AI E DIGITALIZZAZIONE

Misure concrete per il Governo della cybersecurity e dell'Intelligenza Artificiale in azienda

di **Giuseppe Vitrani, Avvocato**

Il presente articolo si pone l'obiettivo di proseguire nell'analisi dei nuovi obblighi che il recepimento della direttiva NIS 2 impone alle aziende; esso si pone come naturale prosecuzione di quanto sviluppato su questa rivista nell'ultimo articolo a firma del sottoscritto, risalente al 18 novembre '25. Invero, data l'importanza della normativa sopravvenuta, appare utile fornire un contributo anche ai professionisti che si trovino ad assistere i propri clienti anche in questi nuovi ambiti della *compliance* digitale aziendale.

È importante innanzitutto considerare che l'Agenzia per la Cybersicurezza Nazionale (ACN) ha assunto un ruolo centrale nell'architettura normativa delineata dal D.Lgs. 138/2024, completando il quadro regolatorio con determinazioni e FAQ che specificano in modo puntuale le condotte dei soggetti coinvolti, le misure da adottare, le tempistiche e le responsabilità. Come evidenziato anche dalla Circolare Assonime n. 23/2025, pubblicata nel novembre 2025, le determinazioni dell'ACN non si limitano a fornire chiarimenti interpretativi, ma definiscono un vero e proprio modello operativo cui le imprese devono conformarsi per costruire il proprio sistema di gestione della sicurezza informatica.

1. Il set minimo di misure da presidiare

Le determinazioni dell'ACN definiscono un set minimo di misure che il Consiglio di amministrazione deve presidiare, approvare e riesaminare periodicamente. Sulla base delle indicazioni fornite dalla normativa e dall'Agenzia, è dunque fondamentale che il CdA si faccia pienamente carico della politica di gestione del rischio cyber, che deve essere coerente con la strategia aziendale complessiva. È inoltre importante adottare un piano di gestione dei rischi connessi alla sicurezza informatica e il documento di valutazione, che rappresentano gli strumenti fondamentali per l'identificazione, l'analisi e la valutazione delle minacce informatiche cui l'organizzazione è esposta.

È inoltre importante che venga adottato il piano di trattamento dei rischi e il piano di valutazione dell'efficacia delle misure adottate. Particolare rilevanza assumono poi i piani di

continuità operativa e di disaster recovery, essenziali per garantire la resilienza dell'organizzazione in caso di incidenti. Il piano di gestione degli incidenti e di notifica al CSIRT completa il quadro dei documenti strategici, unitamente al piano di formazione destinato a tutti i livelli aziendali. L

Questo ampio corredo documentale rende evidente come la cybersicurezza debba entrare a pieno titolo nei piani strategici e industriali, nella valutazione periodica dell'adeguatezza del sistema di controllo interno nonché, come detto nel precedente articolo, degli adeguati assetti organizzativi ai sensi dell'articolo 2086 del Codice civile.

2. La figura del responsabile per la cybersicurezza

La complessità degli adempimenti richiesti dalla normativa NIS 2 rende inoltre fondamentale la nomina di un responsabile per la cybersicurezza che supporti il CdA nella pianificazione e nel monitoraggio delle misure di sicurezza. Tale figura, ormai nota come CISO (*Chief Information Security Officier*) appare fondamentale anche nell'ottica della accountability aziendale, potendo costituire il punto di raccordo tra le competenze tecniche specialistiche e le responsabilità di governance.

Come sottolineato dall'ACN nelle linee guida per i dirigenti delle PMI, il responsabile per la cybersicurezza deve disporre delle risorse e delle competenze necessarie per sviluppare un piano di sicurezza efficace. È essenziale che tale figura sia supportata con gli strumenti necessari per mantenere elevati i livelli di sicurezza e che siano pianificati allineamenti periodici per monitorare i progressi e risolvere eventuali ostacoli.

3. La sicurezza della supply chain

Un altro aspetto rilevante concerne la sicurezza della catena di fornitura (*supply chain*), che invero costituisce uno degli aspetti più delicati e spesso sottovalutati nella gestione del rischio cyber. La Direttiva NIS 2 e il decreto di recepimento attribuiscono a tale profilo un'importanza centrale, riconoscendo che le vulnerabilità dei fornitori possono propagarsi all'intera organizzazione con effetti potenzialmente devastanti.

Il CdA è dunque chiamato a orientare i processi di acquisto e outsourcing affinché incorporino requisiti di sicurezza coerenti con le misure interne. Tale compito implica la necessità di assicurare la valutazione del rischio cyber delle forniture e l'inserimento di clausole di sicurezza nei contratti con impatto sui sistemi informativi e di rete. Le aziende devono pertanto verificare che i propri fornitori rispettino elevati standard di sicurezza, tra cui procedure di gestione degli incidenti e regolare attività di vulnerability assessment e penetration test sui propri servizi.

A tal proposito è opportuno sottolineare come il Global Digital Trust Insights 2026 di PwC, condotto su circa 3.900 dirigenti di imprese di 72 Paesi, abbia evidenziato che le fragili difese della supply chain costituiscono una delle vulnerabilità più significative nel panorama attuale.

Questo dato conferma l'urgenza di un cambio di approccio non solo tecnologico ma anche culturale nella gestione dei rapporti con i fornitori esterni che gestiscono dati o servizi critici.

4. I rischi derivanti dall'uso dell'Intelligenza Artificiale in azienda

L'adozione pervasiva di sistemi di intelligenza artificiale nell'ambiente aziendale introduce una nuova dimensione del rischio cyber che il Consiglio di amministrazione è chiamato a presidiare. Secondo il report citato di PwC, il 69% delle aziende italiane prevede di aumentare il budget per la sicurezza informatica nei prossimi dodici mesi, e una su tre investirà prioritariamente nell'AI, ritenuta strategica rispetto alla cloud security e alle tecnologie tradizionali di data protection.

Tuttavia, i dati mostrano un preoccupante divario tra la volontà di investimento e la consapevolezza dei rischi: solo il 6% delle organizzazioni a livello globale dichiara di sentirsi pienamente preparata a contrastare le minacce informatiche, mentre il 69% cita le fughe di dati alimentate dall'AI come principale preoccupazione di sicurezza. Paradossalmente, quasi il 47% delle aziende non ha ancora implementato controlli di sicurezza specifici per l'intelligenza artificiale.

Gli strumenti di intelligenza artificiale, in particolar modo di quella generativa, sono dunque ormai di uso corrente in azienda ed è pertanto necessario di che si sviluppi una piena consapevolezza circa i benefici e i rischi di cui essi sono portatori. In particolare, occorre considerare che il principale rischio di sicurezza deriva dalle informazioni che i dipendenti inseriscono in questi sistemi, spesso senza considerare le implicazioni sulla privacy mentre cercano soluzioni rapide ai problemi aziendali. Dati sensibili, informazioni strategiche, codice proprietario e altri asset critici possono essere involontariamente condivisi con piattaforme esterne, esponendo l'organizzazione a rischi di data breach e violazioni della normativa sulla protezione dei dati personali.

Inoltre, l'intelligenza artificiale rappresenta un potente strumento anche nelle mani degli attori malevoli. Il phishing basato su AI costituisce l'evoluzione di una minaccia tradizionale, resa più sofisticata dalla capacità dei sistemi intelligenti di personalizzare i messaggi fraudolenti in modo estremamente convincente.

5. Il quadro normativo: l'AI Act e le sue implicazioni

Il Regolamento UE 2024/1689, noto come AI Act, è entrato in vigore il 1° agosto 2024 e prevede un'applicazione graduale delle sue disposizioni. Dal 2 febbraio 2025 sono operative le norme sulle pratiche di AI vietate e gli obblighi di alfabetizzazione in materia. Dal 2 agosto 2025 si applicano le norme che disciplinano i modelli di AI per finalità generali, la governance, la riservatezza e le sanzioni. L'applicazione completa del Regolamento è prevista per il 2 agosto 2026, con un periodo di transizione prorogato fino al 2027 per i sistemi ad alto rischio.

L'AI Act adotta un approccio basato sul rischio, classificando i sistemi di intelligenza artificiale

in quattro categorie: sistemi a rischio inaccettabile (vietati), sistemi ad alto rischio (soggetti a requisiti stringenti), sistemi a rischio limitato (con obblighi di trasparenza) e sistemi a rischio minimo (con adempimenti minimi). Le aziende che utilizzano sistemi AI in ambiti quali la selezione del personale, la valutazione dei dipendenti, la gestione di infrastrutture critiche o l'accesso ai servizi essenziali sono soggette agli obblighi più rigorosi.

Per le organizzazioni non conformi, il regime sanzionatorio prevede multe fino a 35 milioni di euro o al 7% del fatturato globale annuo, analogamente a quanto previsto dal GDPR. Tale cornice normativa si aggiunge agli obblighi derivanti dalla NIS 2, creando un ecosistema regolatorio complesso che richiede una governance integrata della sicurezza informatica e dell'intelligenza artificiale.

6. Le misure organizzative: verso una governance integrata

L'integrazione della gestione dei rischi AI nel più ampio sistema di governance della cybersecurity richiede l'adozione di misure organizzative specifiche, costituendo dunque un ulteriore profilo di compliance tecnologica rilevante ai sensi dell'aer. 2086 c.c. Le aziende dovrebbero procedere innanzitutto alla mappatura dei sistemi AI utilizzati, classificandone il livello di rischio secondo i criteri dell'AI Act. È essenziale redigere la documentazione tecnica richiesta, implementare controlli di qualità e garantire la spiegabilità delle decisioni automatizzate eventualmente gestite, attivando misure di cybersecurity adeguate.

Sul piano organizzativo, può risultare opportuna la designazione di un responsabile AI, analogamente al Data Protection Officer previsto dal GDPR. Tale figura dovrebbe sedere in CdA (non a caso in alcune esperienze già avviate, all'interno del board di amministrazione è stata istituita la figura del CAIO – *Chief Artificial Intelligenze Officier*) e dovrebbe possedere competenze in materia di impatti legali, principi etici e gestione del rischio tecnologico, assicurando il coordinamento tra le diverse funzioni aziendali coinvolte. La formazione dei dipendenti e dei dirigenti sui limiti e sul corretto uso dell'AI rappresenta inoltre un elemento imprescindibile: in assenza di adeguata consapevolezza, aumentano sia gli errori procedurali sia le resistenze culturali all'adozione sicura delle nuove tecnologie.