PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5585 di Venerdì 22 marzo 2024

Le nuove tecnologie, gli obblighi datoriali e il problema della delega

Un contributo si sofferma sulla tecnologia Internet of Things e sull'impatto sugli obblighi datoriali in materia di salute e sicurezza. L'art. 2087, la deriva algoritmica, il principio del controllo umano, la delega di funzioni e i modelli organizzativi.

Urbino, 22 Mar ? La **nuova campagna** 2023-2025 " Sicurezza e salute sul lavoro nell'era digitale" che, promossa dall'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA), sarà lanciata a ottobre, ci permetterà non solo di conoscere più da vicino le nuove tecnologie e le loro applicazione in materia di sicurezza e salute, ma anche di affrontarne i possibili rischi e l'impatto sul mondo del lavoro.

E una tecnologia che ha grandi potenzialità è quella connessa all'**Internet of Things** (IoT - Internet delle Cose), con riferimento ad un insieme di connessioni internet operate da oggetti e da luoghi, senza l'intervento di operatori umani.

Ne abbiamo parlato sul nostro giornale più volte, anche in relazione ai cosiddetti dispositivi di protezione individuale evoluti o smart, e abbiamo anche presentato un interessante contributo/saggio pubblicato sul numero 2/2022 di "**Diritto della sicurezza sul lavoro**", rivista online dell'Osservatorio Olympus dell' Università degli Studi di Urbino.

Il contributo "**Internet of Things al servizio della salute e della sicurezza dei lavoratori**", di Antonio Ambrosino (assegnista di ricerca di Diritto del lavoro nell'Università di Modena e Reggio Emilia), esamina in particolare il nell'ambito del rapporto di lavoro con riferimento all'impiego della c.d. "**tecnologia indossabile**", che rappresenta un'area di sviluppo dell' Internet of Things.

Dopo aver già presentato il saggio per quanto riguarda applicazioni e rischi delle tecnologie IoT, ci soffermiamo oggi invece sulla sua interessante analisi della possibilità, da parte del datore di lavoro, di poter assolvere all'obbligazione di sicurezza di cui all'**art. 2087** c.c. mediante l'utilizzo della tecnologia dell'Internet of Things o delle nuove tecnologie direttamente connesse, o meno, ai sistemi di intelligenza artificiale.

L'articolo si sofferma, dunque, sui seguenti argomenti:

- La tecnologia Internet of Things, gli obblighi datoriali e l'art, 2087 cc
- I rischi, il principio del controllo umano e i possibili problemi delle deleghe
- Le nuove tecnologie, gli algoritmi e i modelli di organizzazione e gestione

La tecnologia Internet of Things, gli obblighi datoriali e l'art, 2087 cc

Riguardo all'adempimento dell'**obbligo datoriale di sicurezza** si indica che un primo elemento da indagare è la possibilità, da parte del datore di lavoro, di "poter assolvere all'obbligazione di sicurezza di cui all'art. 2087 c.c. (*L'imprenditore è tenuto ad adottare nell'esercizio dell'impresa le misure che, secondo la particolarità del lavoro, l'esperienza e la tecnica, sono necessarie a tutelare l'integrità fisica e la personalità morale dei prestatori di lavoro*) mediante l'utilizzo della tecnologia dell'Internet of Things".

Insomma va verificato "se l'**affidamento all'IoT** possa concretamente garantire e salvaguardare l'integrità fisica e la personalità morale dei prestatori di lavoro". E una tale verifica "va, altresì, estesa agli obblighi datoriali scaturenti dal decreto legislativo 9 aprile 2008 n.81 (Testo unico della sicurezza), con cui il legislatore ha riempito di specifici contenuti l'obbligazione generale di cui all'art. 2087 c.c".

Tra l'altro tale verifica è ancor più necessaria considerando le indicazioni fornite dall'**art. 20 del decreto legge 30 aprile 2022, n. 36** (recante "*Ulteriori misure urgenti per l'attuazione del Piano Nazionale di Ripresa e Resilienza*"), che "prevede la possibilità per l'INAIL di porre in essere con aziende e grandi gruppi industriali, impegnati nella esecuzione dei singoli interventi previsti dal Piano nazionale di ripresa e resilienza, appositi protocolli per la sperimentazione delle nuove tecnologie al fine di migliorare gli standard di salute e sicurezza sui luoghi di lavoro". E tale articolo 20, tra le soluzioni tecnologiche da sperimentare, "annovera segnatamente '*esoscheletri, sensoristica per il monitoraggio degli ambienti di lavoro, materiali innovativi per l'abbigliamento lavorativo, dispositivi di visione immersiva e realtà aumentata*', tutte applicazioni che potrebbero astrattamente rispondere alla tecnologia dell'Internet of Things".

I rischi, il principio del controllo umano e i possibili problemi delle deleghe

A questo proposito si sottolinea che bisogna anche valutare "la prospettiva di un **adempimento "disumano"** dell'obbligazione di sicurezza, grazie alle connessioni telematiche di cui all' Internet of Things", adempimento che "genererebbe, in prima battuta, delle forti criticità in relazione all'imputazione di responsabilità in caso di infortunio o nocumento alla persona del lavoratore".

Infatti alcuni dispositivi intelligenti "potrebbero avocare a sé alcune valutazioni ed adottare delle misure che ordinariamente spetterebbero al datore di lavoro".

Tuttavia l'autore ricorda che bisogna distinguere "eventuali smart DPI funzionanti su base algoritmica da quelli dotati di una vera e propria intelligenza artificiale, come potrebbero essere gli strumenti rispondenti alle regole tecnologiche dell'Internet of Things". E la differenza non è di poco conto, poiché, come ha avuto modo di affermare di recente anche la giurisprudenza amministrativa" (**Cons. Stato, sez. III, 25 novembre 2021, n. 7891**), "i sistemi tecnologici su base algoritmica svolgono operazioni meccaniche con risultati volti al raggiungimento di un determinato obiettivo; gli automatismi caratterizzanti il sistema algoritmico, sebbene riducano sensibilmente l'intervento dell'uomo, sono comunque rispondenti ai meccanismi preimpostati dallo stesso agente umano".

Invece l'intelligenza artificiale "non si limita ad applicare i parametri preordinati dall'uomo, ma è essa stessa a possedere capacità deduttive, **elaborando dati ed assumendo decisioni** sulla base di un algoritmo evoluto". E dunque "**più è intelligente il dispositivo di sicurezza e più la delegittimazione del ruolo del datore**, quale garante dell'obbligo di sicurezza di cui all'art. 2087 c.c., **è profonda**, con il fondato pericolo di minare le pretese di adempimento da parte del lavoratore".

In questa situazione - continua il contributo ? un **argine alla deriva algoritmica** del dovere di tutela della persona del lavoratore può risiedere nel "**principio del controllo umano**, secondo cui l'essere umano deve conservare un controllo su quanto svolto dalla macchina, unitamente alla possibilità di intervento sulle decisioni ed i risultati frutto delle elaborazioni dell'intelligenza artificiale". È infatti il rispetto di questo principio che "preserva la posizione di garanzia del datore di lavoro, che continua ad essere l'unico responsabile dell'implementazione dei diversi usi dei dispositivi di sicurezza intelligenti".

Tra l'altro il **controllo umano**, quale elemento di gestione delle tecnologie di *machine learning*, "è stato invocato anche dalle maggiori confederazioni sindacali e imprenditoriali europee nell'accordo quadro europeo sulla digitalizzazione" (giugno 2020).

Nel documento viene espressamente affermato che '*Il controllo degli esseri umani sulle macchine e sull'intelligenza artificiale dovrà essere garantito sul posto di lavoro e dovrà supportare l'utilizzo della robotica e delle applicazioni di intelligenza artificiale, nel rispetto dei controlli di sicurezza*'.

In questo senso la sfida non è tanto quella di "prevedere astrattamente un principio generale di controllo, eventualmente ex ante ovvero ex post, sulle decisioni dell'intelligenza artificiale assunte in sostituzione del management aziendale", ma di "concepire una **verifica istantanea dei meccanismi decisionali della macchina**". E in tema di salute e sicurezza rimesse alla tecnologia IoT, "si potrebbe immaginare provocatoriamente, ad esempio, una **delega circoscritta di funzioni al dispositivo intelligente**, analoga all'art. 16 del d.lgs. n. 81/2008, secondo cui il trasferimento di funzioni o attività non esclude comunque '*l'obbligo di vigilanza in capo al datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite*'".

L'istituzione concettuale del "**rapporto di mandato tra delegante umano e delegato digitale**" ? continua il saggio ? "potrebbe permettere di ridurre le incertezze su come le intelligenze artificiali sviluppano le proprie regole, in quanto il mandante potrebbe trasferire unicamente le attività controllate o controllabili, escludendo tutte le evoluzioni algoritmiche non previste dai programmatori del dispositivo di IoT. Ma "una tale costruzione giuridica ? ovviamente solo teorica, stante la condivisione ed assunzione di responsabilità, anche penali, in capo al delegato, giocoforza non imputabili agli strumenti algoritmici - però genererebbe ulteriori opzioni sinora non contemplate nell'attuale panorama interpretativo".

Ad esempio si può pensare agli "attuali approdi giurisprudenziali che hanno, in materia di obblighi prevenzionistici, individuato **due distinte ipotesi di delega** di cui all'art. 16 del d.lgs. n. 81/2008:

- una **esecutiva**, non traslativa del debito prevenzionistico e delle relative responsabilità, in quanto costituisce solo lo strumento con il quale il debitore, non spogliato della propria posizione passiva ex art. 2087 c.c., decide di adempiere i propri obblighi avvalendosi dell'ausilio di propri incaricati, ai sensi dell'art. 1228 c.c.;
- una di **natura funzionale**, affidando al delegato, a titolo derivativo, l'obbligo di sicurezza e, conseguentemente, imputando al datore le inadempienze del delegato a titolo di responsabilità oggettiva secondo il disposto dell'art. 2049 c.c.".

In questo caso l'utilizzo di dispositivi di sicurezza intelligenti capaci di elaborare dati ed assumere decisioni al posto del datore in un'ottica prevenzionistica sfumerebbe "la predetta distinzione tra delega esecutiva e delega funzionale a seconda del grado di autonomia 'decisionale' del dispositivo, seppur definito preventivamente dal datore al momento dell'adozione del sistema algoritmico, come ipotizzato inizialmente".

Insomma si renderebbe "**difficoltosa l'individuazione dei contorni dell'obbligazione di sicurezza del datore, nonché il titolo**

giuridico delle responsabilità a quest'ultimo ascrivibili". E se l'affidamento al dispositivo digitale "fosse meno marcato il datore continuerebbe ad essere il debitore principale dell'obbligo di sicurezza di cui all' art. 2087, utilizzando il dispositivo intelligente in via meramente funzionale, quale palese espressione di adeguamento dell'adempimento alla massima sicurezza tecnica, organizzativa e procedurale possibile". Mentre nell'ipotesi in cui il dispositivo digitale "venisse adoperato dal datore non in via strumentale, ma principale e sostitutiva dei compiti prevenzionistici, si avrebbe una (indebita) trasposizione dell'obbligazione di sicurezza, e, in virtù della predetta successione atipica, andrebbero individuati dei nuovi profili di responsabilità non necessariamente rispondenti ai canoni degli artt. 1228 e 2049 c.c".

Le nuove tecnologie, gli algoritmi e i modelli di organizzazione e gestione

In definitiva la diffusione attuale e futura della tecnologia dell'Internet of Things in materia di sicurezza "genera delle prevedibili preoccupazioni in quanto l'**algoritmo potrebbe sfuggire all'operatore** e, in autonomia, quale *falsus procurator*, avocare a sé anche attività e funzioni spettanti per legge al solo datore, come ad esempio l'adozione, a seguito di un'autonoma determinazione algoritmica, di misure ritenute opportune per garantire il miglioramento nel tempo dei livelli di sicurezza, rientranti tra gli obblighi non trasferibili a terzi soggetti ai sensi dell'art. 17 del d.lgs. n. 81/2008". Quindi, anche il meccanismo della delega "potrebbe risultare inidoneo a contenere la macchina 'pensante'".

Si indica che l'unico vero argine, al di là della veste giuridica attribuita al *machine learning*, "è la **capacità di monitoraggio ed intervento da parte del datore**".

E la capacità del datore di resettare i dispositivi intelligenti "deve sussistere sia sul piano prettamente operativo sia sul piano macro-organizzativo, come richiesto, d'altronde, dall'**art. 30 del d.lgs. n. 81/2008**, che prevede un idoneo sistema di controllo sull'attuazione del **modello di organizzazione e gestione** e sul mantenimento nel tempo delle condizioni di idoneità delle misure adottate e, soprattutto, il riesame e la modifica del modello stesso tutte le volte che si verificano violazioni significative delle norme relative alla prevenzione degli infortuni e all'igiene sul lavoro, ovvero in occasione di mutamenti nell'organizzazione e nell'attività in relazione al progresso scientifico e tecnologico".

E dunque un modello di organizzazione e gestione, "se correttamente concepito ed attuato, permette l'implementazione di tutti gli strumenti tecnologici, realizzando il concreto adempimento degli obblighi datoriali di protezione e prevenzione finalizzati alla tutela dell''integrità fisica' e della 'personalità morale' dei prestatori di lavoro ex art. 2087 c.c.". Ed è proprio il carattere intrinseco di questi modelli di gestione che può garantire (ed imporre) al datore "di **governare, sul piano organizzativo, ogni risvolto tecnologico**".

Rimandiamo, in conclusione, alla lettura integrale del breve saggio che riporta anche utili considerazioni sulla compatibilità delle innovazioni tecnologiche con la tutela della privacy dei dati dei prestatori di lavoro, con riferimento ad alcune posizioni prese in questi anni (Parlamento europeo, Gruppo di lavoro sulla protezione dei dati, Garante della privacy, ...) in relazione alle tecnologie IoT e ai sistemi di intelligenza artificiale.

Tiziano Menduto

Scarica il documento da cui è tratto l'articolo:

Università di Urbino Carlo Bo, Osservatorio Olympus, Diritto della sicurezza sul lavoro, "Internet of Things al servizio della salute e della sicurezza dei lavoratori", a cura di Antonio Ambrosino, assegnista di ricerca di Diritto del lavoro nell'Università di Modena e Reggio Emilia, DSL n. 2/2022.

---

www.puntosicuro.it