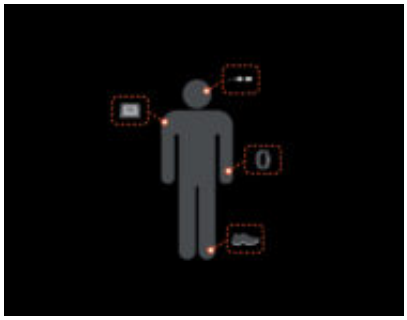
Dispositivi di Protezione Individuale e tecnologie Smart

Author : Giovanni Villarosa

Date : 21 Maggio 2019



PPE Smart, *Personal Protective Equipment Smart*, ovvero attrezzatura protettiva personale **intelligente**: è composta da tutta la **galassia** dei Dispositivi Individuali di Protezione (DPI) definiti dall'art 74 del D.Lgs n° 81/2008 (conosciuto come testo unico sulla sicurezza e adeguato al Regolamento europeo UE 2016/425), ed equipaggiati da tutta una tipologia di sensoristica *smart* di sicurezza, funzionale al mondo IoT (Internet of Things).

L'espressione *Internet of Things* ci indirizza comunemente ad una rete di **oggetti** (devices) interconnessi, **attrezzati** con tecnologie di riconoscimento capaci di **interagire** tra loro e/o verso i punti nodali di un sistema informatico dedicato che li governa.

La tecnica e la tecnologia hanno prodotto una moltitudine di **oggetti** di uso quotidiano, che rientrano nel perimetro IoT; analizzando le stime di Gartner (leader mondiale nella consulenza strategica), emergono dati interessanti: nel 2018 il numero dei dispositivi connessi oscillava sulla cifra di 8,3 miliardi, con una previsione per il 2019 di 14,2 miliardi di oggetti in rete, che diventeranno poi **20,4 miliardi nel 2020** e un'ipotesi per il 2021 che sfiorerà il tetto dei 25 miliardi di *devices* interconnessi.

Ora, oltre ai numeri della crescita nell'uso dei dispositivi, la piattaforma IoT rappresenta, in primo luogo, un valore di mercato notevole; difatti questo vale, a livello domestico, circa 5 miliardi di euro, segnando un positivo +35% rispetto al fatturato del 2017, una crescita resa possibile grazie anche agli incentivi previsti dal Piano Nazionale Industria 4.0.

Non v'è dubbio, dunque, di come la combinazione delle tecnologie offerte dall'**architettura** IoT, a supporto dei DPI (dispositivi previsti all'interno del DVR), apra nuovi e interessanti scenari nella **tutela della salute e sulla sicurezza dei lavoratori**, offrendo nuovi strumenti e nuove strategie aziendali in una prospettiva di riduzione/eliminazione dei rischi connessi alla prestazione lavorativa, associabili parallelamente ai due ambiti, quelli *safety* e *security*, contenuti nel perimetro più ampio della sicurezza.

Non solo: se consideriamo che la maggior parte degli infortuni avvenuti in attività operative è dovuta all'uso improprio dei dispositivi individuali, allora possiamo affermare che dispositivi

evoluti come i DPI smart offriranno prospettive di miglioramento proprio nella gestione delle **misure di prevenzione**; infatti, tali strumenti di sicurezza si trasformeranno sempre più, da semplici dispositivi ad azione passiva, in attivi **presidi** di sicurezza a forte connotazione **proattiva**, perché la prevenzione degli incidenti si svilupperà, primariamente, sul dialogo automatico e bidirezionale, tra i dispositivi di protezione/lavoratori e il campo operativo.

Come visto, solo utilizzando questa tecnologia è possibile organizzare un *network* di dispositivi capaci di trasmettere e ricevere dati e/o informazioni, **reagendo***,* peraltro, alle informazioni acquisite senza alcun bisogno dell'intervento umano.

Le tecnologie *smart* come il bluetooth, le webcam, i tablet, di uso comune nella quotidianità, sono diventati ormai, nell'industria 4.0, strumenti fondamentali per migliorare e rendere più efficiente la sicurezza industriale, tanto in ambito *safety* quanto in quello della *security*, aumentando nel contempo la **consapevolezza** degli operatori in situazioni di emergenza.

Sistemi inerziali composti da sensoristica smart come i giroscopi, gli accelerometri, per citarne alcuni, quando indossati dall'operatore consentono di gestire situazioni di emergenza anche in condizioni di scarsa visibilità, come ad esempio in presenza di fumo (DPI usati dalle squadre antincendio).

Dunque l'evoluzione tecnologica dei DPI, integrati ai sistemi IoT, aumenterà l'efficacia di questi dispositivi, per esempio: nei processi industriali, supervisionando le attività nell'uso di macchinari particolari, un contesto dove un **utilizzo non conforme** dei dispositivi di protezione ne impedirà l'attivazione (avendo i sensori preventivamente analizzato il mancato rispetto delle condizioni di sicurezza) o, allo stesso modo, ne interromperà il funzionamento, se l'operatore se ne libera prima delle fine delle attività, registrando, per di più, tutti gli eventi del processo in un log dedicato, a tutto vantaggio della *safety*.

Un elenco cronologico tipico delle attività **misurate** dai sensori indossati, con dati raccolti in un database che permettano successive verifiche analitiche, utili alla creazione di nuove policy di sicurezza, o correggerne di esistenti, lo possiamo così riassumere:

- elenco DPI, profili di lavoro con lista DPI obbligatori associati;
- gestione degli allarmi;
- visualizzazione dei dati storici e delle statistiche;
- autenticazione dell'operatore e selezione del profilo di processo autorizzato;
- verifica dei DPI previsti, con inibizione delle operazioni se la dotazione risulta inappropriata, incompleta, o erroneamente indossata;
- generazione di un allarme sonoro nel caso di mancata rilevazione dei DPI previsti;
- possibilità per l'operatore di escludere o aggiungere particolari DPI;
- tasto di emergenza per l'operatore (invio di un allarme contenente la posizione geografica per una rapida localizzazione nell'intervento dei soccorsi);
- invio eventi/allarmi in tempo reale a una SOC.

Dal precedente elenco si nota immediatamente come nell'area *safety* la piattaforma IoT (tecnologia dalle potenzialità fino a qualche anno fa impensabili) rappresenti un tangibile

supporto, una grande opportunità per migliorare la sicurezza nelle attività lavorative.

Infatti, fra i dispositivi tecnologicamente più avanzati e applicabili, troviamo:

- dispositivi in grado dirilevare un impatto da caduta, meglio conosciuti come dispositivi di **uomo a terra**, e di comunicarlo direttamente alla SOC ;
- dispositivi in grado di monitorare le dispersioni di gas nocivi nell'area operativa, trasmettendone l'allarme alla SOC, che attiverà le misure di primo soccorso;
- dispositivi in grado di verificare l'integritàdelle combinazioni da lavoro utilizzate in ambienti **contaminati***,* o di segnalarne le potenziali situazioni di pericolo, come il rischio da schiacciamento*,* o la vicinanza dell'operatore ad un'area di manovra e/o di pericolo;
- dispositivi in grado di emettere allarmi di *security* alla SOC, nel caso in cui un operatore risulti vittima di un'aggressione.

Abbiano visto fin qui come le tecnologie IoT consentiranno di assicurare una maggiore protezione dagli infortuni sui luoghi di lavoro, ma soprattutto come miglioreranno la sicurezza dei lavoratori, ma a determinate condizioni, perché con l'aumento dei *devices* interconnessi crescerà anche la quantità di dati prodotti, un fatto questo, che pone una serie di interrogativi: chi proteggerà questa **nuova vulnerabilità** legata a questa tipologia di Big Data? Quali garanzie per il rispetto della *compliance* in tema di controllo a distanza prevista dallo Statuto dei Lavoratori (art 4 Legge n° 300/1970, riformato dall'art. 23 D.Lgs n°151/15 e successivamente novellato dall'art. 5 com. 2 del D.Lgs n° 185/16) e della tutela della privacy? Quali implicazioni sull'intero ciclo della conformità, prevista nel Regolamento GDPR UE 2016/679, in materia trattamento e protezione dei dati personali raccolti?

Quesiti che, come è facile immaginare, innescano un'immediata riflessione sul come, realmente, tali strumenti possano essere conformi al divieto di controllo a distanza dei lavoratori ma, soprattutto, al **trattamento dei dati personali** e alla tutela della privacy.

Orbene, in osservanza al primo punto, è noto come l'art. 4 dello Statuto disciplini l'uso degli **strumenti** aziendali, da cui possa derivare anche incidentalmente un **controllo a distanza dei lavoratori**, autorizzandolo esclusivamente per determinati fini (necessità organizzative, aziendali, tutela della sicurezza del lavoro e del patrimonio aziendale), ma previa concertazione con le RSU/RSA, e dove mancante, per mezzo dell'autorizzazione preventiva rilasciata dall'ispettorato del lavoro; ricordiamo, però, come la stessa norma preveda una **deroga** espressamente riservata agli **strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa**.

Dunque, letto ciò, i DPI quando sono previsti come **obbligatori** dal documento di valutazione dei rischi (DVR), saranno considerati come gli strumenti di lavoro **necessari per rendere la prestazione lavorativa in sicurezza**, rientrando così *inter partes*, nella eccezione contenuta all'interno del comma 2 dell'art. 4 dello Statuto.

In quanto al secondo punto, poi, non va dimenticato che tutti i dati raccolti dai sensori **intelligenti** contenuti nei DPI devono essere trattati (intero ciclo di trattamento del dato e fino alla sua cancellazione) nel pieno **rispetto del Regolamento GDPR** (DPIA, privacy by design e

by default, misure di sicurezza, etc) osservando gli obblighi previsti in tema di trattamento, conservazione, sicurezza e cancellazione del dato personale.

Questi due aspetti consentiranno di contemperare, da un lato, le esigenze di protezione dei dati e della tutela della privacy e, dall'altro, le esigenze di tutela della salute e sicurezza sul luogo di lavoro, a garanzia del lavoratore dipendente.

Ma c'è un ulteriore aspetto da non sottovalutare: quello della *security* logica e fisica dei dispositivi e dei dati, perché con l'espansione continua del c.d. **trend IoT,** applicabile al settore dei DPI smart, le organizzazioni aziendali dovranno dotarsi di un robusto *framework* di *governance* per assicurare una corretta **conformità** al GDPR, in tema di raccolta, archiviazione, utilizzo in sicurezza delle informazioni, come pure per la sicurezza dei processi di aggiornamento dei firmware relativi ai dispositivi IoT.

Quest'ultima maggiore tutela è più sentita da tutte quelle aziende che implementano sistemi e dispositivi IoT di terze parti, perché non avendo il controllo *ab origine* dei software e degli hardware contenuti nei dispositivi utilizzati, devono una particolare attenzione a eventuali attacchi cyber.

In ultima analisi, nonostante il costoso esborso nell'investimento iniziale delle **tecnologie indossabili**, possiamo senz'altro affermare come il risparmio in termini di salute e sicurezza del personale sia incalcolabile!

Avere una traccia in *real time* su dove si trova il singolo dipendente, come un intero *staff*, osservando da remoto cosa accade realmente **sul campo***,* è di fondamentale importanza per l'incolumità degli operatori, cosicché in situazioni di **sicurezza degradata** si potranno impartire le corrette istruzioni da applicare (soprattutto da grandi distanze fa certamente la differenza), anche perché, con le aziende ormai completamente **digitalizzate** occorrono lavoratori intelligentemente equipaggiati!

Siamo ormai giunti alla concretizzazione dei **sistemi adattivi** composti, dalle reti neurali al *machine learning*, tutti temi strategici dell'Internet of Things.

Sitografia

https://www.gartner.com/en.

https://www.puntosicuro.it/.

https://www.anfos.it/.

https://www.osservatori.net/it_it/.

Articolo a cura di **Giovanni Villarosa**