INTELLIGENZA ARTIFICIALE IN AZIENDA: GLI ALERT CHE L'IMPRENDITORE NON PUO' IGNORARE

L'adozione di strumenti di intelligenza artificiale in azienda non è, di per sé, un problema giuridico.

Il punto critico è **come** tali strumenti vengono concretamente utilizzati nei processi interni: sviluppo software, redazione documentale, analisi di file, gestione della produttività, trattamento di e-mail, codice, allegati, immagini e contenuti aziendali.

Dal quadro normativo d'insieme emerge con chiarezza che il vero rischio non sta nell'uso "in astratto" dell'AI, ma nell'assenza di regole, verifiche e limiti operativi.

In questa prospettiva, l'imprenditore deve evitare un equivoco molto diffuso: ritenere che uno strumento AI, solo perché acquistato con un account aziendale o messo a disposizione dal reparto IT, sia automaticamente utilizzabile su qualsiasi dato o documento dell'impresa.

Le cautele dettate dalla normativa vigente vanno in senso diametralmente opposto: l'uso degli strumenti deve essere **circoscritto, autorizzato, minimizzato e verificabile** .

1. Il primo errore: trattare l'AI come un normale software aziendale

La prima cautela **riguarda la governance**.

Gli strumenti AI non possono essere gestiti come un comune applicativo di produttività.

E' necessario definire in modo espresso:

- quali strumenti sono autorizzati;
- per quali finalità possono essere usati;
- quali categorie di dati non possono essere inserite;
- chi approva le eccezioni;
- quali controlli umani sono obbligatori;
- come devono essere gestiti incidenti, cancellazioni e richieste degli interessati.

L'alert per l'imprenditore è semplice: **senza policy interna, senza formazione e senza processo autorizzativo, l'uso dell'AI tende rapidamente a diventare incontrollato**.

E quando l'uso è incontrollato, **aumentano insieme il rischio privacy, il rischio di divulgazione di informazioni riservate e il rischio organizzativo.**

2. Privacy: non tutto ciò che è accessibile può essere caricato in AI

Uno dei principi più netti è che **la mera disponibilità di un dato non ne rende lecito l'inserimento in uno strumento di AI**.

In altri termini, il fatto che un dipendente possa accedere a un file, a un repository, a una e-mail o a un allegato non significa che possa trasmetterne il contenuto a un servizio AI.

Ne discende un alert molto pratico: **prima di usare l'AI bisogna chiedersi se il risultato può essere ottenuto con dati fake, dati anonimizzati, estratti limitati o contenuti redatti**.

Questa logica di minimizzazione è centrale e rappresenta una condizione di ammissibilità del trattamento.

3. Segretezza e riservatezza: il rischio più sottovalutato

Per l'imprenditore, il rischio più immediato non è sempre la sanzione privacy, ma spesso la **dispersione di know-how, credenziali, informazioni commerciali e segreti aziendali**.

In sostanza, la possibile trasmissione di segreti o dati personali da repository, nonché la presenza di credenziali e informazioni riservate nei sistemi aziendali.

Le mere istruzioni operative non equivalgono a un blocco tecnico effettivo.

Per l'impresa, questo significa che la sicurezza non può essere affidata solo alla diligenza del singolo utente o a indicazioni testuali; servono permessi, segregazione, controlli di accesso, limitazioni per directory e repository, e verifiche documentate.

4. Proprietà intellettuale e materiali coperti da vincoli contrattuali

Altro profilo decisivo è quello della proprietà intellettuale e della riservatezza contrattuale.

In quest'ottica si pone **la compatibilità con eventuali NDA, accordi di segretezza o clausole di riservatezza riferibili a clienti e/o partner.**

Per l'imprenditore questo passaggio è essenziale: **l'illecito può nascere anche senza violazione del GDPR**, per esempio quando vengono trasferiti a un sistema AI:

- documenti contrattuali riservati;
- materiale commerciale coperto da NDA;
- codice sorgente proprietario;
- contenuti di terzi protetti da obblighi di confidenzialità.

L'alert è quindi duplice: non solo "**che dati sto caricando?", ma anche "di chi sono quei contenuti?" e "quali vincoli contrattuali o proprietari li proteggono?".**

5. L'uso dell'AI non elimina il controllo umano

Il principio costante è che gli output dell'AI devono essere sempre sottoposti a **verifica umana effettiva**.

Ciò vale tanto per il codice quanto per i testi, i riepiloghi, le analisi documentali e i contenuti destinati a circolazione interna o esterna.

L'alert per l'imprenditore è molto concreto.

L'AI può produrre:

- errori tecnici;
- ricostruzioni inesatte;
- codice vulnerabile;
- testi apparentemente corretti ma giuridicamente o fattualmente inaffidabili;
- output che incorporano informazioni riservate o non pertinenti.

Ne consegue che **l'AI non può sostituire il giudizio professionale, il presidio del management o i controlli di conformità**.

Se l'impresa usa strumenti generativi per documenti, codice, policy, offerte, report o comunicazioni, deve sempre prevedere una revisione competente prima dell'uso effettivo.

6. Base giuridica, informative e diritti: i profili privacy da non banalizzare

Il legittimo interesse può operare solo in termini **condizionati e limitati**, non come base giuridica "automatica" per qualunque trattamento connesso all'AI.

Inoltre, è necessario verificare se l'uso di questi strumenti modifichi finalità, categorie di dati, destinatari, trasferimenti o modalità del trattamento in misura tale da richiedere l'aggiornamento delle informative.

L'imprenditore deve quindi porsi almeno tre domande:

1. **Per quale finalità sto usando l'AI?**
2. **Qual è la base giuridica del trattamento concretamente coinvolto?**
3. **Le informative e le procedure interne sono ancora coerenti con questo nuovo scenario?**

E' poi opportuno creare una procedura elettronica dedicata alla gestione delle richieste degli interessati, della cancellazione e della verifica della propagazione della cancellazione.

Ciò evidenzia un ulteriore alert: **se i dati transitano tra conversazioni, transcript, log, ticket, audit e backup, l'impresa deve sapere dove cercarli e come governarne la cancellazione**.

7. Trasferimenti, retention e rapporti con i fornitori: il rischio "invisibile"

Una parte particolarmente rilevante dell'argomento in oggetto riguarda ciò che spesso l'impresa non vede: i rapporti con il fornitore del servizio AI.

E' necessario verificare e conservare evidenza del piano effettivamente acquistato, dei termini applicabili, del DPA, dei sub-responsabili, delle retention, delle opzioni di cancellazione e degli eventuali trasferimenti internazionali.

L'alert imprenditoriale è decisivo: **non basta comprare il servizio; bisogna capire contrattualmente e tecnicamente dove vanno i dati, per quanto tempo restano, chi può accedervi e a quali condizioni**.

Sotto questo profilo, l'uso dell'AI richiede una verifica integrata tra funzioni legali, privacy, IT e security, non una scelta rimessa solo all'utente finale.

8. Formazione del personale: il presidio senza il quale la policy resta solo carta

La formazione non è un elemento accessorio ma una misura essenziale.

Essa deve riguardare almeno:

- dati che non possono essere inseriti;
- minimizzazione;
- rischio di output inesatti;

- proprietà intellettuale e riservatezza;
- gestione dei segreti;
- incident reporting;
- trasparenza e diritti degli interessati.

Per l'imprenditore l'alert è intuitivo: **la maggior parte dei rischi nasce dal comportamento operativo quotidiano**. Anche la migliore policy fallisce se chi usa gli strumenti non sa distinguere tra dato ammesso e dato vietato, tra sintesi lecita e upload improprio, tra uso interno e trasferimento esterno di informazioni sensibili.

9. Gli alert essenziali per l'imprenditore

a) Governare prima di adottare

L'AI non deve essere introdotta senza policy, ruoli, regole e verifiche.

b) Minimizzare prima di caricare

Non tutto ciò che è disponibile in azienda può essere inviato a uno strumento di AI.

c) Proteggere segreti e credenziali

Password, token, chiavi, segreti applicativi e contenuti riservati devono restare fuori dal perimetro non autorizzato.

d) Verificare NDA e proprietà intellettuale

Documenti e materiali di clienti, partner o terzi non possono essere trattati senza previa verifica dei vincoli applicabili.

e) Mantenere il controllo umano

L'output dell'AI va sempre verificato prima dell'uso effettivo.

f) Allineare basi giuridiche, informative e diritti

L'uso dell'AI può imporre aggiornamenti documentali e procedurali.

g) Formare il personale e presidiare gli incidenti

La compliance si gioca soprattutto sul piano operativo quotidiano.

10. Le aree di intervemto del professionista

Nel contesto così delineato si inserisce la figura del consulente che deve affiancare l'imprenditore nelle seguenti attività.

- Mappatura: individuazione degli strumenti AI già utilizzati e dei relativi casi d'uso.
- Classificazione: valutazione dei dati, dei vincoli contrattuali e dei rischi associati.
- Regolamentazione: predisposizione di policy interne e procedure autorizzative.
- Controllo: individuazione delle verifiche umane e tecniche necessarie.
- Monitoraggio: aggiornamento periodico delle misure, gestione degli incidenti e formazione.

11. Conclusione

L'intelligenza artificiale in azienda non è un'area franca, né un semplice tema di innovazione tecnica.

È un ambito in cui si intrecciano protezione dei dati, riservatezza, sicurezza delle informazioni, vincoli contrattuali, proprietà intellettuale e responsabilità organizzativa.

Per l'imprenditore, il rischio maggiore non è adottare strumenti di AI, ma adottarli senza presidi adeguati.

In assenza di una disciplina interna chiara, di una selezione consapevole dei dati caricabili, di controlli tecnici, di verifica umana e di formazione del personale, l'efficienza promessa dall'AI può trasformarsi rapidamente in esposizione giuridica e organizzativa.

L'uso dell'AI, dunque, richiede una scelta di metodo: non improvvisazione, ma governance.

Avv. Luca Maione

Founding partner TMDPLEX

Dipartimento Civile Societario