UNIONE INDUSTRIALI
Torino

Laura Marengo

Area servizi legali, compliance e segreteria generale
Unione Industriali Torino

AI e Cybersicurezza:

come si stanno organizzando le imprese

26/05/2026

Osservatorio Unione Industriali Torino

Più di 2.200 aziende associate

20 gruppi merceologici

Filiere:

DIGITAL INNOVATION
ENERGY AND SUSTAINABLE MOBILITY
ITALIAN LIFESTYLE
LIFE SCIENCES

PMI: circa 85% DELLE AZIENDE ASSOCIATE

TAVOLO PRIVACY E NUOVE TECNOLOGIE

Cybersicurezza

- Un primo tema che emerge è il cambio di paradigma: la cybersicurezza non riguarda più soltanto i reparti IT, ma coinvolge **la governance aziendale, i vertici e i manager → Team aziendali multidisciplinari**

- La sicurezza informatica sta diventando anche **un fattore di fiducia nelle relazioni di mercato**: clienti e partner richiedono sempre più garanzie. Possiamo quindi considerarla non solo come un obbligo, ma come **un elemento di qualificazione dell'impresa**

- la NIS2 non riguarda solo la conformità normativa, ma **la resilienza e la capacità delle imprese di operare in un'economia sempre più digitale e interconnessa ai principali temi che le imprese devono affrontare:** governance; risk management; sicurezza della filiera, formazione e competenze.

- Un aspetto molto interessante è quello della **sicurezza della supply chain**. Sappiamo che spesso gli attacchi entrano nelle filiere attraverso fornitori più piccoli o meno strutturati. **Quanto cambieranno le relazioni tra imprese proprio su questo terreno?** A livello di selezione fornitori, audit, clausole contrattuali, … (richieste da parte dei soggetti essenziali e importanti NIS2)

La cybersicurezza non è più solo un tema tecnico, ma un elemento strutturale della competitività delle imprese

CdA e Organi direttivi: ruolo centrale nella compliance della NIS2

- Approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica
- Sovrintendere all'adozione degli obblighi di implementazione delle misure di gestione dei rischi, di notifica, di registrazione sulla piattaforma messa a disposizione dall'Agenzia per la Cybersicurezza Nazionale
- Seguire una formazione in materia di cybersecurity
- Promuovere l'offerta periodica di formazione per favorire l'acquisizione di conoscenze e competenze sufficienti ai propri dipendenti e collaboratori
- Flussi informativi: necessità di istituire canali di comunicazione sugli incidenti e sulle notifiche
- **Responsabili per le violazioni della normativa: destinatari della sanzioni**
- **Deleghe?**

ALCUNE MISURE ORGANIZZATIVE NIS2

- **Governance interna all’azienda ed esterna della filiera**
- **Policy aziendali e formazione a tutti i livelli**
- **Organigramma aziendale**
- **Analisi dei rischi**
- **Gestione degli incidenti**
- **Dimostrabilità della sicurezza della catena di approvvigionamento (supply chain)**
- **Sicurezza nell’acquisizione, sviluppo e manutenzione dei sistemi informatici e di rete**
- **Strategie e procedure per valutare l’efficacia delle misure di gestione dei rischi cyber**
- ….

Utilizzo di sistemi di Intelligenza Artificiale

- Con l'entrata in vigore dell'AI Act, le aziende non possono più permettersi un approccio reattivo alla regolamentazione dell'intelligenza artificiale. Serve una **strategia di compliance proattiva**, che integri aspetti legali, organizzativi e tecnologici.

- Per **DPO**, **AI-Officer** e **Compliance Manager** sarà fondamentale la capacità di dimostrare:
  ✓ formazione adeguata
  ✓ consapevolezza dei rischi AI
  ✓ human oversight effettivo
  ✓ governance documentata

  diventerà probabilmente uno degli elementi centrali nelle verifiche di accountability

Governare l’IA nelle imprese

1. **Mappatura dei sistemi che potrebbero qualificarsi come sistemi di IA** (la mappatura e l’analisi dei rischi costituiscono la base per definire controlli, procedure e strumenti di monitoraggio efficaci);

2. **Verifica dei contratti con i fornitori** (la gestione dei fornitori diventa un tema di governance del rischio);

3. **Analisi della conformità con il GDPR e con il Sistema Privacy aziendale** (i sistemi di IA devono essere progettati e utilizzati nel rispetto dei principi di liceità, minimizzazione e trasparenza);

4. **Analisi di conformità con altre disposizioni quali diritto di autore e proprietà intellettuale;**

5. **Protezione delle informazioni confidenziali e dei segreti commerciali (tutela del know how);**

6. **Attenzione all’uso non autorizzato** di applicazioni di IA da parte dei dipendenti sui device aziendali e peggio ancora personali

7. **Adozione di Linee guida e policy per regolare l’utilizzo dell’IA all’interno dell’azienda**;

8. **Formazione del personale sui rischi e sulle aspettative dell’IA;**

9. **Trasparenza sull’utilizzo dei sistemi di IA (informative/policy);**

10. **Valutazione dei possibili impatti organizzativi**

11. **Cybersicurezza**

IA e compliance opportunità e rischi

L'utilizzo dell'intelligenza artificiale nelle imprese può essere utile anche per il rafforzamento degli **assetti organizzativi ma può** rappresentare un **rischio** che la società deve adeguatamente identificare e gestire per evitare addebiti in termini di "**colpa di organizzazione**".

L'IA consente di eseguire monitoraggi **automatizzati**, **veloci** e con un **minor dispendio** di energie "umane".

- Nella fase di *risk assesment*, la capacità **predittiva** dell'IA permette di identificare potenziali rischi e problemi prima che essi si verifichino.
- Nella fase di *risk management*, l'analisi di **grandi quantità di dati** da parte dell'IA permette di rilevare comportamenti anomali e di adottare azioni risolutive.
- Nel complesso l'IA garantisce **processi decisionali più informati** e strumenti utili per gli attori del cd. "**sistema di controllo interno**" della società.

MA

Attenzione a **governare** adeguatamente l'utilizzo dell'IA al fine di non violare norme del nostro ordinamento

Verso la compliance integrata

- Il *trend* delle norme che maggiormente impattano su questi aspetti è significativo, si tratta di un *trend* incentrato proprio sul principio della **prevenzione mediante organizzazione**.

- Anche i **Modelli 231** dovranno tenere conto dell'utilizzo dell'**IA** per lo svolgimento delle attività di business prevedendo in tal senso presidi volti a mitigare i relativi rischi. L'assenza di presidi relativi ai sistemi di IA e alla cybersicurezza può configurare **colpa nell'organizzazione.**

- **Rischio Cyber**: la crescente digitalizzazione dei processi aziendali e l'evoluzione della disciplina dei reati informatici impongono di integrare il rischio cyber nella **governance dell'impresa** e, pertanto, nei **Modelli Organizzativi 231**.

- La ***compliance* aziendale** richiede un ruolo centrale dell'imprenditore, che deve affrontare un'attività multidisciplinare, nella quale hanno un ruolo fondamentale i suoi manager che insieme ai professionisti devono costruire sistemi organizzativi e di *governance* idonei e soprattutto adeguati a ogni singola realtà. Fondamentale è l'integrazione fra le diverse funzioni aziendali: **cybersecurity, protezione dei dati, risk manager, area legale/compliance e, ove presente, odv.**

- **L'IA, la Cybersicurezza, la protezione dei dati,** richiedono un approccio integrato, capace di connettere **tecnologia**, **diritto** e **organizzazione** al fine di trasformare obblighi normativi in vantaggi competitivi.

- Questi concetti sono già ben noti da tempo alle grandi imprese ma le aziende minori hanno ancora bisogno di tempo e di aiuto, molte di esse non sono dotate di procedure idonee ad assicurare l'efficienza e la trasparenza dei processi operativi e la gestione dei principali rischi aziendali

DIGITAL OMNIBUS

- Accordo provvisorio in sede di trilogo tra Parlamento europeo, Consiglio UE e Commissione europea su IA; Cybersecurity; Protezione dei Dati Personali, Data Act …: valutazione positiva di Confindustria ma restano criticità su AI ACT, Data Act, Cybersecurity e Protezione dei Dati → servono regole più chiare e maggior coordinamento (Position Paper)

- **Rinvio a dicembre 2027** per la conformità dei sistemi ad **alto rischio** (Identificazione biometrica, Infrastrutture critiche, Istruzione e Formazione, Risorse Umane, Servizi essenziali, Forze dell'Ordine e Giustizia)

- **Consiglio**: utilizzare il tempo supplementare concesso da Bruxelles per integrare i diritti fino dalla progettazione, approccio **BY DESIGN** al fine di rendere l'attuazione delle regole più sostenibile e sfruttare al meglio le opportunità che si presentano

UNIONE INDUSTRIALI
Torino

Grazie,
Laura Marengo

Area Legale, Compliance e Segreteria Generale

Unione Industriali Torino