenza operativa**, affrancando le organizzazioni dai contratti o le politiche dei provider di cloud globali, potendo così adattare le loro soluzioni in modo flessibile, senza dipendere da aggiornamenti esterni. Una flessibilità operativa che consente alle aziende di muoversi secondo i propri ritmi e necessità, senza doversi conformare a infrastrutture cloud pubbliche, spesso troppo generiche per soddisfare le esigenze specifiche di un settore o di un Paese.

1.1.2. Differenze rispetto agli operatori globali extraeuropei

Mentre le Private AI offrono un livello di controllo, sicurezza e personalizzazione che risponde perfettamente alle esigenze specifiche delle organizzazioni, soprattutto in settori dove la protezione dei dati è fondamentale, dall’altro canto i servizi di AI forniti dagli hyperscaler globali, che seppur vantano una scala di costi e una versatilità difficili da eguagliare, presentano alcune limitazioni.

Innanzitutto, i dati dei clienti gestiti dagli hyperscaler sono spesso trattati in ambienti multi-tenant, dove i dati di più aziende condividono le stesse risorse, sollevando potenziali preoccupazioni riguardo alla privacy e alla sicurezza.

Inoltre, nonostante i servizi di AI degli hyperscaler siano potenti e ampiamente accessibili, tendono a essere standardizzati, offrendo meno possibilità di adattamento alle esigenze specifiche di ogni realtà, il che può risultare limitante per le aziende che necessitano di soluzioni altamente personalizzate per raggiungere gli obiettivi prefissati.

Infine, come accennato, affidarsi a infrastrutture globali comporta anche rischi di conformità, in particolare per quanto riguarda il rispetto delle normative locali sulla protezione dei dati. In regioni con leggi stringenti, come il GDPR in Europa, le organizzazioni potrebbero incontrare difficoltà a garantire che i propri dati rimangano all'interno delle giurisdizioni desiderate, complicando ulteriormente il quadro normativo e la gestione della conformità.

1.1.3. Introduzione al concetto di cloud nazionale e focus italiano

L'esigenza di affidarsi a soluzioni di Private AI è quindi una priorità per le organizzazioni che cercano di mantenere il controllo sui propri dati, garantire la sicurezza e rispettare le normative locali. Purtroppo, in Italia attualmente lo sviluppo di competenze avanzate in questo campo è ancora limitato, costringendo molte aziende a rivolgersi ai provider globali per le loro soluzioni di intelligenza artificiale. Una dipendenza che, dicevamo, espone le organizzazioni ai rischi legati alla gestione dei dati in ambienti multi-tenant, ma limita anche la possibilità di personalizzare le tecnologie AI in modo che rispondano specificamente alle esigenze italiane.

Diventa quindi necessario promuovere un'indipendenza tecnologica e investire nello sviluppo di competenze e infrastrutture a livello locale, come il cloud nazionale. Un cloud nazionale, integrato con soluzioni di Private AI, può essere davvero un passo importante verso la creazione di un ecosistema tecnologico autosufficiente e che valorizzi le eccellenze italiane[3].

Un approccio che permetterebbe alle aziende di sviluppare e gestire autonomamente le proprie soluzioni di AI, senza dover dipendere da provider esteri e assicurando che i dati rimangano sotto la giurisdizione italiana, su un'infrastruttura altamente sicura e resiliente, in grado di resistere a cyber-attacchi e garantire la continuità operativa, oltre che dell'economia privata, dei servizi pubblici essenziali.

Con il risultato di rafforzare la sovranità digitale del Paese, stimolando l'innovazione e la crescita di competenze locali nel campo dell'intelligenza artificiale.

2. Il contesto attuale: l'oligopolio dell'AI

Il contesto attuale del mercato dell'intelligenza artificiale è dominato da un ristretto gruppo di grandi provider globali ed extraeuropei, che detengono una posizione di forza che consente loro di influenzare pesantemente lo sviluppo e la distribuzione delle tecnologie AI a livello globale.

Una concentrazione di potere che comporta importanti implicazioni, soprattutto per le aziende italiane che si trovano sempre più dipendenti da strumenti e servizi offerti da provider extraeuropei.

2.1. L'AI come fenomeno oligopolistico: il dominio dei grandi provider globali

Pochi grandi player internazionali detengono quindi non solo le infrastrutture necessarie per l'elaborazione e l'archiviazione dei dati, ma anche le piattaforme di sviluppo e i modelli di machine learning più avanzati.

Questa concentrazione crea un fenomeno oligopolistico, in cui un numero limitato di attori globali stabilisce le regole del gioco, imponendo standard tecnologici, politiche di prezzo e condizioni contrattuali spesso svantaggiose per gli utenti finali, soprattutto in Paesi che non hanno (ancora) sviluppato infrastrutture proprie. E l'Italia è tra questi.

[3] Sulle strategie utili a creare un ecosistema AI a beneficio del progresso del Paese si legga anche: https://www.seeweb.it/files/WhitePaper-Economia-dei-Dati-nell'Intelligenza-Artificiale.pdf

2.2.Impatti dell’AI sul sistema produttivo italiano: ritardo nelle strategie e nella formazione di competenze nazionali

Il sistema produttivo italiano, come quello di tutti i Paesi, è destinato a subire una profonda trasformazione dall’utilizzo strategico dell’Intelligenza artificiale, ma la carenza di una strategia nazionale ben definita e di competenze locali adeguate rischia di rallentare questo processo.

Il ritardo nello sviluppo di competenze avanzate in AI non solo impedisce al nostro Paese di competere su scala globale, ma rende anche più difficile l'integrazione di queste tecnologie nei processi produttivi nazionali. Un gap formativo e strategico che comporta un doppio svantaggio: da un lato, le aziende italiane sono costrette a pagare un premium per l'accesso a servizi di AI forniti da hyperscaler globali; dall'altro, la mancanza di conoscenze locali limita l'innovazione interna e la possibilità di creare soluzioni AI che rispondano alle peculiarità del tessuto economico italiano.

Per superare questi impedimenti, è necessario promuovere lo sviluppo di un ecosistema nazionale dell’AI, basato su un’infrastruttura di cloud nazionale che consenta di mantenere il controllo sui dati e sulle tecnologie strategiche.

Solo attraverso un consistente investimento in competenze locali e in tecnologie proprietarie l'Italia potrà ridurre la sua dipendenza dagli hyperscaler globali, proteggendo nel contempo la propria sovranità digitale e favorendo la crescita di un sistema produttivo più innovativo e competitivo.

3.Perché scegliere l’AI privata: vantaggi strategici e operativi

Scegliere di implementare una AI privata offre alle aziende una serie di vantaggi strategici e operativi che vanno ben oltre la semplice gestione delle informazioni, consentendo un controllo completo sui dati, una maggiore sicurezza e una personalizzazione delle soluzioni AI che è difficilmente raggiungibile con i servizi offerti dai provider globali.

3.1.Sicurezza e protezione dei dati

Uno dei principali vantaggi derivanti da una Private AI è la **tutela della proprietà intellettuale**. Le aziende che sviluppano e gestiscono internamente le proprie soluzioni AI riducono il rischio di condivisione involontaria dei dati sensibili, che potrebbe accadere quando si utilizzano piattaforme cloud pubbliche gestite da terze parti. Questo è particolarmente importante in settori in cui la proprietà intellettuale rappresenta un asset strategico, come nel caso degli algoritmi proprietari o dei set di dati unici utilizzati per l'addestramento dei modelli AI.

Inoltre, la Private AI garantisce una piena **conformità al GDPR** e alle altre normative europee sulla protezione dei dati, superando le lacune regolamentari che spesso affliggono gli hyperscaler globali. Questi ultimi, pur offrendo soluzioni di AI potenti e scalabili, operano spesso in contesti normativi extraeuropei, il che può comportare difficoltà nel garantire il rispetto delle stringenti normative UE. Con una Private AI, invece, le aziende possono essere sicure che i propri dati rimangano all'interno delle giurisdizioni desiderate, riducendo il rischio di violazioni e garantendo una protezione legale adeguata.

La protezione della conoscenza aziendale è un altro elemento da tenere in considerazione: oltre ai dati, infatti, una gestione interna delle soluzioni AI permette di **salvaguardare anche il know-how e l'expertise** che fanno parte del patrimonio informativo dell'azienda. In un mercato sempre più competitivo la conoscenza che si è accumulata nel tempo all'interno di un'azienda rappresenta un vantaggio strategico che va difeso. Con le stesse misure applicate ai dati sensibili.

3.2. Mancanza di garanzia della privacy nei modelli degli hyperscaler

L'adozione di soluzioni AI basate su hyperscaler globali solleva interrogativi importanti anche sulla reale garanzia della privacy e della riservatezza dei dati aziendali. Nonostante le grandi piattaforme dichiarino di rispettare le normative internazionali in materia di protezione dei dati, la loro struttura operativa e il loro modello di business pongono diversi dubbi sulla gestione delle informazioni sensibili.

3.2.1. Il rischio di accesso ai dati da parte del provider

Le infrastrutture degli hyperscaler operano spesso in più giurisdizioni, con server distribuiti tra diversi Paesi, il che comporta che i dati delle aziende europee possano essere trattati e archiviati anche al di fuori dell'Unione Europea, esponendoli a normative di Paesi terzi come il Cloud Act statunitense[4], che consente alle autorità americane di accedere ai dati ospitati da società con sede negli Stati Uniti, indipendentemente dal luogo in cui questi siano fisicamente conservati. Questo scenario mette a rischio la sovranità dei dati e la protezione delle informazioni aziendali riservate, con conseguenze che possono andare anche oltre la semplice conformità normativa.

3.2.2. La condivisione dei dati per l'addestramento dei modelli AI

Gli operatori globali migliorano continuamente le proprie soluzioni sfruttando i dati degli utenti, *anche quando dichiarano di non accedere direttamente alle informazioni aziendali*. L'analisi dei metadati, dei pattern di utilizzo e delle interazioni con il sistema permette di generare conoscenze strategiche che contribuiscono all'ottimizzazione degli algoritmi proprietari. In questo modo, le aziende che si affidano a questi servizi alimentano indirettamente i modelli di tali operatori, senza poter controllare l'effettiva destinazione e l'uso delle informazioni che le caratterizzano, rischiando di trasformare un semplice servizio in un elemento di dipendenza tecnologica, riducendo il controllo che le imprese hanno sui propri dati e sul valore che questi possono generare nel tempo.

3.2.3. Politiche di data retention e difficoltà nel recupero dei dati

Anche le politiche di conservazione dei dati adottate dai provider globali sono un aspetto da considerare con attenzione. Nel momento in cui un'azienda decide di migrare verso una soluzione più controllata, i termini di servizio imposti dagli hyperscaler possono complicare il recupero delle informazioni. Spesso vengono applicati periodi minimi di conservazione,

[4] Secondo il Cloud Act, emanato nel 2018, le forze dell'ordine possono ottenere un mandato finalizzato a costringere le aziende tecnologiche a fornire qualsiasi dato su cui abbiano controllo: https://it.wikipedia.org/wiki/CLOUD_Act

restrizioni sui formati di esportazione o costi elevati per il trasferimento dei dataset aziendali, generando di fatto effetti di lock-in[5] che ostacolano la possibilità di spostarsi verso alternative più sicure e trasparenti senza subire oneri imprevisti.

3.2.4. Private AI: una risposta concreta alla tutela della privacy

L'adozione di un approccio basato su Private AI riesce invece a garantire un controllo completo sui dati. Al contrario dei modelli proposti dagli hyperscaler, le soluzioni di intelligenza artificiale private permettono alle aziende di mantenere i dati all'interno di un'infrastruttura dedicata, evitando qualsiasi accesso da parte di terzi e assicurando il rispetto delle normative europee in materia di protezione delle informazioni. Questo approccio permette di evitare la dispersione della proprietà intellettuale e del know-how aziendale, riducendo i rischi legati all'utilizzo improprio dei dati e garantendo una maggiore indipendenza dalle piattaforme globali. In un contesto in cui la sovranità digitale sta diventando sempre più rilevante, la possibilità di adottare modelli di intelligenza artificiale pienamente controllabili offre un vantaggio strategico sia in termini di sicurezza che di autonomia operativa.

3.3. Competitività e vantaggio concorrenziale

Un altro vantaggio chiave della Private AI è la possibilità di personalizzare e adattare i modelli AI alle esigenze specifiche dell'azienda. A differenza delle soluzioni standardizzate offerte dai provider globali, che spesso non tengono conto delle peculiarità operative delle singole aziende, la AI privata consente di sviluppare modelli su misura, ottimizzati per rispondere alle esigenze specifiche del proprio settore. Un livello di personalizzazione che si traduce in una maggiore efficacia delle applicazioni AI e in risultati più rilevanti.

La proprietà esclusiva degli algoritmi e dei preziosi dati aziendali utilizzati per l'addestramento degli algoritmi può fare la differenza, rappresentando un vero, peculiare, vantaggio nel contesto competitivo.

In un modello strategico in cui i dati sono uno degli asset più preziosi delle aziende, poterli utilizzare internamente senza condividerli con terze parti o, peggio ancora, potenziali concorrenti, significa mantenere il controllo totale sul proprio patrimonio distintivo. Si evita così la dispersione del valore dei dati, che possono essere sfruttati per creare vantaggi competitivi "personali", difficili da imitare.

Infine, la sovranità digitale e l'indipendenza dai servizi dei provider extraeuropei sono aspetti fondamentali per ridurre il rischio di dipendenza da un singolo fornitore che può limitare la flessibilità aziendale e comportare costi aggiuntivi. Utilizzando una AI privata, invece, le aziende possono evitare le restrizioni imposte dalle piattaforme bigtech e mantenere la libertà di evolvere le proprie tecnologie in base alle esigenze di mercato, senza essere vincolate da contratti o politiche imposte esternamente.

3.3.1. Governance e controllo dei costi

Dal punto di vista della governance e del controllo dei costi, i modelli di Private AI consentono una sicurezza e un **controllo completo dei dati** che vengono elaborati, cosa che non è

[5] Il lockin tecnologico rende difficile alle aziende svincolarsi da un provider cloud, ma può essere mitigato attraverso una serie di misure: https://docs.italia.it/italia/manuale-di-abilitazione-al-cloud/manuale-di-abilitazione-al-cloud-docs/it/v1.2/pianificare-la-migrazione/lock-in.html

possibile avere con le soluzioni basate su cloud pubblici. Pur comportando un investimento iniziale maggiore, la Private AI può risultare più conveniente nel lungo termine, dal momento che **si eliminano o riducono i costi ricorrenti** dovuti ai servizi di public cloud. Inoltre, con una piattaforma privata, le aziende possono gestire in maniera centralizzata e controllata il ciclo di vita dei dati, garantendo che tutte le fasi, dalla raccolta alla conservazione, fino all'eliminazione, siano conformi alle proprie politiche interne e alle normative vigenti.

La localizzazione dei dati all'interno del proprio Paese o di specifiche giurisdizioni facilita anche la data governance, assicurando che i dati non siano soggetti a leggi straniere che potrebbero creare problemi per la loro protezione. In più, con una Private AI, si **semplificano le procedure di audit e tracciabilità dei dati**, potendo avere una visibilità completa sulle operazioni, il che consente di rilevare tempestivamente eventuali anomalie o violazioni.

4.AI Act: Implicazioni e opportunità per le aziende italiane

L'AI Act rappresenta un punto di svolta nella regolamentazione dell'intelligenza artificiale a livello europeo. Si tratta di una nuova legge, approvata nel 2024, che punta a creare un quadro normativo unico e armonizzato per lo sviluppo e l'utilizzo dell'intelligenza artificiale all'interno dell'Unione Europea.

L'obiettivo principale dell'AI Act è garantire che l'intelligenza artificiale sia sviluppata e utilizzata in modo sicuro, etico e rispettoso dei diritti fondamentali dei soggetti europei. In questo modo, si cerca di bilanciare la promozione dell'innovazione tecnologica con la tutela dei diritti individuali e collettivi.

Un aspetto fondamentale dell'AI Act è la classificazione dei sistemi di intelligenza artificiale in base al livello di rischio che pongono. I sistemi considerati a rischio inaccettabile, come quelli che manipolano le persone o discriminano, saranno vietati. Al contrario, i sistemi a rischio minimo, come i videogiochi, saranno soggetti a obblighi minimi. Per i sistemi a rischio intermedio, come quelli utilizzati in ambito sanitario o nelle risorse umane, saranno previsti requisiti più stringenti in termini di trasparenza, sicurezza e controllo umano.

4.1.Le implicazioni a livello aziendale ed economico

Al di là degli aspetti etici, l'AI Act influenza profondamente le strategie basate sull'intelligenza artificiale delle aziende italiane ed europee. Le nuove normative impongono infatti un livello più alto di rigore nella gestione dei dati, nella resilienza e nella sicurezza informatica, ma offrono anche un'opportunità per rivedere l'approccio aziendale all'AI e adottare soluzioni che garantiscano maggiore controllo e conformità. E in questo contesto, orientarsi verso l'impiego di una Private AI, può dimostrarsi una mossa strategicamente vantaggiosa, che consente di mantenere la governance sui dati all'interno dei confini aziendali.

4.2.Quali vantaggi offre l'AI Act alle aziende

- **Certezza del diritto e riduzione dei rischi:** L'AI Act fornisce un quadro normativo certo e prevedibile,consentendo alle aziende di operare in un ambiente regolamentato e di mitigare i rischi legati all'utilizzo di sistemi di IA non conformi.
- **Stimolo per l'innovazione:** Pur ponendo limiti a pratiche considerate rischiose, l'AI Act incoraggia l'innovazione responsabile, offrendo alle aziende l'opportunità di sviluppare soluzioni basate sull'IA sicure,affidabili e conformi ai più alti standard europei.
- **Protezione della proprietà intellettuale:** Il regolamento tutela la proprietà intellettuale delle aziende, garantendo che i loro sviluppi in ambito IA siano protetti da eventuali usi illeciti.
- **Accesso al mercato unico europeo:** Le aziende che rispettano le disposizioni dell'AI Act avranno maggiori facilità ad accedere al mercato unico europeo, evitando barriere normative e facilitando la commercializzazione dei propri prodotti e servizi.
- **Miglioramento della reputazione:** L'adozione di pratiche conformi all'AI Act contribuisce a migliorare la reputazione aziendale, aumentando la fiducia dei consumatori e degli investitori.

4.3.Su quali aspetti l'AI Act si concentra in particolare per le aziende

- **Valutazione dei rischi:** Le aziende dovranno condurre valutazioni approfondite dei rischi associati ai loro sistemi di IA, identificando e mitigando potenziali minacce alla sicurezza, alla privacy e ai diritti fondamentali.
- **Trasparenza:** Le aziende dovranno garantire la trasparenza dei loro sistemi di IA, informando gli utenti sull'utilizzo dell'IA e sui suoi limiti.
- **Qualità dei dati:** L'AI Act pone l'accento sulla qualità dei dati utilizzati per addestrare i sistemi di IA, richiedendo che i dati siano accurati, completi e non discriminatori.
- **Supervisione umana:** Anche nei processi decisionali automatizzati, l'AI Act prevede un ruolo fondamentale per la supervisione umana, al fine di garantire il controllo e la responsabilità.

4.4.Addestramento accurato dei dataset

L'AI Act dell'Unione Europea introduce una serie di obblighi volti a garantire che i dataset utilizzati per l'addestramento siano accurati, completi e rappresentativi, richiedendo alle aziende di implementare strumenti avanzati per monitorare e tracciare i dati lungo tutto il loro ciclo di vita. Per le imprese che vogliono mantenere un controllo rigoroso sui propri dati, la Private AI offre un'infrastruttura ideale, dove i dati non devono essere esternalizzati, riducendo così i rischi associati a possibili violazioni normative.

4.5.Resilienza dei modelli: sicurezza e affidabilità sono d'obbligo

In un ambiente economico sempre più dipendente dall'AI, le aziende devono anche garantire la resilienza operativa dei loro modelli. L'AI Act pone proprio l'accento sulla sicurezza e sull'affidabilità dei sistemi, richiedendo piani di emergenza e backup. La geo-ridondanza, che consente la distribuzione dei carichi di lavoro tra diverse sedi, e l'integrazione di soluzioni

ibride tra cloud pubblico e privato, sono alcune delle strategie che possono rafforzare la continuità operativa delle imprese.

Inoltre, il regolamento evidenzia l'importanza di mantenere il controllo sui dati e sui modelli, evitando accessi non autorizzati o manipolazioni. Le aziende possono sfruttare l'AI federata, che consente di accedere a vasti dataset mantenendo al tempo stesso la proprietà intellettuale e la riservatezza del proprio know-how. Questo approccio non solo facilita la conformità normativa, ma protegge anche il valore strategico delle informazioni aziendali.

4.6.La Private AI semplifica la gestione dell'AI Act

Implementare una strategia di private AI aiuta le aziende a gestire le complessità dell'AI Act, assicurando che ogni fase dello sviluppo e dell'uso dei modelli sia in linea con i requisiti normativi. Questa soluzione si adatta alle esigenze di governance, sicurezza e sostenibilità, permettendo alle imprese di crescere senza rinunciare al controllo dei propri asset digitali. Nell'ottica di lungo termine, l'adozione della private AI rappresenta una scelta strategica per garantire competitività e conformità, preparandosi alle sfide del futuro regolamentare.

5.Come il Private AI facilita la conformità all'AI Act rispetto alle soluzioni hyperscaler

Il Private AI offre una serie di vantaggi rispetto alle soluzioni proposte dagli hyperscaler globali anche in termini di conformità all'AI Act, che richiede un maggiore controllo e trasparenza sui dati e sui processi di intelligenza artificiale.

Il Private AI permette infatti alle aziende di mantenere il controllo totale sui propri dati, evitando di doverli trasferire a fornitori terzi o a piattaforme cloud gestite dai grandi nomi tra i gestori internazionali. L'AI Act richiede che i dati utilizzati per addestrare i modelli siano accurati, rappresentativi e privi di errori. Con un'infrastruttura di Private AI, le aziende possono monitorare in maniera più rigorosa l'intero ciclo di vita dei dati, tracciandone la provenienza, la qualità e le eventuali modifiche, garantendo una conformità più agevole ai requisiti normativi.

5.1.Sovranità digitale

Tutte le normative europee, tra cui l'AI Act, pongono una forte enfasi sulla protezione dei dati e sulla loro localizzazione all'interno dell'Unione Europea. Utilizzando un'infrastruttura di Private AI, le aziende possono garantire che i dati sensibili non lascino i confini nazionali o

europei, riducendo il rischio di violazioni delle normative sulla sovranità digitale e mantenendo il controllo sulle informazioni critiche senza dipendere da fornitori globali che operano in giurisdizioni con regole differenti.

5.2.Maggiore trasparenza e auditabilità

L'AI Act impone standard rigorosi sulla trasparenza e l'accountability, richiedendo che le aziende possano dimostrare la conformità dei propri modelli AI. Con una soluzione di Private AI, le organizzazioni possono implementare procedure di audit più solide e mantenere registri dettagliati di ogni fase del processo di addestramento e utilizzo dei modelli. A differenza delle soluzioni hyperscaler, dove i processi interni potrebbero non essere completamente trasparenti, il Private AI consente una maggiore visibilità e tracciabilità su tutti gli aspetti operativi.

5.3.Minimizzazione del rischio di lock-in

Le soluzioni offerte dagli hyperscaler globali tendono a creare una forte dipendenza tecnologica, con potenziali difficoltà nella migrazione dei dati e nell'adattamento ai requisiti normativi locali. Con il Private AI, le aziende possono costruire e gestire i propri modelli e infrastrutture, riducendo il rischio di lock-in e facilitando l'adeguamento ai cambiamenti normativi, incluso l'AI Act. Questo approccio garantisce una maggiore flessibilità e adattabilità rispetto alle piattaforme hyperscaler.

5.4.Protezione della proprietà intellettuale

La Private AI consente alle aziende di mantenere il pieno controllo sui modelli di intelligenza artificiale e sugli algoritmi proprietari, il che rappresenta un aspetto fondamentale per rispettare le disposizioni dell'AI Act in materia di protezione della proprietà intellettuale e di know-how. A differenza delle piattaforme hyperscaler, che potrebbero implicare la condivisione o l'uso incrociato di algoritmi e dati, i sistemi di Private AI offrono una protezione più robusta contro il rischio di dispersione o accesso non autorizzato a risorse strategiche aziendali.

5.5.Adattamento alle normative locali e alle policy interne o di settore

La Private AI può essere adattata in modo più preciso alle esigenze normative di ogni singola azienda o Paese. L'AI Act richiede spesso adattamenti specifici, come la personalizzazione dei modelli AI per essere conformi a norme settoriali o locali. Le piattaforme hyperscaler, per contro, offrono soluzioni più standardizzate, con minore possibilità di personalizzazione. Questo rende il Private AI particolarmente vantaggioso per le aziende che operano in settori regolamentati o con esigenze specifiche di compliance.

6. Governance dei dati e opportunità per il Private AI nel contesto del Data Act

Il Data Act è una normativa europea che mira a regolamentare l'accesso e la gestione dei dati per promuovere una condivisione più equa e controllata delle informazioni tra imprese, fornitori di servizi e utenti finali. Si tratta di una legge che avrà un notevole impatto sulla strategia di gestione dei dati aziendali, in particolare per quanto riguarda le tecnologie basate sull'intelligenza artificiale. In tutto questo, le aziende italiane potranno trarre vantaggi

strategici adottando infrastrutture nazionali e soluzioni di Private AI, evitando di dipendere dagli hyperscaler globali.

6.1.Panoramica del Data Act e come influisce sulla gestione dei dati aziendali

Il Data Act, approvato a livello europeo, ha l'obiettivo di creare un quadro normativo che favorisca una gestione dei dati più trasparente e controllata. Tra gli elementi chiave del Data Act vi è l'enfasi sul diritto di **accesso ai dati** da parte degli utenti e l'obbligo per le aziende di **facilitare lo scambio di dati** con altri soggetti in determinati casi. Tutto questo per evitare la concentrazione di dati nelle mani di poche grandi aziende e per favorire una più ampia partecipazione al mercato dei dati.

Per le aziende italiane, che spesso operano in settori strategici come la manifattura, l'agroalimentare la moda, la ricerca pharma, questo nuovo quadro normativo rappresenta un'opportunità per migliorare la gestione dei dati a livello locale, ma anche una sfida in termini di compliance. Affidarsi a infrastrutture nazionali o private, invece che ai grandi provider globali, può facilitare la governance dei dati, garantendo che i dati sensibili e strategici non escano dai confini europei e che le aziende rispettino i requisiti imposti dal Data Act in modo più sicuro e flessibile.

6.2.Implicazioni per l'accesso e la condivisione dei dati nell'ambito delle soluzioni AI

Il Data Act introduce norme chiare sull'**accesso ai dati** e la **condivisione delle informazioni**. In particolare, obbliga le aziende a garantire che i dati generati dai dispositivi o sistemi connessi siano accessibili anche a terzi, purché non compromettano la privacy o la sicurezza. Per le aziende che utilizzano soluzioni AI, questo significa che dovranno assicurarsi che l'accesso ai dati sia gestito in modo trasparente, tracciabile e conforme alle normative.

Le imprese italiane, spesso vincolate alla protezione del proprio know-how e delle informazioni sensibili, devono quindi fare scelte oculate su come gestire questa condivisione. Utilizzare soluzioni di Private AI in infrastrutture nazionali offre maggiore controllo sui dati. A differenza delle piattaforme hyperscaler, che **sono soggette a regolamentazioni diverse in base alla giurisdizione in cui operano**, il Private AI consente alle aziende di mantenere i dati entro i confini legali e geografici desiderati, riducendo i rischi legati alla divulgazione non autorizzata o all'accesso da parte di terzi.

Inoltre, le soluzioni di Private AI permettono di sviluppare modelli di **AI proprietari** su dataset interni senza condividere queste risorse con fornitori esterni, mantenendo il vantaggio competitivo che i dati aziendali rappresentano. Questo è particolarmente rilevante per le aziende italiane che operano in settori dove la conoscenza e l'innovazione sono centrali, come l'automotive, il design o l'ingegneria.

6.3.Vantaggi per le aziende che scelgono di mantenere i dati in ambienti privati rispetto all'uso di operatori globali

Scegliere di utilizzare infrastrutture nazionali o soluzioni di Private AI piuttosto che affidarsi agli hyperscaler globali offre numerosi vantaggi per le aziende italiane, soprattutto in termini di sicurezza, sovranità digitale e costi a lungo termine.

Sovranità digitale e conformità normativa - Con il Data Act e le normative europee come il GDPR, le aziende italiane devono garantire che i loro dati rimangano sotto il controllo europeo. Utilizzando Private AI e infrastrutture locali, le imprese possono assicurarsi che i dati non vengano esportati in Paesi extra-UE, dove le leggi sulla protezione dei dati potrebbero essere meno rigide. Questo riduce il rischio di violazioni della normativa e potenziali sanzioni.

Al contrario, i grandi hyperscaler globali spesso hanno data center in tutto il mondo, il che può complicare la gestione della conformità, soprattutto quando si tratta di dati sensibili. Inoltre, in situazioni di contenzioso o richieste governative, le aziende italiane che utilizzano infrastrutture locali sono più protette contro il rischio di dover cedere dati a governi stranieri.

Controllo e personalizzazione - Le soluzioni Private AI offrono alle aziende italiane un maggiore controllo su come i dati vengono gestiti, utilizzati e condivisi. A differenza dei servizi hyperscaler, che tendono a essere più standardizzati e meno personalizzabili, le infrastrutture Private AI possono essere configurate su misura per soddisfare esigenze specifiche. Questo significa che le aziende possono implementare politiche di governance dei dati più rigide, garantendo che l'accesso ai dati sia limitato solo a personale o partner autorizzati.

Inoltre, le soluzioni Private AI consentono alle imprese di adattare e personalizzare i modelli di intelligenza artificiale in base alle proprie esigenze operative e di business, rendendole più agili e competitive sul mercato.

Sicurezza e resilienza - La sicurezza dei dati è un altro fattore importante. Il Data Act introduce nuove misure per garantire che i dati siano protetti durante la condivisione e l'accesso. Le soluzioni Private AI offrono un vantaggio significativo in termini di sicurezza, poiché i dati rimangono all'interno del perimetro aziendale o su infrastrutture controllate a livello nazionale, riducendo il rischio di attacchi informatici o accessi non autorizzati.

Inoltre, la resilienza operativa è più elevata quando le aziende italiane possono gestire direttamente le proprie infrastrutture, implementando misure di sicurezza avanzate, come la crittografia end-to-end e il monitoraggio costante delle operazioni. Gli hyperscaler, al contrario, operano su scala globale e non sempre possono offrire lo stesso livello di dettaglio e di personalizzazione nella protezione dei dati.

Costi a lungo termine e prevenzione del lock-in - Infine, adottare soluzioni di Private AI può risultare più conveniente a lungo termine, soprattutto in termini di gestione dei dati e conformità normativa. Gli hyperscaler globali spesso applicano modelli di pricing complessi e ricorrenti che possono aumentare significativamente i costi operativi nel tempo. Inoltre, il rischio di lock-in tecnologico, dove le aziende diventano dipendenti da un unico fornitore di

servizi, è elevato. Appoggiandosi a un Private AI, invece, le aziende italiane possono evitare tali rischi, mantenendo la flessibilità necessaria per gestire i propri dati e modelli in modo indipendente, riducendo i costi legati alle licenze software o all'uso di infrastrutture globali.

7.L’offerta di Private AI da parte degli operatori globali: rischi e costi nascosti

Con l'aumento della domanda di soluzioni di Private AI, anche gli hyperscaler globali, come AWS, Microsoft Azure e Google Cloud, stanno adattando le loro proposte, offrendo soluzioni di intelligenza artificiale private su infrastrutture localizzate a livello nazionale. Questa mossa presenta però diversi rischi e costi nascosti che possono mettere le aziende italiane in situazioni complicate, soprattutto in termini di governance dei dati, rispetto delle normative come il Data Act, e controllo operativo. È necessario esaminare attentamente queste dinamiche per evitare di cadere in trappole che potrebbero compromettere la sovranità dei dati e la flessibilità aziendale.

7.1.I costi non detti: dal lock-in alla riconsegna dei dati

Uno dei principali rischi delle soluzioni Private AI offerte dagli hyperscaler globali è il "vendor lock-in", ossia la dipendenza da un unico fornitore. Le aziende italiane che scelgono di affidarsi a queste soluzioni potrebbero scoprire che, una volta che i loro dati e modelli di intelligenza artificiale sono stati migrati sulle infrastrutture di un hyperscaler, diventa estremamente costoso e complesso recuperarli o trasferirli su altre piattaforme.

Un esempio lampante di questa problematica riguarda i costi per la riconsegna dei dati. Molti hyperscaler impongono tariffe elevate per restituire alle aziende i dati una volta caricati nei loro sistemi. Questo può rappresentare un serio ostacolo per chi vuole passare a soluzioni alternative o desidera ritirare i propri dati per ragioni di sicurezza o conformità normativa. Si tratta però di costi che spesso non sono così trasparenti all'inizio della relazione con il fornitore e possono emergere solo quando l'azienda decide di uscire dal contratto.

In questo contesto, la **gratuità della riconsegna dei dati** dovrebbe essere garantita e regolamentata. Il Data Act introduce già dei principi per favorire l'interoperabilità e l'accesso equo ai dati, ma non sempre copre i costi associati alla loro movimentazione o trasferimento tra fornitori. Gli hyperscaler, forti della loro posizione dominante, tendono a creare barriere

finanziarie che scoraggiano la migrazione a piattaforme più sicure o locali, perpetuando il lock-in.

Per le aziende italiane, questo aspetto è un vero e proprio rischio operativo e finanziario. Le imprese potrebbero infatti ritrovarsi bloccate in contratti con hyperscaler che non solo limitano la loro libertà di scelta, ma che continuano ad aumentare i costi operativi a lungo termine. È fondamentale, quindi, negoziare clausole chiare e trasparenti nei contratti con gli hyperscaler, garantendo che il trasferimento e la restituzione dei dati siano sempre gratuiti o che almeno i costi siano ben delineati fin dall'inizio.

7.2.Conformità al Data Act: potenziali conflitti con le soluzioni degli hyperscaler

Il Data Act, dicevamo, pone un forte accento sulla sovranità dei dati e sulla condivisione trasparente delle informazioni, ma affidarsi agli hyperscaler globali per soluzioni di Private AI può presentare delle problematiche in questo contesto. Sebbene gli hyperscaler abbiano avviato iniziative per localizzare i loro data center all'interno dei confini europei, esiste ancora una netta differenza tra un'infrastruttura locale e una gestita da un hyperscaler globale.

Gli hyperscaler spesso operano a livello globale, il che significa che, nonostante possano avere data center in Italia o in altri Paesi dell'UE, sono comunque soggetti a legislazioni esterne, come il **Cloud Act degli Stati Uniti**, che consente alle autorità statunitensi di richiedere l'accesso ai dati detenuti da aziende americane, anche se quei dati risiedono fuori dagli Stati Uniti. Questo può creare un conflitto diretto con le normative europee come il GDPR e il Data Act, che mirano a proteggere la sovranità e la sicurezza dei dati all'interno dell'UE.

Le aziende italiane che si affidano a hyperscaler per soluzioni di Private AI potrebbero quindi rischiare di vedere compromessi i propri obblighi di conformità al Data Act, senza nemmeno esserne consapevoli. Il problema non riguarda solo la sicurezza dei dati, ma anche la governance e la gestione dei dati stessi, poiché i fornitori hyperscaler potrebbero non garantire lo stesso livello di controllo e trasparenza che una soluzione locale o proprietaria può offrire.

7.3.Vantaggi di infrastrutture nazionali e Private AI rispetto agli hyperscaler

Alla luce di questi rischi, le aziende italiane possono trarre vantaggi significativi dall'utilizzo di infrastrutture nazionalio soluzioni di Private AI rispetto agli hyperscaler globali. Mantenere i dati all'interno di infrastrutture nazionali garantisce alle aziende un maggiore controllo sui loro asset digitali e minimizza il rischio che dati sensibili o strategici siano soggetti a normative straniere. Le soluzioni di Private AI italiane possono essere conformi al Data Act senza compromessi, offrendo alle imprese maggiore trasparenza e sicurezza rispetto a quanto offerto dai provider globali.

Le infrastrutture private, gestite internamente o tramite partner locali, offrono inoltre una maggiore trasparenza dei costi. A differenza degli hyperscaler, dove i costi di uscita e la

restituzione dei dati possono essere elevati e nascosti, le soluzioni di Private AI possono essere progettate con modelli di pricing più prevedibili e senza costi aggiuntivi per la riconsegna dei dati.

L'utilizzo di infrastrutture nazionali permette alle aziende di essere più flessibili nel modo in cui gestiscono i propri dati e modelli AI. Questo non solo facilita la conformità al Data Act, ma permette alle aziende di adattarsi più rapidamente ai cambiamenti normativi o di mercato senza dover dipendere da fornitori esterni con politiche globali.

Infine, le soluzioni Private AI permettono una gestione più sicura e controllata dei dati rispetto agli hyperscaler. I dati rimangono sotto il diretto controllo delle aziende o di partner locali, riducendo il rischio di accessi non autorizzati o violazioni della sicurezza. Inoltre, le aziende italiane possono beneficiare di una maggiore resilienza operativa, evitando interruzioni o downtime dovuti a problemi infrastrutturali su scala globale.

8.Confronto tra Private AI e hyperscaler AI

Dal confronto tra le soluzioni di Private AI e quelle offerte dagli hyperscaler globali emergono differenze in termini di prestazioni, costi, flessibilità e controllo. Entrambe le opzioni hanno sia vantaggi sia limitazioni che devono essere valutati in base alle esigenze specifiche delle singole aziende. Se la scelta di affidarsi agli hyperscaler è adatta per organizzazioni che necessitano di soluzioni AI standardizzate, a basso costo iniziale e con rapida scalabilità, la Private AI rappresenta invece una scelta strategica per le aziende che chiedono prestazioni personalizzate, controllo completo e una pianificazione a lungo termine dei costi. La flessibilità e la possibilità di adattare le soluzioni AI alle esigenze aziendali, unita alla protezione della proprietà intellettuale e alla conformità normativa, rendono perciò la Private AI una scelta sempre più attraente per chi punta all’indipendenza e alla sovranità digitale.

8.1.Prestazioni e scalabilità

In termini di prestazioni, le soluzioni di Private AI offrono livelli di efficienza che, se ben progettate, possono competere con quelle degli operatori internazionali ma, mentre i grandi cloud provider globali forniscono infrastrutture già ottimizzate e pronte all'uso per gestire una vasta gamma di applicazioni AI, la Private AI consente di ottenere prestazioni più mirate grazie alla possibilità di personalizzare le risorse e i modelli in base ai bisogni specifici dell'azienda. Tutto questo si traduce in algoritmi meglio ottimizzati e capaci di rispondere in maniera più precisa alle esigenze operative del proprio settore.

Per quanto riguarda la scalabilità, gli hyperscaler hanno il vantaggio di potere espandere velocemente risorse su richiesta. Ma dal canto suo, anche la Private AI sta colmando questo gap: oggi, infatti, esistono soluzioni di Private AI progettate per essere scalabili, potendo gestire un volume crescente di dati e permettendo alle aziende di crescere senza essere costrette a migrare a un'infrastruttura cloud pubblica. Ormai anche una infrastruttura privata ben costruita può scalare progressivamente man mano che aumentano le esigenze operative, mantenendo sicurezza e controllo.

8.2.Costi ed efficienza economica

L’analisi dei costi calcolati su un lungo periodo è certamente determinante nella scelta tra Private AI e hyperscaler, ma vanno fatte alcune considerazioni che tengano presente

l’impatto nel medio-lungo periodo. Nonostante gli hyperscaler possano sembrare inizialmente più economici grazie ai loro modelli di pay-per-use, i costi ricorrenti a lungo termine possono crescere rapidamente con l'aumento del consumo di risorse. Al contrario, le soluzioni di Private AI richiedono certamente un investimento iniziale significativo per l’acquisto di hardware e lo sviluppo delle infrastrutture, ma tendono poi a essere più convenienti nel lungo periodo, dal momento che i costi operativi diventano più prevedibili e gestibili.

A beneficio anche del **ROI** (Return On Investment) di una Private AI, che può essere particolarmente interessante per aziende che vogliono mantenere un controllo completo sui propri dati e algoritmi, visto che in tal modo si evitano i costi legati all'outsourcing dei servizi, oltre a minimizzare il già citato rischio di lock-in. Inoltre, il **TCO** (Total Cost of Ownership) di una soluzione privata, considerando i benefici in termini di sicurezza, governance e personalizzazione, può superare il modello più standardizzato e universale offerto dagli hyperscaler, soprattutto per quei settori che esigono requisiti di compliance stringenti o un alto grado di innovazione interna.

8.3.Flessibilità e controllo

La flessibilità delle soluzioni è tra gli aspetti che maggiormente risaltano dal confronto tra le due modalità. Gli hyperscaler forniscono un’ampia gamma di servizi AI preconfigurati e altamente scalabili, ma spesso limitano la possibilità di personalizzazione, obbligando le aziende a lavorare con strumenti che non sono sempre perfettamente allineati alle loro esigenze. La Private AI, invece, consente una personalizzazione totale delle soluzioni, permettendo alle aziende di sviluppare algoritmi, modelli e infrastrutture specifici che rispondano direttamente alle loro necessità.

Il controllo diretto delle risorse e delle infrastrutture è un altro vantaggio distintivo della Private AI. Le organizzazioni che scelgono di sviluppare soluzioni AI interne possono infatti mantenere il controllo completo sulle loro risorse computazionali e sui dati, gestendo direttamente l’accesso, la sicurezza e l’implementazione di nuove funzionalità. Questo livello di controllo offre una maggiore adattabilità alle esigenze specifiche dell'azienda, consentendo di modificare e aggiornare le soluzioni AI in modo rapido e mirato, senza dover attendere aggiornamenti o modifiche imposte esternamente, come nel caso degli hyperscaler.

9.I costi nascosti dell’AI offerta dagli hyperscaler, dal lock-in al pay-per-use incontrollato

L'adozione di soluzioni AI offerte dagli hyperscaler internazionali, come Amazon Web Services, Google Cloud, e Microsoft Azure, può sembrare inizialmente attraente per molte aziende, grazie a modelli di pricing flessibili, scalabilità immediata, e la possibilità di accedere a infrastrutture potenti senza un grande investimento iniziale. Ma bisogna fare attenzione: dietro queste offerte si celano una serie di costi nascosti che possono rendere l’AI pubblica molto più costosa nel lungo termine rispetto all’opzione Private AI.

9.1.Storage e trasferimento dei dati

I costi di archiviazione su piattaforme di operatori globali possono crescere

esponenzialmente con l’aumentare della quantità di dati. Inoltre, trasferire i dati da un fornitore di servizi internazionale verso altre infrastrutture o recuperare i dati per utilizzarli altrove può comportare tariffe elevate. Ad esempio, AWS e Google Cloud applicano costi non trascurabili per l’uscita dei dati (data egress fees), che rendono particolarmente costoso spostare grandi volumi di dati al di fuori del loro cloud.

9.2.Costo del recupero dei dati (data lock-in)

Gli hyperscaler spesso utilizzano un modello di "data lock-in", ossia vincolano i clienti alla propria infrastruttura tramite costi elevati per il recupero e la migrazione dei dati. Ad esempio, il trasferimento di terabyte di dati verso un ambiente privato può comportare spese considerevoli, rendendo il passaggio alla Private AI più difficile e costoso.

9.3.Scalabilità e over-provisioning (strutture sovradimensionate rispetto all’uso reale)

Gli hyperscaler permettono alle aziende di scalare rapidamente, ma il costo della scalabilità può diventare esponenziale. Quando un'azienda scala e utilizza maggiori risorse di calcolo, i costi possono diventare ingestibili, soprattutto se non si ottimizza l'uso delle risorse (es. GPU, CPU, memoria). È comune che le aziende finiscano per pagare per risorse non utilizzate o non necessarie.

9.4.Licenze software e accesso a funzionalità avanzate (e costose)

Molti servizi AI offerti dagli hyperscaler hanno livelli di licenza che includono funzionalità avanzate, come l'elaborazione del linguaggio naturale, il machine learning su larga scala, o l'analisi dei big data. Questi livelli premium richiedono spesso costi aggiuntivi, che non sono chiaramente visibili nelle offerte iniziali.

9.5.Supporto tecnico e consulenza

Le aziende che si rivolgono agli hyperscaler potrebbero scoprire che il supporto tecnico avanzato è disponibile solo a fronte di costi aggiuntivi significativi. Inoltre, le spese per la consulenza o per configurare l’infrastruttura cloud possono aumentare notevolmente il costo complessivo.

10.Confronto tra Private AI e Hyperscaler AI: scenari e costi stimati

Per dimostrare l'efficacia economica della Private AI rispetto agli hyperscaler, consideriamo un caso reale, esaminando il **TCO** (Total Cost of Ownership) di un'azienda media che decide di implementare una soluzione AI per analizzare grandi quantità di dati.

Costo	Hyperscaler AI (Annuale)	Private AI (Annuale)
Storage dati	50-70 €/TB/mese per 50 TB (~42.000 €/anno)	12.000 € (dischi locali e backup su cloud)
Data egress fees	5-10 €/TB per 10 TB (~6.000 €/anno)	N/A
Calcolo (GPU/CPU)	30.000 € (GPU per AI su hyperscaler)	15.000 € (GPU on-premises ammortizzata)
Scalabilità infrastrutturale	Dinamico (~25.000 €/anno)	Fissa (~10.000 € di gestione IT e upgrade)
Licenze software	12.000 €/anno per funzionalità avanzate	5.000 €/anno per stack software open source
Supporto e consulenza	5.000 €/anno	Incluso nelle spese di gestione
Totale stimato	~120.000 €/anno	~42.000 €/anno

Dati stimati sulla base di benchmark di settore e analisi interne

Con la Private AI, le organizzazioni scelgono dove archiviare i propri dati: on premise o su cloud di operatori EU in grado di garantire la protezione delle informazioni strategiche delle aziende. Un approccio che consente di:

- controllare come i dati interagiscono con i modelli;
- decidere quanti dati fornire;
- stabilire quando limitare l'accesso.

In questo modo, è possibile anche tenere maggiormente sotto controllo i costi, e misurare il ritorno dell'investimento.

I clienti con infrastrutture di AI privata, i quali utilizzano modelli open source e li gestiscono su proprie infrastrutture o su cloud public fidati, in cui dispongono di risorse pronte all'uso e

al contempo dedicate, arrivano a risparmiare da 3 a 5 volte di più evitando costi mensili per token che spesso nella public AI sfuggono al controllo.

10.1.Risparmio a lungo termine

Nel caso del Private AI, il costo iniziale di setup può essere più elevato a causa dell'investimento in hardware e infrastrutture, ma i costi operativi a lungo termine sono significativamente inferiori. Le aziende che utilizzano Private AI risparmiano sui costi di storage, evitano le spese di uscita dei dati (data egress fees), e possono gestire il proprio stack tecnologico in modo più efficiente, senza dover pagare per risorse non utilizzate o servizi superflui.

In questo scenario, un'azienda potrebbe **risparmiare oltre il 65%** in costi annui utilizzando un'infrastruttura Private AI rispetto a un hyperscaler. Inoltre, nel lungo termine, il ritorno sull'investimento della Private AI aumenta man mano che l'azienda riesce a mantenere pieno controllo su dati e infrastrutture.

10.2.Cosa considerare nelle offerte degli hyperscaler

Quando si analizzano le offerte degli hyperscaler, è importante tenere in considerazione alcuni elementi fondamentali per il calcolo finale dei costi diretti e connessi.

- **Costo totale di possesso (TCO) -** Assicurarsi di valutare non solo i costi iniziali ma anche quelli che emergono nel tempo, inclusi i costi di storage, trasferimento dati e scalabilità.
- **Flessibilità e scalabilità -** Gli hyperscaler offrono la possibilità di scalare rapidamente, ma spesso con costi variabili che diventano difficili da prevedere e gestire a lungo termine.
- **Proprietà e controllo dei dati -** Le regole di accesso ai dati e i costi di recupero imposti dagli hyperscaler possono limitare il controllo che un'azienda ha sui propri dati. È essenziale capire a fondo le politiche di data lock-in.
- **Costi di licenza e abbonamento -** Molti hyperscaler utilizzano modelli di pricing a livelli con costi crescenti per funzionalità avanzate. Considerare attentamente quali funzionalità sono davvero necessarie per evitare spese superflue.

11.L'Impatto della Private AI sulle aziende italiane: vantaggi e opportunità per il Made in Italy

L'intelligenza artificiale sviluppata e gestita internamente dalle aziende senza ricorrere a soluzioni esterne gestite da terze parti ha il potenziale per **aumentare la competitività delle imprese italiane**, a cominciare dal fatto che questo modello consente un controllo diretto sui dati, il che risulta essere estremamente importante per la tutela della privacy e la protezione delle informazioni.

Le aziende italiane, specialmente quelle manifatturiere, possono sfruttare il Private AI per ottimizzare i processi produttivi, migliorare la qualità dei prodotti e ridurre i tempi di sviluppo grazie all'automazione avanzata. La personalizzazione e l'efficienza che l'intelligenza artificiale su misura può offrire consentono alle aziende italiane di rispondere più rapidamente alle esigenze del mercato, differenziandosi rispetto alla concorrenza globale.

Il Private AI offre quindi un insieme di vantaggi che vanno oltre la semplice implementazione tecnologica, incidendo profondamente sulla competitività, l'innovazione e l'autonomia delle aziende italiane. Grazie a soluzioni su misura, protezione del know-how e accesso democratizzato per le PMI, l'industria italiana può trarre grandi benefici dall'integrazione dell'intelligenza artificiale privata nei suoi processi, preservando al contempo il proprio carattere distintivo e le sue competenze uniche.

11.1. Valorizzare le eccellenze nazionali attraverso modelli AI su misura

L'Italia è conosciuta a livello internazionale per le sue eccellenze, specialmente nei settori della moda, del design, dell'agroalimentare e della meccanica di precisione. Ciò che rende uniche le aziende italiane, specialmente le medie imprese, è la capacità di produrre beni di alta qualità, con un forte accento sulla tradizione e sull'artigianalità. Il Private AI può avere un ruolo determinante nel valorizzare queste eccellenze, creando soluzioni che rispettano e potenziano le specificità di ogni settore.

Fashion - Ad esempio, nel caso di un'azienda italiana di pelletteria di lusso. Utilizzare un modello AI su misura per gestire la catena di approvvigionamento potrebbe consentire all'azienda di ottimizzare l'acquisto delle materie prime, ridurre gli sprechi e assicurarsi che ogni fase della produzione mantenga gli standard di qualità tradizionali. Inoltre, la differenza rispetto all'utilizzo di un sistema standard esterno è che l'AI privata sarebbe costruita per comprendere i ritmi produttivi, i tempi di lavorazione manuale e la qualità dei materiali specifici di quell'azienda, integrandosi armoniosamente nei processi artigianali senza comprometterli.

Agroalimentare - Nel settore agroalimentare, una cantina vinicola che esporta in tutto il mondo potrebbe sviluppare un'AI che analizza le condizioni metereologiche, il terreno e il ciclo di vita delle viti per prevedere la qualità della vendemmia, permettendo di prendere decisioni informate e strategiche sul processo di vinificazione, preservando il carattere unico del vino prodotto. Qui, l'AI non sostituisce l'esperienza dell'enologo, ma amplifica le sue capacità, permettendo all'azienda di migliorare i propri risultati mantenendo la propria identità distintiva.

Meccanica - Un altro esempio: un'azienda di meccanica di precisione potrebbe utilizzare un'AI privata per migliorare i processi produttivi. L'intelligenza artificiale, integrata nel ciclo produttivo, può analizzare in tempo reale i dati provenienti dalle macchine per ottimizzare l'uso delle risorse e ridurre al minimo i tempi di fermo, garantendo una migliore efficienza per mantenere la leadership nel settore.

Pharma - Nel settore farmaceutico, l'Italia si distingue per una lunga tradizione di eccellenza nella produzione di farmaci e nella ricerca clinica. In questo contesto, un modello di AI privata potrebbe supportare lo sviluppo di nuovi farmaci e trattamenti personalizzati, analizzando grandi volumi di dati clinici e genetici in maniera sicura.

L'AI potrebbe anche essere utilizzata per ottimizzare le sperimentazioni cliniche, analizzando i risultati in tempo reale per prendere decisioni più rapide e informate, riducendo i tempi di

sviluppo e migliorando la precisione delle terapie, riducendo nel contempo la dipendenza da piattaforme globali e proteggendo al tempo stesso il valore strategico delle ricerche farmaceutiche avanzate.

Retail - Citiamo solo un'altra casistica, ma la lista, è evidente, sarebbe infinita. In ambito retail, un negozio di abbigliamento potrebbe beneficiare di un'AI su misura per analizzare i comportamenti dei clienti e personalizzare l'offerta, migliorando la gestione degli stock e prevedendo la domanda in base alle tendenze, anche locali. L'utilizzo di una AI privata garantirebbe la protezione delle informazioni sensibili sui clienti e i dati esclusivi sui trend di consumo, in modo da preservare il vantaggio competitivo in un mercato sempre più globale.

11.2.Evitare la dispersione di know-how strategico: mantenere l'innovazione in Italia

Non solo tecnologia, ma tutela delle competenze ed esperienze. Tra le principali preoccupazioni delle aziende italiane, specialmente quelle che hanno un know-how specifico e altamente qualificato, è la dispersione di informazioni strategiche. Esternalizzare la gestione dei dati o affidarsi a grandi piattaforme internazionali di AI potrebbe esporre al rischio che queste competenze siano trasferite o replicate altrove, perdendo un vantaggio competitivo fondamentale.

Evitare la dispersione di know-how strategico è fondamentale per preservare la competitività e l'identità distintiva delle aziende italiane. Il Private AI, con la sua capacità di operare in ambienti sicuri e controllati, consente alle imprese di sfruttare i vantaggi dell'intelligenza artificiale senza rischiare che il loro know-how, fatto di creatività, di stile e di conoscenza del mercato locale nei settori chiave venga disperso o utilizzato da terzi.

Meccanica di precisione - In questo settore, l'innovazione tecnologica si fonda sull'esperienza e sull'expertise dei tecnici italiani, che spesso hanno una conoscenza profonda di tecniche produttive uniche. Utilizzando un'AI privata, un'azienda di meccanica può ottimizzare il ciclo produttivo e gestire in tempo reale l'analisi dei dati provenienti dalle macchine. Questo consente di mantenere in-house le tecniche di produzione avanzate e di proteggere il know-how esclusivo. Ad esempio, i parametri tecnici precisi, l'uso ottimale dei materiali e le procedure di calibrazione possono essere preservati all'interno di un contesto AI privato, riducendo il rischio che queste informazioni finiscano nelle mani di competitor globali.

Pharma - Il settore farmaceutico italiano è riconosciuto per le sue innovazioni scientifiche e i progressi nella ricerca clinica. La private AI permette alle aziende farmaceutiche di proteggere le proprie scoperte e i dati di ricerca clinica sensibili. Ad esempio, durante la fase di sviluppo di un nuovo farmaco, i dati relativi alle prove cliniche e ai modelli di previsione della risposta ai trattamenti sono estremamente preziosi. Grazie alla private AI, le aziende possono mantenere questi dati al sicuro, evitando che vengano condivisi involontariamente con concorrenti o soggetti esterni, preservando così il proprio vantaggio competitivo e mantenendo l'innovazione nel Paese.

Fashion - Nel settore della moda, la creatività e il design sono il cuore pulsante del successo delle aziende italiane. Utilizzando un modello AI su misura, un'azienda di moda potrebbe integrare l'intelligenza artificiale per analizzare tendenze, gestire la produzione e ottimizzare la logistica, senza mai rinunciare alla protezione del proprio know-how creativo e stilistico. Ad esempio, un'AI privata potrebbe aiutare un'azienda di pelletteria a ottimizzare il processo

di lavorazione manuale, preservando i dettagli artigianali che caratterizzano i suoi prodotti, proteggendo i dati relativi alle tecniche di lavorazione e agli stili specifici, senza il rischio di condividerli con partner o hyperscaler globali.

Retail - Nel settore del retail, l'AI privata può essere utilizzata per personalizzare l'offerta ai clienti in base alle preferenze locali, mantenendo il controllo sui dati relativi ai comportamenti dei consumatori e alle tendenze di mercato specifiche di ogni regione. Ad esempio, un retailer italiano che vende abbigliamento potrebbe usare un modello AI per analizzare in modo sicuro le preferenze dei clienti in diverse regioni d'Italia, personalizzando l'inventario e le offerte promozionali senza dover condividere i dati di vendita o di comportamento con un hyperscaler globale. Questo mantiene il vantaggio strategico locale, poiché le informazioni sui trend e sulle abitudini di consumo non vengono disperse al di fuori dell'azienda.

Agroalimentare - Nel settore agroalimentare, l'Italia è conosciuta per i suoi prodotti di alta qualità e le tradizioni culinarie radicate nel territorio. Un'AI privata può aiutare a ottimizzare la produzione, garantendo che le tecniche tradizionali di coltivazione e lavorazione siano mantenute intatte. Ad esempio, una cantina vinicola italiana potrebbe utilizzare un modello AI per monitorare il terreno e il clima, ottimizzando la qualità della produzione senza rischiare di perdere informazioni sui metodi di vinificazione unici e di alta qualità che distinguono il proprio prodotto sul mercato internazionale. Il know-how tradizionale viene così protetto e tramandato, mentre l'azienda continua a migliorare l'efficienza grazie all'AI.

In tutti questi settori, l'adozione di soluzioni AI private rappresenta un baluardo contro la dispersione del know-how strategico, permettendo alle eccellenze italiane di sfruttare la tecnologia mantenendo l'innovazione e la creatività radicata nel tessuto industriale e artigianale del Paese.

11.3.Il ruolo delle PMI: democratizzare l'accesso all'AI senza dipendere dai grandi player internazionali

Le piccole e medie imprese sono il cuore pulsante dell'economia italiana, ma spesso trovano difficoltà nell'accedere a tecnologie avanzate come l'intelligenza artificiale a causa dei costi e della complessità iniziale di implementazione. Nonostante la Private AI richieda un investimento iniziale non trascurabile, nel lungo termine si rivela una scelta strategicamente vantaggiosa. A differenza dei servizi offerti dagli operatori globali, che comportano costi operativi continui e la dipendenza da terze parti, una soluzione di Private AI consente alle PMI di mantenere il controllo completo sui dati aziendali, tutelando la loro proprietà intellettuale e riducendo i costi su scala. In questo modo, anche le imprese più piccole possono accedere a strumenti personalizzati che migliorano efficienza e competitività.

Inoltre, l'evoluzione delle tecnologie AI e la maggiore disponibilità di strumenti open source o customizzabili stanno gradualmente abbattendo le barriere d'ingresso, permettendo alle PMI di avviare progetti più accessibili. La Private AI democratizza l'accesso all'innovazione senza compromessi sul controllo dei dati, stimolando un ecosistema industriale più inclusivo, dove anche le aziende di dimensioni minori possono competere ad armi pari con le grandi multinazionali, preservando però il proprio carattere distintivo e la propria autonomia tecnologica.

12.Come implementare una Private AI: linee guida operative

L'implementazione di una Private AI richiede un approccio strutturato che comporta una serie di decisioni strategiche e tecniche, a partire dalla scelta dell'infrastruttura su cui appoggiarsi, alle tecnologie di machine learning da adottare e alle metodiche di addestramento dei modelli AI.

12.1.Scelta dell'infrastruttura: cloud privato, on-premise o hybrid cloud

La prima fase nell'implementazione di una Private AI riguarda la **scelta dell'infrastruttura** su cui verrà eseguito il motore AI. Le opzioni principali sono il cloud privato, l'on-premise e l'hybrid cloud, ognuna con caratteristiche peculiari, da considerare in base alle esigenze/possibilità delle singole aziende.

Il **cloud privato,** ambiente di calcolo dedicato all'azienda e offerto da un provider di cloud, ha il pregio di fornire flessibilità e al contempo isolamento delle risorse, garantendo un elevato controllo sui dati, e rappresenta l'opzione ideale per coniugare scalabilità e gestione dei dati in un ambiente chiuso e sicuro.

In alternativa, l'**on-premise** prevede la gestione dei server fisici direttamente in azienda, permettendo un controllo completo sui dati e sui sistemi. Una scelta che ovviamente comporta costi impegnativi e richiede competenze tecniche specifiche per gestire e mantenere l'infrastruttura hardware e software.

Infine, l'**hybrid cloud** combina i vantaggi delle due soluzioni precedenti: consente di mantenere i dati sensibili in locale, mentre il cloud può essere utilizzato per gestire applicazioni meno critiche o per espandere la capacità di calcolo, garantendo flessibilità e ottimizzando sicurezza ed efficienza operativa.

12.2.Modellare un motore AI proprietario: processi, tecnologie e competenze necessarie

Una volta definita l'infrastruttura, il passaggio successivo è modellare un motore AI proprietario, processo che richiede un'attenta pianificazione. È importante stabilire

chiaramente gli obiettivi aziendali che l'AI dovrà supportare, come, ad esempio, migliorare l'efficienza operativa, ottimizzare le decisioni aziendali o potenziare le capacità di analisi predittiva. Le tecnologie utilizzate per creare il motore AI includono strumenti di machine learning come **TensorFlow** o **PyTorch**, oltre a risorse hardware avanzate come **GPU** (Graphic Processing Unit)[6] o **TPU** (Tensor Processing Unit), necessarie per accelerare l'addestramento dei modelli.

In ogni caso, il successo di un progetto AI dipende anche dalle **competenze** presenti in azienda: data scientist, ingegneri del machine learning e sviluppatori AI sono figure chiave per lo sviluppo, l'implementazione e la manutenzione del sistema. Potrebbe essere utile formare un team interno o collaborare con partner esterni specializzati.

Si consiglia comunque di iniziare sempre con **prototipi limitati** (PoC) per testare il funzionamento del motore AI su piccole parti dei dati aziendali, correggere eventuali problemi e ottimizzare il modello prima di scalare.

12.3.Integrazione di soluzioni open source nel motore AI proprietario

L'integrazione di soluzioni open source all'interno di un motore AI proprietario può essere una scelta strategica per molte aziende, poiché consente di accedere a un'ampia gamma di **librerie e framework** (TensorFlow, PyTorch e Hugging Face), senza dover investire enormi risorse nello sviluppo da zero. Questa opzione non solo riduce drasticamente i costi associati alle licenze di software proprietario, ma è particolarmente vantaggiosa per le PMI che possono sfruttare questi strumenti senza affrontare pesanti investimenti iniziali.

Inoltre, la natura open source[7] favorisce una continua collaborazione con la **Community** globale di sviluppatori e ricercatori, che contribuiscono costantemente al miglioramento e all'innovazione delle soluzioni. Questo ambiente dinamico permette alle aziende di restare sempre all'avanguardia senza essere legate a vendor specifici. Un ulteriore vantaggio è poi la **trasparenza del codice**, che consente alle imprese di effettuare audit interni per garantire che non vi siano vulnerabilità o backdoor, aumentando così la sicurezza dei propri sistemi.

L'open source, infine, risponde anche a esigenze di **conformità normativa**, specialmente in ambito europeo, offrendo piena visibilità e tracciabilità del codice utilizzato. La sua flessibilità consente una **personalizzazione totale** delle soluzioni AI, permettendo alle aziende di adattare i modelli alle proprie necessità, riducendo al minimo il rischio di lock-in tecnologico con fornitori esterni e aumentando la loro competitività.

12.4.Strategie di addestramento: utilizzare dati interni senza compromettere la riservatezza

Un aspetto fondamentale nell'addestramento dei modelli è la gestione dei dati. Le aziende devono sviluppare **strategie di addestramento** che sfruttino al massimo i dati interni senza intaccarne la riservatezza. Utilizzare tecniche come il **federated learning** consente di addestrare i modelli AI senza trasferire effettivamente i dati, mantenendo così la loro privacy. Implementare processi di anonimizzazione e crittografia garantisce che i dati sensibili rimangano protetti durante l'addestramento dei modelli, aspetto particolarmente importante per la conformità a normative come il GDPR.

---

[6] Il GPU Computing o "high performance computing" è fondamentale per l'intelligenza artificiale: https://blog.seeweb.it/server-per-intelligenza-artificiale-caratteristiche/

[7] Un esempio di framework AI opensource è quello di Stregatto, creato da Piero Savastano: https://stregattoai.altervista.org/

12.5.Integrazione con i processi aziendali esistenti per garantire l’efficacia operativa

Per ottenere il massimo dall'intelligenza artificiale, è fondamentale che possa essere integrata senza difficoltà nei processi aziendali esistenti. L'integrazione con i processi aziendali richiede una mappatura approfondita delle operazioni correnti per identificare i punti in cui l'AI può avere l'impatto più significativo. L'automazione dovrebbe essere introdotta gradualmente, iniziando con piccole implementazioni per testare e adattare il sistema. La formazione del personale è altrettanto importante: chi lavora in azienda deve comprendere i benefici della tecnologia AI e sentirsi preparato a utilizzare i nuovi strumenti senza timori o resistenze.

12.6.Integrazione con un cloud nazionale

Per le aziende che vogliono mantenere la sovranità sui propri dati, un'opzione da considerare è l'integrazione con un cloud nazionale, che garantisce che i dati aziendali siano gestiti all'interno della giurisdizione del proprio Paese, riducendo i rischi legati all'esposizione dei dati a normative straniere. Il cloud nazionale offre anche garanzie di sicurezza e conformità normativa, scelta strategica per le imprese che vogliono proteggere le informazioni sensibili.

12.7.Sicurezza e protezione dei dati

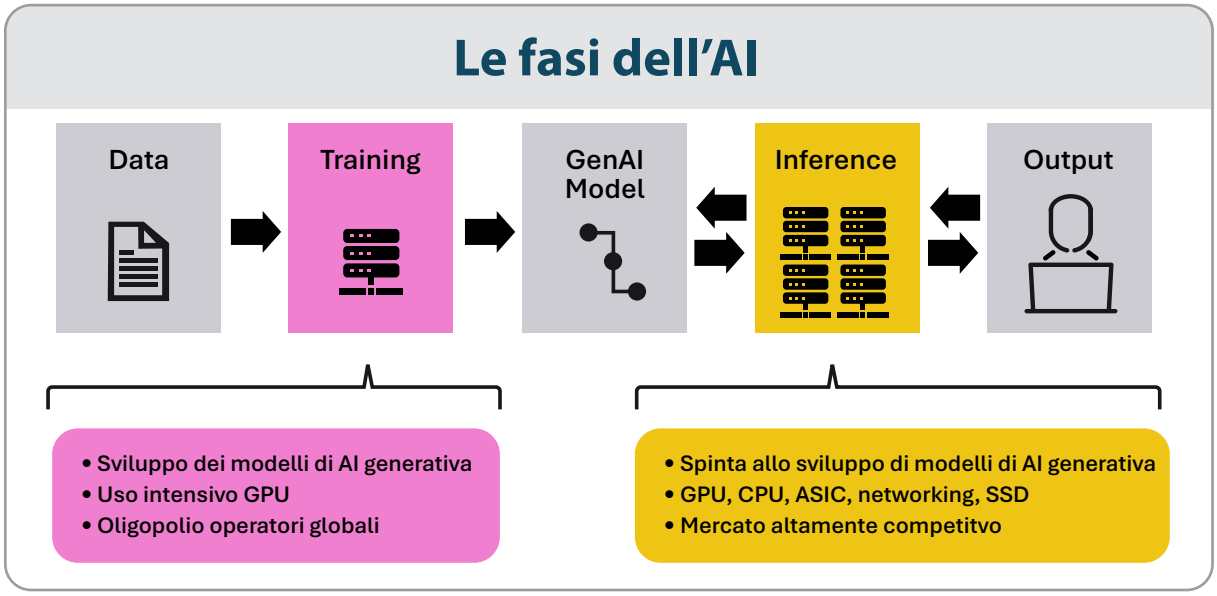
Infine, un elemento imprescindibile di ogni progetto di Private AI è la sicurezza e protezione dei dati. La **crittografia** avanzata dovrebbe essere utilizzata sia per i dati a riposo che per quelli in transito, in modo da garantirne la protezione contro accessi non autorizzati. I sistemi di **controllo degli accessi**, basati sui ruoli (RBAC – Role Based Access Control), devono limitare chi può accedere ai dati sensibili. È consigliabile implementare anche un'**autenticazione multifattore** per aumentare la sicurezza complessiva del sistema. Le aziende dovrebbero inoltre disporre di piani chiari di **incident response**, in modo da poter reagire rapidamente in caso di violazioni di sicurezza, e condurre audit regolari per monitorare l'integrità del sistema e individuare eventuali vulnerabilità.

Linee guida che valgono in generale, ma che **nel caso delle PMI** devono considerare alcuni aspetti, come la mancanza di budget e di know-how specifico, che può ostacolare l'adozione di soluzioni AI avanzate. In questi casi, un approccio progressivo, iniziando con progetti pilota e utilizzando tecnologie open source o soluzioni pronte all'uso, può aiutare a ridurre i costi

iniziali. Inoltre, le PMI possono cercare partner esterni o **supporto governativo** per colmare il gap di competenze e fondi necessari, potendo beneficiare di incentivi pubblici o di eventuali programmi di supporto promossi dal governo o dalle associazioni di categoria, mirati a favorire l'adozione di tecnologie avanzate come l'AI.

13.Le fasi dell'addestramento di un modello AI - training, fine-tuning, inferenza e RAG

Le quattro principali fasi dell'addestramento di un modello AI sono la fase di **training**, in cui il modello apprende dai dati; il **fine-tuning**, per adattarlo a esigenze specifiche; l'**inferenza**, dove il modello applica quanto appreso; e il **RAG** (Retrieval-Augmented Generation), che combina l'AI con fonti esterne per risposte più accurate. Già queste fasi, se sviluppate in un contesto di Private AI, possono offrire vantaggi distinti rispetto alle soluzioni generalistiche, garantendo maggiore personalizzazione, controllo sui dati e ottimizzazione delle risorse.



13.1.Training

La fase di training in un modello di Private AI è un momento da gestire con estrema attenzione, per garantire che l'intelligenza artificiale si adatti alle esigenze specifiche dell'azienda e del settore di riferimento. In contrasto, appunto, con le soluzioni generalistiche degli hyperscaler.

Il training è la fase in cui il modello AI viene addestrato su grandi quantità di dati per imparare a riconoscere schemi e relazioni, sviluppando capacità di previsione e automazione. Il training può essere supervisionato, semi-supervisionato o non supervisionato, a seconda del tipo di dati e delle esigenze aziendali.

13.1.1.Vantaggi di una Private AI nella fase di Training:

Personalizzazione profonda - Nelle soluzioni Private AI, l'addestramento può essere fatto utilizzando dataset altamente specifici, che riflettono le particolarità dell'azienda o del

settore. Ad esempio, un'azienda che opera nella meccanica di precisione può addestrare il modello su dati unici, acquisiti dalle sue linee di produzione o dai suoi fornitori, garantendo una precisione superiore rispetto ai modelli generali forniti dagli hyperscaler, che non hanno accesso a tali dati.

Sovranità dei dati - Uno dei vantaggi principali della Private AI è la protezione e il controllo sui dati. Il processo di training avviene su infrastrutture private o cloud nazionali, mantenendo così la sovranità e la riservatezza dei dati aziendali, spesso critici in settori regolamentati come il pharma o l'agroalimentare.

Raffinamento continuo - L'AI può essere addestrata continuativamente in base all'evoluzione delle esigenze dell'azienda, con aggiornamenti frequenti che riflettono nuove informazioni o cambiamenti del mercato. Questo è particolarmente vantaggioso rispetto agli hyperscaler, i cui modelli standard tendono a essere statici o aggiornati globalmente, senza tener conto delle peculiarità locali.

Ottimizzazione delle risorse - Nel contesto di Private AI, l'azienda ha la possibilità di ottimizzare l'allocazione delle risorse computazionali per il training. I modelli possono essere progettati per adattarsi alle capacità hardware specifiche, riducendo il consumo di risorse e i costi rispetto ai modelli predefiniti offerti dagli hyperscaler, che possono essere sovradimensionati per molte realtà aziendali.

Trasparenza e controllo - Le aziende che sviluppano una Private AI possono avere pieno accesso ai processi di training, comprese le metriche di performance e i meccanismi di apprendimento. Al contrario, i modelli degli hyperscaler spesso funzionano come “black box”, senza possibilità di intervento diretto o personalizzazione del processo di training.

Sfide che diventano opportunità

La fase di training richiede spesso grandi risorse computazionali e dati di alta qualità, ma con l'uso di Private AI le aziende possono sfruttare soluzioni cloud ibride o nazionali per bilanciare i costi e garantire efficienza, mantenendo il controllo sui dati.

Inoltre, la fase di training può essere affiancata da specialisti interni o da partner di fiducia, contribuendo allo sviluppo di competenze locali in ambito AI, favorendo un ecosistema nazionale forte.

13.2.Fine-tuning

Il fine-tuning nei modelli AI è un processo fondamentale che segue il training. Una volta che il modello è stato addestrato su un dataset generico, il fine-tuning permette di raffinare ulteriormente il modello utilizzando dati specifici per un’applicazione particolare, adattandolo così alle esigenze precise dell’azienda. In questo modo, si sfrutta la base di un modello già pre-addestrato, evitando di ricominciare da zero e risparmiando notevoli risorse.

Adattamento specifico - Il fine-tuning in un contesto di Private AI consente di sfruttare un modello generico e personalizzarlo con dati proprietari che rispecchiano le peculiarità

aziendali. In settori come il fashion o la meccanica di precisione, ad esempio, il modello può essere affinato per cogliere dettagli unici che un'AI generalistica non riuscirebbe a rilevare.

Risparmio di risorse e tempo - Il fine-tuning riduce la necessità di avviare un training completo, risparmiando tempo e risorse computazionali. Le aziende possono focalizzarsi su aree specifiche di miglioramento senza investire enormemente in infrastrutture o processi, rendendo la Private AI più accessibile anche a realtà di medie dimensioni.

Controllo e sovranità - Il controllo sui dati e sul modello rimane nelle mani dell'azienda. Spesso, i modelli di hyperscaler sono forniti come "black box", con limitate possibilità di intervento. Con la Private AI, invece, le aziende possono effettuare un fine-tuning con piena trasparenza, sapendo esattamente quali modifiche vengono apportate.

Competitività e unicità - Il fine-tuning consente di differenziarsi dai concorrenti, creando soluzioni che riflettono al 100% i requisiti aziendali. Anche se molte aziende affermano di possedere un proprio modello AI, spesso ciò che realmente fanno è effettuare il fine-tuning su un modello di terzi, spesso preso in licenza (sia a pagamento che open-source). Tuttavia, con Private AI, l'azienda può mantenere un controllo maggiore sul risultato finale.

13.3.Inferenza

La fase di **inferenza** in un modello AI è il momento in cui il sistema, dopo essere stato addestrato e affinato, viene utilizzato per fare previsioni o classificazioni su nuovi dati, ovvero su input che non ha mai visto prima. È qui che l'AI entra in azione per risolvere problemi reali e fornire valore concreto, ad esempio identificando oggetti in un'immagine o generando raccomandazioni basate su pattern appresi.

Caratteristiche dell'Inferenza - Durante l'inferenza, il modello applica quanto appreso nelle fasi precedenti (training e fine-tuning) per produrre risultati che rispondano a specifiche esigenze aziendali.

Questa fase può essere eseguita con architetture efficienti che minimizzano o addirittura eliminano l'uso di GPU, soprattutto se il modello è stato ottimizzato per funzionare su CPU o dispositivi edge, riducendo così i costi operativi e migliorando la scalabilità.

13.3.1.Vantaggi per chi adotta una Private AI

Ottimizzazione personalizzata - Con una Private AI, le aziende possono ottimizzare l'inferenza per funzionare sulle loro infrastrutture esistenti. Invece di dipendere da risorse di calcolo esterne, come nel caso degli hyperscaler, il modello può essere eseguito in locale o su un cloud privato, riducendo i costi e il consumo di risorse.

Maggiore controllo sui tempi di risposta - Le soluzioni di Private AI permettono di mantenere un controllo rigoroso sulle latenze e sui tempi di risposta. Questo è particolarmente vantaggioso in contesti industriali o in applicazioni critiche dove è essenziale che i risultati siano generati in tempo reale o con un ritardo minimo, come nel settore della meccanica di precisione o della sicurezza.

Rispetto della sovranità dei dati - Durante la fase di inferenza, soprattutto quando si tratta di elaborare dati sensibili (ad esempio, nel settore medico o finanziario), l'adozione di una Private AI garantisce che i dati non escano mai dall'infrastruttura controllata dall'azienda. Questo aumenta la sicurezza e conformità alle normative, riducendo i rischi legati alla gestione esterna dei dati.

Efficienza in ambienti edge - Una Private AI può essere configurata per l'inferenza su dispositivi edge o periferici, come sensori o macchine industriali, senza la necessità di inviare dati a server centrali. Questo approccio è particolarmente vantaggioso per applicazioni distribuite, dove l'accesso ai dati deve essere rapido e locale, riducendo così la dipendenza dalla connessione internet.

13.4.RAG (Retrieval-Augmented Generation)

Il RAG (Retrieval-Augmented Generation) rappresenta una fase avanzata nell'evoluzione dei modelli AI, particolarmente rilevante per i sistemi documentali e le applicazioni che richiedono la gestione di grandi quantità di informazioni testuali. RAG combina due componenti fondamentali: il **recupero di informazioni**, ossia un modulo di ricerca che scansiona un corpus di dati esistente per trovare informazioni rilevanti e la **generazione di testo**, che è un modulo di generazione che utilizza le informazioni recuperate per produrre risposte coerenti, dettagliate e contestualizzate.

Questo approccio si rivela particolarmente utile per applicazioni come i **chatbot intelligenti**, i sistemi di **compilazione automatica di documenti legali o amministrativi**, e altre situazioni in cui il modello deve rispondere in modo accurato basandosi su dati preesistenti che sono difficilmente accessibili manualmente.

13.4.1.Vantaggi del RAG in una Private AI:

Accesso e gestione di dati aziendali riservati - Una delle maggiori potenzialità della Private AI nell'ambito del RAG è la possibilità di accedere a corpus documentali interni e riservati, mantenendo tutto il processo all'interno dell'infrastruttura aziendale. Questo è particolarmente importante per documenti legali, amministrativi, contratti, report tecnici o altro materiale sensibile, che non dovrebbe essere esposto su piattaforme esterne.

Personalizzazione e contesto aziendale - Le soluzioni Private AI permettono di affinare il modulo di recupero su fonti specifiche, come archivi documentali interni, CRM aziendali, manuali tecnici, o banche dati personalizzate. Ciò consente di generare risposte non solo pertinenti, ma anche altamente contestualizzate al linguaggio e alle pratiche specifiche dell'azienda, migliorando notevolmente l'efficienza rispetto a modelli generalistici.

Efficienza nei flussi di lavoro - L'adozione del RAG in una Private AI può ottimizzare flussi di lavoro complessi, come la redazione di contratti, regolamenti, o documenti legali, che richiedono spesso la consultazione di vasti corpus documentali. La capacità di estrarre informazioni rilevanti in modo rapido e preciso da migliaia di documenti riduce drasticamente

il tempo e il lavoro umano necessari, rendendo il sistema particolarmente utile per settori come il legale, la sanità, e la finanza.

Controllo sulla qualità delle risposte - Nelle soluzioni hyperscaler, il modulo di generazione spesso si basa su fonti di dati generiche e potenzialmente inadeguate per contesti aziendali specifici. Con una Private AI, invece, le risposte prodotte dal sistema RAG possono essere monitorate e raffinate direttamente dall'azienda, che ha il pieno controllo sia sui dati recuperati che sul modo in cui vengono utilizzati, garantendo una maggiore accuratezza e qualità delle risposte.

Sicurezza e conformità normativa - Settori regolamentati come la finanza, la sanità o il settore legale beneficiano enormemente dall'adozione di Private AI, perché il processo di recupero e generazione può essere limitato a risorse conformi alle normative di sicurezza e protezione dei dati. Utilizzare RAG su un'infrastruttura privata o ibrida consente di mantenere i dati sempre protetti e conformi a leggi come il GDPR.

14.Il ruolo strategico dell’ecosistema italiano ed europeo nell’AI

Per il futuro dell'economia italiana ed europea, specialmente nel contesto della sovranità tecnologica e della competitività globale, l’intelligenza artificiale sta assumendo un ruolo sempre più rilevante. Il suo sviluppo richiede un supporto politico, strategico ed economico, poiché le sue applicazioni diventeranno parte integrante della quotidianità delle aziende e delle Pubbliche Amministrazioni, influenzando direttamente produttività, innovazione e autonomia decisionale. Creare un ecosistema AI nazionale ed europeo significa costruire una rete di investimenti, formazione e infrastrutture condivise, favorendo una crescita tecnologica che garantisca trasparenza, sicurezza e indipendenza.

Una strategia che sia efficace in questa direzione deve comprendere misure concrete per rafforzare la capacità di innovazione e sviluppo nel territorio. La creazione di infrastrutture tecnologiche nazionali e sovranazionali, il sostegno alla formazione e alle competenze avanzate, la promozione della collaborazione tra pubblico e privato e la tutela del know-how europeo sono elementi chiave per ridurre la dipendenza dai grandi provider internazionali. In questo scenario, il procurement pubblico può diventare uno strumento determinante per rafforzare le industrie locali, incentivando soluzioni progettate e sviluppate in Europa e contribuendo alla crescita di un mercato in cui le aziende europee possano competere con maggiore autonomia.

Perché tutto questo si possa concretizzare, le innovazioni nel campo dell’intelligenza artificiale devono essere sviluppate e registrate in Europa, evitando la dispersione del valore tecnologico e della conoscenza. Favorire l’adozione di licenze aperte e modelli open-source permette di consolidare un sistema in cui le imprese possano collaborare e personalizzare le soluzioni senza dipendere da tecnologie esterne. Un impegno in questa direzione consentirebbe di trasformare l’Europa in un punto di riferimento per l’innovazione tecnologica, creando un ambiente competitivo e sostenibile capace di rispondere alle esigenze del mercato con flessibilità e autonomia.

14.1.La necessità di sviluppare un ecosistema AI nazionale o europeo: ridurre la dipendenza dagli altri Paesi

La crescente centralità dell'AI sta trasformando settori chiave come l'industria manifatturiera, i servizi finanziari, la sanità e l'agricoltura. A oggi, gran parte delle infrastrutture e delle tecnologie AI proviene da aziende statunitensi e cinesi, come Amazon, Google, Microsoft o Alibaba. Una dipendenza dagli hyperscaler internazionali che non solo espone le aziende europee a rischi legati alla sovranità dei dati, ma limita anche il controllo sulle innovazioni future.

L'obiettivo di sviluppare un ecosistema AI nazionale o europeo è dunque quello di costruire una solida infrastruttura tecnologica autonoma che permetta di gestire dati sensibili, garantire la privacy dei cittadini e promuovere l'innovazione all'interno del continente. Questi sforzi devono essere rafforzati per includere l'intero ciclo di vita dell'AI, dalle piattaforme di calcolo all'analisi dei dati e alla distribuzione dei modelli di intelligenza artificiale.

14.2.Politiche e investimenti: incentivi per le aziende che investono in soluzioni AI private

Per supportare lo sviluppo di un ecosistema AI, servono politiche mirate e incentivi che incoraggino le aziende a investire in soluzioni private. In Italia, il Piano Nazionale di Ripresa e Resilienza destina una buona parte delle risorse all'innovazione digitale, includendo il potenziamento delle tecnologie emergenti come l'AI. All'interno del PNRR, l'iniziativa "Transizione 4.0" offre **incentivi fiscali e crediti d'imposta** per le aziende che investono in digitalizzazione e AI, consentendo alle imprese di ricevere un credito d'imposta fino al 50% sugli investimenti in ricerca e sviluppo, compresi i progetti di AI, migliorando la competitività e riducendo i costi di accesso alla tecnologia.

A livello europeo, il programma **Horizon Europe** finanzia progetti di ricerca e innovazione nell'AI attraverso bandi specifici, come il bando **AI, Data and Robotics**.

Il programma ha l'obiettivo di rafforzare la competitività europea e di supportare le aziende che sviluppano nuove soluzioni AI per affrontare mercati sempre più globalizzati. I fondi disponibili contano di oltre **95 miliardi di euro** stanziati per il periodo 2021-2027, di cui una parte destinata specificamente all'AI.

(*altri dettagli e informazioni per la partecipazione ai bandi si possono trovare su Funding & Tenders Portal https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/home*)

14.3.Formazione e sviluppo delle competenze: colmare il gap tecnologico attraverso programmi mirati

Uno dei principali ostacoli alla diffusione dell'AI in Italia ed Europa è la mancanza di competenze. Molte aziende, specialmente le PMI, non hanno personale qualificato per sviluppare, implementare e gestire sistemi di AI e per colmare questo gap è necessario investire nella formazione e nello sviluppo degli skill attraverso programmi mirati.

In Italia, progetti come **Digital Talent** (https://innovazione.gov.it/argomenti/competenze-digitali/) e il **Fondo Nuove Competenze** (https://myanpal.anpal.gov.it/myanpal/) supportato dal PNRR, forniscono formazione continua per aggiornare i lavoratori sulle competenze digitali, tra cui l'intelligenza artificiale. Inoltre, le università italiane stanno intensificando i corsi in data science e AI per formare una nuova generazione di professionisti qualificati.

A livello europeo, l'iniziativa **European Digital Innovation Hubs** (EDIH) supporta le aziende nell'accesso a tecnologie avanzate come l'AI, promuovendo la formazione dei dipendenti e facilitando l'adozione di soluzioni digitali. Gli EDIH forniscono anche consulenze tecniche e organizzano corsi di aggiornamento per favorire l'adozione dell'AI nelle PMI e nelle startup. Questi hub rappresentano una risorsa preziosa per le aziende che vogliono esplorare le opportunità offerte dall'AI senza dover costruire competenze interne da zero.

14.4.Creazione di un'infrastruttura comune per sostenere l'innovazione basata su AI private

Lo sviluppo di un'AI privata richiede un'infrastruttura tecnologica robusta e condivisa, che permetta alle aziende di innovare senza dover dipendere da soluzioni proprietarie straniere. Da qui l'importanza di creare una infrastruttura comune, a livello nazionale ed europeo, per garantire che le imprese possano accedere a risorse computazionali, dati e strumenti di sviluppo necessari per implementare e scalare i propri progetti AI.

Il programma europeo **Digital Europe** (https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/digital)sta investendo nella costruzione di **supercomputer e centri di calcolo ad alte prestazioni (HPC)** per consentire alle aziende europee di accedere a risorse di calcolo potenti e sicure, fondamentali per l'addestramento di modelli AI su larga scala.

La creazione di queste infrastrutture comuni contribuisce alla riduzione dei costi per le singole imprese per accedere a tali risorse, oltre a favorire anche la collaborazione tra aziende, istituti di ricerca e Pubbliche Amministrazioni. Un modello di co-innovazione che permette di condividere dati e conoscenze, accelerando lo sviluppo di soluzioni AI avanzate in settori strategici come la Sanità, la Mobilità e l'Energia.

15.Cosa chiediamo ai Governi e all'Unione Europea

Lo sviluppo e la tutela delle tecnologie Private AI in Italia e in Europa richiedono un ruolo attivo dei governi e delle istituzioni europee, che potrebbero, dovrebbero, contribuire a sostenere le aziende nello sviluppo e nella protezione di tali tecnologie. Attraverso un insieme di politiche mirate, finanziamenti, regolamentazioni e iniziative di formazione, l'Italia e l'Unione Europea possono creare un ecosistema favorevole per lo sviluppo di tecnologie Private AI, riducendo la dipendenza dagli hyperscaler globali. Questo approccio non solo garantisce la sovranità tecnologica, ma rafforzerebbe la competitività delle aziende italiane ed europee nel lungo termine, mantenendo il know-how strategico e l'innovazione all'interno dei confini nazionali. Concetti che abbiamo già accennato nei capitoli precedenti, ma che riteniamo sia il caso di sottolinearli, essendo essenziali per potersi appropriare della tecnologia, dei dati, dell'expertise che caratterizzano la nostra economia. Perché sono nostri , sono preziosi e vanno sviluppati e tutelati.

15.1.Politiche di incentivi fiscali e finanziamenti

Per incentivare lo sviluppo di Private AI, il governo italiano e le istituzioni europee potrebbero attuare politiche di sgravi fiscali e agevolazioni per le aziende che investono in soluzioni AI proprie.

Credito d'imposta per le aziende che sviluppano infrastrutture e competenze AI in-house.

Fondi di ricerca e sviluppo specifici per l'AI privata, con finanziamenti dedicati per progetti che mirano a sviluppare tecnologie AI localizzate, sicure e personalizzate.

Finanziamenti per le PMI che potrebbero non avere le risorse finanziarie per sviluppare autonomamente infrastrutture AI, ma che rappresentano una parte vitale del tessuto produttivo italiano.

15.2. Creazione di infrastrutture nazionali e sovranazionali

L'Italia e l'Unione Europea potrebbero investire nella costruzione di **cloud nazionali** o **infrastrutture cloud europee** che consentano alle aziende di accedere a tecnologie AI senza dipendere dai provider globali.

In questo modo si potrebbe garantire che i dati sensibili e il know-how rimangano sotto il controllo delle aziende europee. Inoltre si potrebbero sviluppare infrastrutture comuni che abbiano criteri di sovranità digitale, garantendo l'accesso a piattaforme sicure per l'addestramento e l'implementazione di modelli AI.

15.3. Sovvenzioni per la formazione e lo sviluppo delle competenze

Le competenze nel campo dell'AI sono fondamentali per lo sviluppo di tecnologie Private AI. Il governo italiano, in collaborazione con l'Unione Europea, potrebbe investire in **programmi di formazione e riqualificazione** per sviluppare una forza lavoro con le competenze necessarie.

Finanziare **master universitari** e **corsi di specializzazione** in AI e data science, focalizzati sullo sviluppo e sull'implementazione di soluzioni AI private e attivare collaborazioni con istituzioni accademiche e aziende per creare **hub di innovazione** che promuovano lo scambio di conoscenze e lo sviluppo di tecnologie AI sicure e indipendenti.

15.4. Creazione di un quadro normativo chiaro e favorevole

Il governo italiano e l'UE potrebbero lavorare per sviluppare un **quadro normativo favorevole** al Private AI, attraverso regolamenti come il **Data Act** e l'**AI Act**.

Normative chiare potrebbero garantire che le aziende siano protette contro il rischio di lock-in con gli hyperscaler e possano mantenere il controllo sui propri dati, e una regolamentazione attenta per favorire la **portabilità dei dati** e che imponga che gli hyperscaler non possano addebitare costi elevati per la riconsegna dei dati, tutelando così le aziende che desiderano migrare verso soluzioni Private AI.

15.5. Promozione di partenariati pubblico-privati

Essenziale, inoltre, sarebbe la promozione di **collaborazione tra università, aziende e istituzioni pubbliche**, creando centri di eccellenza per l'AI. Oltre a incoraggiare la **condivisione di best practice** tra le aziende e gli istituti di ricerca italiani ed europei,

assicurando che il know-how sviluppato nel campo dell'AI rimanga all'interno dei confini europei.

15.6.Tutela del know-how strategico

Per proteggere l'innovazione e il know-how strategico delle aziende italiane, i governi dovrebbero inoltre introdurre misure specifiche per prevenire la **dispersione di proprietà intellettuale** sviluppata dalle aziende europee in favore di attori globali. Oltre a questo, incentivare l'uso di **licenze aperte e modelli open-source** per l'AI sviluppata in Europa, così da favorire l'accesso a tecnologie condivise pur mantenenod il controllo sulla distribuzione e lo sviluppo locale. Infine, implementare **meccanismi di protezione della proprietà intellettuale**, garantendo che le innovazioni AI siano brevettate e tutelate in Europa.

15.7.Supporto all'internazionalizzazione

Oltre a proteggere il know-how, il governo italiano e le istituzioni europee potrebbero supportare le aziende anche nell'espandere le loro tecnologie AI a livello internazionale, fornendo **sostegno all'export** e facilitando l'accesso ai mercati internazionali per le realtà che sviluppano AI private e promuovendo **accordi di cooperazione internazionale** che favoriscano lo scambio di dati e tecnologie senza compromettere la sovranità digitale europea.

I servizi infrastrutturali a supporto della Private AI

Che si tratti di un server locale o un'infrastruttura in cloud, uno dei requisiti più importanti per servire progetti di private AI e di intelligenza artificiale in senso ampio sono le GPU.

Le GPU, o Graphic Processing Unit, sono diventante una componente necessaria nello sviluppo e nel deploy dell'intelligenza artificiale in quanto in grado di processare, in parallelo, enormi quantità di dati.

Con la Private AI si può perseguire un approccio "privacy first" adottando infrastrutture GPU sia on premise che in cloud presso operatori europei che consentano piena compliance agli standard normativi.

L'approccio in cloud genera maggiore sostenibilità sia economica che ambientale, unendo i vantaggi di pagare il servizio a seconda dell'utilizzo a quello di mitigare l'impatto sul pianeta grazie a un utilizzo a consumo.

I servizi di Seeweb dedicati ai carichi di lavoro dell'intelligenza artificiale e del machine learning si ispirano a un approccio di democratizzazione dell'AI, normalmente molto costosa soprattutto per le aziende medio-piccole, e propongono a imprese e pubbliche amministrazioni una vasta gamma di servizi basati su schede grafiche molto potenti, con un modello di billing flessibile e il vantaggio di un servizio manutenuto, aggiornato e supportato da Seeweb.

In hosting sui data center dell'azienda parte del Gruppo DHH, i server cloud GPU di Seeweb consentono alle imprese e alla PA (sono qualificati ACN, ndr) di ospitare progetti di private AI efficientando costi e prestazioni, all'insegna della sostenibilità ambientale.

Per saperne di più: https://www.seeweb.it/prodotti/cloud-server-gpu

Private AI: competitività, sicurezza e sovranità per le aziende

Autore: **Loris Frezzato**

Giornalista professionista, da sempre specializzato nell'ambito IT con esperienza presso diversi editori e testate tra cui Computer Dealer&Var, Reseller Weekly e ICTBusiness Ecosystem.

Oggi collabora con importanti editori sempre nell'ambito IT e sue declinazioni, dal digitale all'AI.

Con il contributo Scientifico di: **EuropIA**
Un lavoro sponsorizzato da: **Seeweb**

Data pubblicazione Marzo 2025

Pubblicato nel mese di Marzo 2025

seeweb | Istituto EuroplA.it Comprendere per Agire