

# Sicurezza convergente e GDPR: quali effetti sulle organizzazioni pubbliche e private?

a colloquio con Luisa Franchina, Presidente AIIC  
a cura di Raffaello Juvara

## Quali sono gli effetti per la sicurezza delle IC determinati dalla convergenza tra sicurezza fisica e quella logica?

Il concetto di *cyber-physical system* può essere considerato uno degli elementi chiave del processo di digitalizzazione del settore industriale – e in particolare del manifatturiero – nell’ambito della cosiddetta Industria 4.0.

Protagoniste di questa quarta rivoluzione industriale sono infatti tutte quelle tecnologie abilitanti in grado di creare dei sistemi “intelligenti”, interconnessi e intercomunicanti, in grado non solo di acquisire ed elaborare enormi quantità di dati, ma anche di sfruttare questa capacità computazionale e di comunicazione reciproca per migliorare i processi, non soltanto produttivi, ma anche decisionali.

Questa convergenza pone altresì una serie di questioni relative alla sicurezza che non vanno assolutamente sottovalutate: pensiamo ai sistemi ICS (Industrial Control Systems), altrimenti detti SCADA (Supervisory Control And Data Acquisition), che vengono impiegati anche per la gestione dei processi che garantiscono il funzionamento delle infrastrutture critiche, la cui continuità operativa risulta essenziale per il mantenimento del benessere della popolazione.

I dati statistici e i report redatti dalle maggiori compagnie di sicurezza informatica e dalle principali agenzie nazionali e sovranazionali (come il CLUSIT e l’ENISA) ci mostrano un trend molto chiaro: gli attacchi informatici sofisticati in grado di determinare un impatto materiale, sfruttando la convergenza tra il dominio cyber e quello fisico, sono sempre più diffusi e rappresentano ormai una realtà.



## Le organizzazioni sono pronte ai cambiamenti?

In Italia notiamo diversi segnali positivi: la Legge di Bilancio 2018 ha dato un notevole input al piano Industria 4.0, presentato nel biennio precedente, incoraggiando il rilancio degli investimenti da parte delle imprese, la costruzione di competenze, la governance.

La principale sfida della “trasformazione digitale” delle organizzazioni è legata a una questione culturale, di mentalità. Il principale ostacolo al processo di digitalizzazione delle imprese, ma anche del settore pubblico, è costituito dalla difficoltà di sganciarsi da una visione che, da un lato, considera la spesa in nuove tecnologie come una dispersione di risorse anziché un investimento; dall’altro, considera il mondo del “cyber” come qualcosa di poco gestibile se non addirittura pericoloso.



Tuttavia, per essere competitivi sullo scenario internazionale, oggi, investire sulle tecnologie digitali e sulle soluzioni di sicurezza atte a tutelare i propri asset materiali e immateriali è diventato un imperativo. Parlando di sicurezza, è necessario in primis ripensare la visione dell'intero ecosistema difensivo, privilegiando un approccio più «agile» e trasversale, in grado di operare su più domini.

### **E le competenze delle persone preposte sono all'altezza della situazione?**

Uno dei pilastri del piano Industria 4.0 è proprio la creazione di competenze, attraverso iniziative atte a finanziare centri di eccellenza e la creazione di competence center, in cui è previsto un forte coinvolgimento sia di istituzioni universitarie che di realtà private, con il supporto di altri centri di competenza a livello europeo. Tutte queste realtà sono accomunate da un focus su ambiti tecnologici specifici e da una vision in ottica Industria 4.0.

È importante, in futuro, puntare sempre di più su un'attività formativa adeguata alle nuove competenze richieste dal mercato del digitale: Internet of Things, cybersecurity, data science e Intelligenza artificiale saranno i settori con cui le imprese dovranno necessariamente interfacciarsi nei prossimi anni e in cui i nuovi professionisti del digitale dovranno sviluppare le proprie competenze.

### **Come valuta la risposta delle Pubbliche Amministrazioni?**

Secondo la fotografia scattata dall'Osservatorio Agenda Digitale del POLIMI, in collaborazione con l'AgId, negli

ultimi quattro anni lo slancio dell'Italia per allinearsi all'Europa nella "corsa al digitale" è stato notevole, ed è necessario continuare su questa linea evitando battute d'arresto o ulteriori ritardi per non vanificare gli sforzi fatti sino ad ora.

Sempre secondo l'Osservatorio, dal 2013 al 2015 la spesa in tecnologie digitali da parte della PA italiana ammontava a circa 5,6 miliardi di euro l'anno. Con la diminuzione della spesa pubblica in digitale (come previsto dalla Finanziaria del 2016), entro la fine del 2018 sarà possibile liberare risorse per gli investimenti relativi al Piano Triennale per l'Informatica nella Pubblica amministrazione, grazie all'adesione delle PA a sistemi come PagoPA, il sistema nazionale per i pagamenti a favore della Pubblica Amministrazione, o il Sistema pubblico di identità digitale (SPID), portando a un'ottimizzazione e a un significativo risparmio dei costi di acquisto e della gestione delle soluzioni digitali adottate all'interno delle PA.

### **GDPR, solo adempimenti o anche opportunità per le organizzazioni?**

ndubbiamente la nuova normativa in materia di privacy richiede alle aziende alcuni sforzi di adeguamento, in particolare per le piccole e medie imprese e soprattutto dal punto di vista delle misure di sicurezza richieste per la protezione dei dati personali. Tuttavia, si tratta di investimenti che possono rappresentare un'opportunità di sviluppo per le piccole realtà italiane che sono ancora restie all'adozione di tecnologie digitali.

