ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4129 di Venerdì 24 novembre 2017

Robotica, rischio informatico e sicurezza sul lavoro

È importante riflettere sull'impatto della robotica e dei rischi informatici anche in riferimento alla tutela della salute e sicurezza sul lavoro. Ne parliamo con Roberta Gatto, Michele Colajanni ed Ernesto Cappelletti.

Modena, 24 Nov ? Sono tanti gli aspetti rilevanti, anche con riferimento all'impatto su salute e sicurezza sul lavoro, che riguardano l'attuale evoluzione tecnologica e industriale, gli scenari aperti dalla cosiddetta quarta rivoluzione industriale, la digitalizzazione dei processi di produzione e la crescita del crimine informatico. Tutti aspetti che ormai i vari attori che si occupano di gestione della sicurezza nelle aziende devono conoscere.

Ad esempio è importante soffermarsi sulle conseguenze della diffusione, sempre maggiore nel mondo industriale, della **robotica** o, di fronte alla continua crescita del *cyber crime* e alla possibilità di minacciare la sicurezza delle macchine, su come comportarsi in relazione al **rischio informatico** aziendale.

Per affrontare questi temi e fornire qualche utile informazione ai nostri lettori abbiamo realizzato durante la manifestazione " Ambiente Lavoro Convention" (Modena, 13/14 settembre 2017) un'intervista ad alcune persone che hanno partecipato, come relatori o come referenti organizzativi al convegno modenese "**La ROBOTICA, opportunità e rischi di salute e sicurezza**".

Con **Roberta Gatto** (Coordinatrice politiche ambientali della Confederazione Nazionale dell'Artigianato e della Piccola e Media impresa, CNA), con **Michele Colajanni** (Direttore del Centro di ricerca Interdipartimentale sulla sicurezza e prevenzione dei rischi, CRIS - Università degli Studi di Modena e Reggio Emilia) e con **Ernesto Cappelletti** (direttore tecnico) abbiamo cercato di comprendere quali siano gli aspetti positivi e negativi dei nuovi sviluppi industriali in materia di sicurezza dei lavoratori.

Perché parlare oggi di robotica?

Quanto la robotica è diffusa anche nella piccola e media industria?

Che cosa è il rischio informatico? E perché è un problema che ha a che fare anche con la sicurezza sul lavoro?

Le aziende sono in grado di dare un'idonea valutazione e gestione del rischio informatico?

Ci sono carenze, lacune in materia di leggi e normative tecniche?

Riguardo all'evoluzione dell'industria riusciremo a guidare questo processo di trasformazione e non a subirlo?

Riguardo al rischio informatico, **Michele Colajanni** ci ricorda, ad esempio, alcuni aspetti rilevanti. Oggi sono presenti per le aziende **nuove minacce**: "*l'attaccante può essere motivato da aspetti economici, da aspetti vandalistici, da aspetti, diciamo, di spionaggio dei segreti industriali, da aspetti di ricatto, di guadagno, di crimine tradizionale a cui un industriale non era abituato*". E quindi c'è da portare avanti l'attenzione verso questo tipo di minacce che prima non erano "*parte della cultura industriale*". Ma la vera sfida è **come li trattiamo questi rischi**. E "*quello che è emerso dal convegno è: per favore non pensate che si possono trattare soltanto dal punto di vista tecnologico. Anche se sono coinvolti degli aspetti tecnologici, qui stiamo parlando di processi, stiamo parlando di persone, stiamo parlando di norme da attuare*".

Come sempre diamo ai nostri lettori la possibilità di seguire integralmente la video intervista e/o di leggerne una parziale trascrizione.

Articolo e intervista a cura di Tiziano Menduto

L'utilizzo e le conseguenze della robotica riguardano anche il mondo dell'artigianato e della piccola e media impresa?

Roberta Gatto: "(...) Il mondo della piccola impresa, dell'artigianato, comunemente ma erroneamente, viene considerato un po' lontano dal **tema della robotica**, più in generale delle innovazioni tecnologiche che chiamiamo poi "**quarta rivoluzione industriale**".

In realtà è proprio il contrario. Oggi anche nelle molte presentazioni che sono state fatte in questo convegno, abbiamo visto che i robot ormai hanno uno sviluppo rapidissimo e una diffusione rapidissima che entra anche nelle imprese più piccole. Non è un aspetto che riguarda soltanto le grandi imprese industriali e proprio per questo, come CNA, necessariamente ci dobbiamo interessare a questo tema nel nostro ruolo di supporto alle imprese e, nel caso specifico di supporto alle imprese per aiutarli a rispettare correttamente le regole di salute e sicurezza sui luoghi di lavoro.

Chiaramente con l'avvento della **robotica** il tema della salute e sicurezza sul lavoro cambia e quindi cambiano anche gli strumenti che le nostre imprese devono adottare per essere in regola. Abbiamo affrontato il tema importante dei nuovi rischi che emergono con l'avvento dei robot nel mondo delle imprese e di conseguenza come associazione vogliamo attrezzarci per guidare correttamente le imprese in questo percorso. Anche perché, lo dicevo proprio nel convegno, poi la responsabilità in questo campo ricade sul datore di lavoro quindi, dal nostro punto di vista, è assolutamente opportuno garantire che il datore di lavoro abbia tutti gli strumenti per essere in regola. Ma volendo analizzare non solo il lato delle conseguenze sui nuovi rischi di salute e sicurezza, c'è anche un lato positivo che può essere colto. Ed è il lato positivo derivante da tutte le nuove opportunità che invece questo sviluppo può dare per garantire, invece al contrario, una maggiore sicurezza sui luoghi di lavoro grazie alle nuove tecnologie" (...).

Veniamo al rischio informatico. Come il rischio informatico può avere conseguenze sul tema della sicurezza sul lavoro?

Michele Colajanni: "Nel momento in cui cominciamo a diffondere i componenti elettronici e le connessioni e il software, che sono patrimonio classico dei computer e delle reti di computer, e cominciamo innestarli nel mondo industriale, nel mondo del controllo da remoto, nel mondo robotico è inevitabile che le problematiche di un mondo cyber, più virtuale, si vadano poi a estendere anche al mondo fisico industriale. Quello che abbiamo detto e sostenuto è che **nel momento in cui si parla di software industriale, bisogna agire in maniera più oculata, più attenta**. Non ci possiamo permettere un modello di produzione del software in cui offro dei semilavorati che continuo ad aggiornare, dove continuo a risolvere i problemi offrendo delle patch, delle soluzioni. Ma devo invece cercare di evitare, nei limiti del possibile, più problemi fin dalla progettazione, dall'installazione, dal testing". (...)

C'è abbastanza attenzione nelle aziende sul rischio informatico? Ci sono idonee analisi dei rischi informatici che tengano conto anche degli aspetti relativi alle conseguenze sulla sicurezza dei lavoratori?

Michele Colajanni: "Una cultura dell'analisi dei rischi nelle aziende, mi permetto di dire, è diffusa. **Meno diffusa è l'analisi del rischio informatico in ambito industriale**, questo sì. Però riguardo all'approccio metodologico - quali sono le minacce, quali sono le vulnerabilità, come trattare i rischi ? (...) stiamo parlando della stessa cultura.

E' chiaro che qui ci sono due aspetti diversi.

Uno l'attaccante può essere motivato da aspetti economici, da aspetti vandalistici, da aspetti, diciamo, di spionaggio dei segreti industriali, da aspetti di ricatto, di guadagno, di crimine tradizionale a cui un industriale non era abituato. E quindi c'è da portare avanti l'attenzione verso questo tipo di minacce che prima non erano, diciamo, parte della cultura industriale.

L'altro aspetto è come si trattano questi rischi. Perché l'analisi dei rischi è soltanto la prima fase, poi la vera domanda, la vera sfida, è come li trattiamo. E quello che è emerso dal convegno è: **per favore, non pensate che si possono trattare soltanto dal punto di vista tecnologico. Anche se sono coinvolti degli aspetti tecnologici, qui stiamo parlando di processi, stiamo parlando di persone, stiamo parlando di norme da attuare**".

Trattiamo il tema normativo. Ci sono carenze, lacune in Italia e in Europa? E ci sono normative tecniche idonee?

Ernesto Cappelletti: "Sì, direi che questo aspetto in questo momento non è trattato. Non è trattato dalle leggi e in particolar modo non è trattato dalle direttive europee di prodotto, in particolar modo la Direttiva Macchine. Perché la Direttiva Macchine si preoccupa di far fare una valutazione dei rischi al fabbricante della macchina per quanto riguarda l'uso previsto della macchina o l'uso scorretto ma ragionevolmente prevedibile; quindi **non c'è nessun accenno, nell'ambito della legislazione europea, a un atto criminale quale è un attacco informatico**. L'attacco informatico è un'esplicita violazione di una regola, voluta. Quindi non è come un uso improprio di una macchina, che è un uso fatto in modo appunto improprio, non corretto, ma per un intenzione che è diversa: potrebbe essere quella di usare la macchina in maniera più semplice, potrebbe essere quella di risparmiare del tempo, ma non è quella di commettere un atto criminale. Quindi questo aspetto è completamente fuori da quanto chiede la Direttiva Macchine ed è anche completamente fuori da tutto quello che è la valutazione rischi che riguarda l'ambiente di lavoro. Quindi tutti gli aspetti che, in particolare nel Testo Unico sulla sicurezza nei luoghi di lavoro legislativo (D.Lgs. 81/2008), riguardano ad esempio la valutazione rischi dell'uso delle macchine, (...) **non richiedono che il datore lavoro faccia una valutazione rischi per quanto riguarda attività illegali come sono gli attacchi informatici**.

Questa cosa è sicuramente, al momento, aggravata anche dal fatto che **nemmeno le norme tecniche comprendono questi aspetti**. Le norme tecniche attualmente sono state scritte in conformità con quello che chiede la Direttiva Macchine, sono state scritte come supporto alla la Direttiva Macchine e quindi anche le norme tecniche prevedono di fare una valutazione dei rischi per quanto riguarda l'uso previsto e l'uso ragionevolmente prevedibile delle macchine.

Da questo punto di vista, però, in ambito internazionale ci si sta muovendo. E sia in ambito ISO, cioè per quanto riguarda la

normazione internazionale meccanica, sia in ambito IEC, per quanto riguarda la normazione in ambito internazionale relativa agli equipaggiamenti elettrici ed elettronici, si stanno sviluppando - in ambito ISO un rapporto tecnico, in ambito IEC una norma - che andranno proprio ad affrontare questi aspetti. Ovvero andranno a fornire quelli che saranno i requisiti che i fabbricanti di macchine dovranno rispettare per fare in modo che le loro macchine siano, per quanto possibile, **invulnerabili** ? passatemi il termine, sicuramente improprio, perché non saranno mai invulnerabili - agli attacchi informatici.

Una cosa però fondamentale di queste norme è che stanno già impostando questa valutazione dei rischi come una valutazione che non può limitarsi alla semplice fabbricazione della macchina, in modo tale che i rischi di attacco informatico siano evitati il più possibile. Ma prevedranno una **valutazione dei rischi che poi dovrà continuare, quando la macchina viene utilizzata**. Perché una caratteristica fondamentale delle minacce informatiche è le minacce non sono statiche. Quindi si possono prevedere delle minacce all'atto della fabbricazione della macchina, ma poi nel corso della vita della macchina, queste minacce evolveranno. Quindi anche le misure di protezione dovranno evolvere" (...). E le norme chiederanno quindi di dare delle indicazioni, anche all'utilizzatore della macchina, su come dovrà essere condotta la macchina e quindi anche manutenuto il sistema di sicurezza informatico, in modo tale che questa sicurezza sia mantenuta nel tempo".

Veniamo all'ultima domanda. Riguardo all'evoluzione tecnologica, informatica del mondo industriale riusciremo a guidare questo processo di trasformazione e non solo a subirlo? Da questo punto di vista siete ottimisti o pessimisti?

Ernesto Cappelletti: "Io penso che il mondo industriale riuscirà ad affrontare questa minaccia. (...) Il problema è sicuramente che queste minacce (...) sono in costante aumento. Quindi nonostante si continuino ad aumentare le difese, gli investimenti e la sicurezza informatica, le minacce continuano ad aumentare. Quindi c'è una proporzione diretta tra minacce e, comunque, difese. Però io sono assolutamente convinto che il mondo industriale riuscirà a difendersi, perché lo si deve fare. (...)

Mi viene da dire che a metà degli anni 90, quando sono state introdotte le direttive, in particolare la direttiva macchine, il mondo industriale non sapeva cosa fosse la valutazione dei rischi di una macchina. Ad oggi mi permetto di dire che oramai tutti i fabbricanti di macchine hanno la valutazione rischi nel proprio DNA. E quindi questo è stato proprio un processo di trasformazione culturale che è già avvenuto. Sono molto ottimista che il prossimo processo avverrà come è successo in passato per questo".

Michele Colajanni: "Anch'io tendo all'ottimismo (...) perché vedo dei trend. Il parlare di queste cose 3-4 anni fa, non avrebbe trovato ascolto. Già adesso c'è molta più sensibilità, la tematica cyber è uno dei nove "pillar" dell'Industria 4.0, l'Europa ha emanato una direttiva sulle infrastrutture critiche che poi sono fondamentalmente le industrie dell'energia, del trasporto. Quindi alcuni settori saranno trainanti per quanto riguarda queste tematiche.

Senza dubbio è una **sfida enorme** perché non riguarda solo una componente industriale, riguarda tutto l'ecosistema industriale, perché si può arrivare ad attaccare una macchina da un'email, da una rete, da un wireless, da una chiavetta USB: quindi non sarà facile. La consapevolezza che stiamo portando avanti è senza dubbio il primo passo. Ci sono già delle soluzioni, ci saranno delle buone pratiche, ci saranno senza dubbio delle norme, ci saranno degli investimenti e poi ci sarà quel processo dove un prodotto industriale più sicuro avrà più mercato di uno insicuro e quindi in questo caso il prodotto sicuro butterà via la moneta meno valida (...)".

Roberta Gatto: "Anch'io proseguo nella scia positiva, con qualche nota importante. Sicuramente la scelta non è se percorrere questa strada, perché questo cambiamento è già in corso ed è in corso anche velocemente. Il punto non è se decidiamo di cogliere questa occasione, ma **come decidiamo di coglierla**. E da questo punto di vista i passi ancora da fare per attrezzarci sono tanti e sono tanti non soltanto dal punto di vista del sistema economico, del sistema imprese, sono tanti come sistema-paese. È un cambiamento rapido e complesso e per gestirlo correttamente, per gestirlo anche tenendo conto di tutti gli impatti che abbiamo visto oggi, non soltanto in materia di salute e sicurezza nei luoghi di lavoro (...), dobbiamo percorrere una strada avendo chiara la strategia. Allora ci deve essere un **impegno del decisore politico**, che in parte ha avviato un percorso

(...) ma in maniera ancora un po' timida. E tra l'altro, direi, in maniera timida anche nel campo specifico nell'impatto che si ha sulla salute e sicurezza sui luoghi di lavoro. Sicuramente serve anche un impegno del mondo delle imprese, che però da sole non possono farcela (...)".