PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5873 di Giovedì 19 giugno 2025

Forse è il caso di cambiare approccio alla salute e sicurezza sul lavoro?

Chissà se e quando si capirà nel nostro Paese che le strategie, messe in atto dal nostro sistema regolatorio, si sono dimostrate palesemente fallimentari e il miglioramento avvenuto è dovuto alla sola evoluzione tecnologica.

I tempi stanno cambiando. Nei prossimi 10-15 anni, i megatrend che influenzano in modo significativo la società, l'economia e le dinamiche globali e cioè le tendenze complesse in grado di produrre cambiamenti significativi sul lungo termine, influenzeranno anche la salute e la sicurezza sul lavoro (SSL) costringendoci a riesaminare il nostro approccio.

Quindi, dovremmo cominciare a domandarci:

- quale impatto potranno avere queste tendenze sia sulle organizzazioni che su chi si occupa professionalmente di SSL;
- quali nuovi metodi di produzione, nuove organizzazioni e nuovi profili professionali saranno necessari;
- come, tutto ciò, visti i cambiamenti tecnologici previsti, impatterà su una nuova generazione di lavoratori e sulle aspettative della società civile;
- come le imprese dovranno adattare la propria visione e le proprie attività in materia di SSL per far fronte ai citati cambiamenti.

Prima di tutto, dobbiamo aver ben chiaro che i cambiamenti con il relativo carico di incertezza, complessità e instabilità avranno un impatto sulla SSL.

Ad esempio la diffusione della AI e IoT, con l'aumento delle capacità di raccolta dati e di calcolo, porteranno ad accrescere l'affidabilità dei processi e una maggiore sicurezza nell'ambito dei processi sistemici conosciuti.

I sistemi acquisiranno la possibilità di una maggiore interconnessione con conseguente aumento della complessità vista anche la coesistenza di tecnologie vecchie e nuove.

Il tutto senza dimenticare anche un altro aspetto e cioè l'aumento della vulnerabilità di questi sistemi.

Altro aspetto da mettere ben in chiaro è che gli individui, con il loro bagaglio di competenze, con i loro atteggiamenti, con le loro motivazioni e con i loro valori e principi contribuiranno sempre alla SSL a prescindere dalla diffusione di AI, IoT, ecc..

Questo perché sarà sempre l'individuo a mantenere il controllo, a prendere le decisioni, ad adattarsi a situazioni non prevedibili che si manifesteranno e a governare il conseguente cambiamento.

Non va dimenticato che, visti i cambiamenti che ci aspettano, le competenze, comprese quelle in materia di SSL, diverranno sempre più importanti.

Oggi, è indubbio che nel nostro Paese, oltra alla bassa natalità degli ultimi decenni, non c'è solo il problema della numerosità della forza lavoro ma anche e soprattutto quello della qualità della stessa.

Per quanto riguarda la SSL il modello formativo attuale deve essere completamente rivisto data anche la certa difficoltà a formare gran parte della forza lavoro alle nuove tecnologie. In Italia, le cronache, periodicamente, ci portano all'attenzione eventi infortunistici dove le vittime sono prevalentemente soggetti appartenenti a fasce d'età che hanno davanti almeno un paio di decenni di attività. Ciò significa che la forza lavoro oggi presente nelle aziende dovrà "*confrontarsi*" con le nuove tecnologie e con le conseguenti ovvie difficoltà.

Questo senza dimenticare che, visto che in Italia, più del 95% delle imprese operanti ha meno di 10 dipendenti, non ci saranno al loro interno soggetti dotati di competenze informatiche adeguate per far fronte ai cambiamenti tecnologici che stanno avvenendo.

In altri contributi il sottoscritto ha ampiamente discusso della " *Cultura della Sicurezza*" come parte della "*Cultura Organizzativa*" di una impresa.

I cambiamenti che stanno avvenendo, con una forza lavoro che invecchia, con almeno due generazioni di lavoratori che operano insieme in una organizzazione e con la tendenza a frammentare ed esternalizzare le attività, non potranno che inibire qualunque processo di sviluppo di una " *Cultura Organizzativa*" e quindi della "*Cultura della Sicurezza*" e, ove queste già presenti, un loro certo indebolimento.

Sempre questi cambiamenti spingeranno ulteriormente per una delocalizzazione delle attività ed alla globalizzazione della "*Value Chain*" favorendo sempre più una "*finanziarizzazione*" delle attività produttive.

Il tutto con il più che certo aumento del divario culturale tra i Paesi occidentali e quelli dove le attività verranno delocalizzate (nei Paesi africani politicamente stabili, il processo è già iniziato da qualche anno) e il conseguente indebolimento del modello europeo di gestione della SSL.

Questi cambiamenti produrranno anche l'accesso di altri soggetti nella gestione delle organizzazioni e questi portatori d'interessi, specialmente se provenienti da contesti in cui la SSL non era certo in cima alle priorità sociali, molto probabilmente manterranno il proprio approccio con la conseguenza che la SSL sarà considerata un insieme di norme e procedure che non produce valore alcuno ma, anzi, va a creare ostacoli al raggiungimento degli obiettivi prioritari dell'azionariato.

Il risultato sarà quello che vedrà, nel nostro Paese, crescere le aspettative della società civile che vorrà, visti i comportamenti organizzativi dei nuovi soggetti, essere coinvolta nei processi decisionali specialmente quando si tratterà di attività produttive che impattano fortemente sul territorio.

Quindi, le organizzazioni che si troveranno in queste condizioni, sappiano che verranno messe sotto la lente d'ingrandimento e le conseguenze, in caso di eventi (infortuni, ecc.), saranno decisamente maggiori sia come costi diretti che, soprattutto, indiretti.

Come noto, in Italia, il modello di "*governance*" della SSL è essenzialmente basato su un sistema normativo, regolamentare e di controllo.

Visti i cambiamenti in arrivo, questo modello dovrà essere profondamente rivisto.

In particolare, andranno rafforzate le competenze dei soggetti chiamati a "*dettare le regol*e" per le attività lavorative perché, altrimenti, il rischio concreto è che le regole vengano definite "*a tavolino*" e, quindi, ben poco aderenti alla realtà concreta degli ambienti di lavoro.

Non fare ciò potrebbe comportare una delega di fatto al settore privato (ovviamente non neutrale), per la definizione delle citate regole.

Ecco perché, è fondamentale l'acquisizione, per i soggetti incaricati di scrivere le regole, di competenze relative ai processi lavorativi in modo da potersi confrontare, sullo stesso piano, con gli operatori privati.

Analogo discorso va fatto con il personale addetto al controllo operante negli enti di vigilanza.

Non si può assumere personale privo di qualunque esperienza operativa maturata nel mondo del lavoro, fargli una settimana di corso in modalità FAD e spedirlo, con una check list in mano, a fare controlli nelle aziende.

In altri Paesi UE, l'accesso a tali posizioni, avviene previa verifica di una precedente esperienza pluriennale in ambito SSL nel mondo del lavoro all'interno delle aziende. Naturalmente, per attirare soggetti più qualificati da adibire ad attività di vigilanza, andrebbero riviste profondamente le retribuzioni che oggi sono tra le più basse dei Paesi UE.

Fino ad oggi, l'approccio prevalente è stato quello basato sul rispetto delle regole pensate in ottica preventiva, sulla conseguente riduzione delle incertezze e sui controlli.

Quindi, oggi tutto, è basato sulla "*sicurezza come dimostrata*".

I cambiamenti che stanno avvenendo potrebbero, invece, indirizzarci verso un approccio diverso che metta al centro la "*sicurezza come praticata*" e cioè un nuovo modello di riferimento per la governance della SSL

Fatte queste premesse, appare palese la necessità di adottare ben altro approccio rispetto quello seguito negli ultimi decenni.

In questi anni, la tecnologia e cioè l'insieme delle conoscenze scientifiche che si traducono in applicazioni socialmente rilevanti, ha costantemente migliorato il livello di sicurezza, anche se, i soliti profeti dell'integralismo repressivo ci presentano una situazione disastrosa al solo fine di mantenere visibilità tra gli addetti ai lavori. Per averne prova basta dare un'occhiata ai dati pubblicati dall'INAIL degli ultimi 30 anni.

Nulla ci fa pensare che tale trend non proseguirà.

Non va però trascurato che la complessità, che viaggia con l'evoluzione tecnologica ad una notevole velocità, potrebbe rendere il sistema più fragile con eventi le cui cause prime sono nascoste nelle pieghe della complessità stessa.

Questi rischi residui, nonostante il miglioramento complessivo del livello di sicurezza, potrebbero non essere accettati dalla

società civile in quanto le aspettative della stessa potrebbero essere in fase evolutiva.

Pertanto, la futura concezione della SSL necessiterà di ben altro approccio rispetto quello seguito fino ad oggi nel nostro Paese.

Dovrà essere un approccio interdisciplinare ampliando, così, il modo con cui la SSL viene oggi considerata, mettendola sullo stesso piano e in combinazione con tutte le altre sfide strategiche che i cambiamenti origineranno.

Quindi, è necessario un nuovo approccio più ampio e integrativo che produca delle conseguenze sia sulla governance della SSL che sulla sua concreta applicazione nei processi aziendali.

In sintesi, si dovrà:

- promuovere una visione complessiva della SSL nelle aziende che vada oltre l'approccio livello per livello;
- considerare la SSL in combinazione con le altre sfide strategiche dell'azienda;
- considerare l'organizzazione in un contesto in continua evoluzione e non chiusa in una sfera di cristallo impermeabile a ciò che succede all'esterno.

Come già detto, l'evoluzione tecnologica porta con sé nuove vulnerabilità sistemiche derivanti anche dall'ibridazione delle tecnologie, dall'interconnessione e dai network dilaganti, dato che queste sono altre fonti di complessità ed incertezza.

La necessità di gestire la SSL in modo diverso probabilmente richiederà l'adozione di un approccio olistico, sia a livello di gestione che di governance con il conseguente abbandono di un sistema regolatorio organizzato a compartimenti stagni e la conseguente e necessaria modifica delle strutture e dei meccanismi di controllo.

L'attuale modello di gestione della SSL, è basato sulla presunta affidabilità dei vari componenti del sistema e sulle varie tipologie di governance adottate in funzione dei vari fattori di rischio.

Questo modello è palesemente inadeguato per fare fronte all'imprevedibilità della complessità e, pertanto, è necessario sviluppare un modello in cui le strategie puntino sempre sull'affidabilità non più per singolo componente ma per il sistema nel suo complesso.

Se da una parte è vero che ci si è concentrati di più sulla "*sicurezza dimostrata*" e cioè su ciò che era visibile e che implicava una serie di decisioni e azioni necessarie per assicurare la SSL, dall'altra gli addetti ai lavori, anche con un minimo di esperienza, sanno bene che la SSL viene garantita anche attraverso la pratica reale e cioè da una serie di regole applicabili alla specificità e la cui combinazione, a fronte di incertezze e instabilità, permette di far fronte alla situazione che si ha di fronte facendo divenire così, la "*sicurezza praticata*" di fondamentale importanza.

Pertanto, in futuro, la "*sicurezza praticata*", in genere poco visibile e dimostrabile, diverrà sempre più integrata, sia concettualmente che concretamente, nell'organizzazione.

Tutto ciò non vuol dire che le strategie utilizzate fino ad oggi debbano essere abbandonate in quanto il modello attuale ci ha permesso di raggiungere un più che accettabile livello di sicurezza.

Vuol solo dire che, visti i cambiamenti all'orizzonte, l'approccio deve essere modificato per tenere conto esplicitamente degli effetti della complessità.

Ricapitolando, quindi, sarà necessario:

- implementare un approccio integrativo per quanto riguarda il rischio e la SSL;
- irrobustire il modello di gestione dei rischi basato sull'anticipazione e su metodologie che tengano in debito conto della complessità e dell'incertezza.

Un altro aspetto da considerare è quello che riguarda, a fronte dei cambiamenti che avverranno, la necessità di garantire la coerenza tra prescrizione, gerarchia e autonomia a livello organizzativo.

Infatti, vista la velocità del cambiamento, le strategie elaborate e praticate per garantire la SSL, possono risultare inadeguate a fronte della crescente complessità e praticamente irrilevanti rispetto al cambiamento che sta avvenendo.

Si pensi, ad esempio, all'AI ed all'accelerazione tecnologica che sta provocando.

Ad esempio, questo articolo, potrebbe essere scritto con il suo supporto(!) senza che nessuno se possa accorgere.

Battute a parte, si è aperto un interessante dibattito su questa innovazione e sui vantaggi che essa potrebbe portare ai fini della SSL.

Il problema, però, è che l'autorità regolatoria non riesce a tenere il passo con l'innovazione.

Al riguardo, attualmente, il dibattito verte su due aspetti.

Il **primo aspetto** è quello che riguarda la dimostrazione che l'adozione delle nuove tecnologie, lo sviluppo dei relativi standard e la definizione di quadro normativo possa portare ad un reale miglioramento dei livelli di SSL.

Il **secondo aspetto** è quello che riguarda la necessità di innovare e adottare velocemente le nuove tecnologie per evitare di rimanere indietro rispetto ad altri Paesi che non prestano molta attenzione a tematiche sociali, etiche e di SSL e, di conseguenza, perdere competitività sul mercato globale.

Per risolvere quello che sembra un dilemma, la scelta non può che essere quella che porta alla sperimentazione di queste innovazioni in contesti protetti al fine di verificare l'efficacia delle nuove tecnologie e solo dopo permetterne la diffusione e l'applicazione sul campo.

Infine, reputo opportuno evidenziare che nonostante la SSL abbia palesemente dimensioni sistemiche, a livello politico, se ne discute poco e solo dopo qualche grave evento che abbia impattato sulla Pubblica Opinione con il risultato di partorire l'ennesima leggina ad alto impatto mediatico ma ad effetto concreto nullo, reiterando così il solito approccio da " *sistema prevenzionale da manutenzione a guasto*".

Da una parte abbiamo continui dibattiti sul futuro dell'industria anche alla luce dei recenti dazi "*trumpiani*" mentre dall'altra, la SSL continua a rimanere sullo sfondo, in una visione sfocata.

Questo perché la SSL, purtroppo, continua ad essere vista come un vincolo o un ostacolo al raggiungimento di migliori performance aziendali in altri ambiti.

Pertanto, è necessario che nel nostro Paese si abbandonino gli approcci che vedono la SSL come qualcosa di specialistico ed estraneo ai normali processi aziendali e si passi ad approcci che la facciano divenire oggetto di discussione negli "*ambienti che contano*", dove vengono definite le strategie e prese le decisioni e cioè in quegli ambienti da cui, fino ad oggi è stata tenuta

fuori o, nella migliore delle ipotesi, fatta entrare dalla porta di servizio solo dopo gravi eventi che hanno impattato sulla Pubblica Opinione.

Carmelo Catanoso

Ingegnere Consulente di Direzione
