Chiara Piccaglia De Eccher
Avvocato penalista,
componente della Rete Giuridica AIAS

Stefania Calosso
Avvocato, Cultrice della materia Data Protection Law presso l'Università di Bologna,
componente della Rete Giuridica AIAS

Smart DPI: *punctum dolens* o opportunità?

Le innovazioni tecnologiche e, in particolare, l'intelligenza artificiale (AI), applicate al mondo del lavoro, seppur ricche di potenzialità, presentano profili di elevata criticità che potrebbero, da un lato, alterare i meccanismi di esercizio dei diritti del lavoratore e, dall'altro, snaturare il ruolo del Datore di Lavoro.

Le decisioni "suggerite" (e, talvolta o per lo più, "assunte" direttamente) dallo strumento tecnologico, infatti, riguardano, per quanto qui rileva, la salute e la sicurezza dei lavoratori e i suoi diritti fondamentali: in questo contesto, la tecnologia, per preservare la salute del dipendente, si "alimenta" dei dati personali di quest'ultimo senza che il Datore di Lavoro possa intervenire nei processi di elaborazione di tali dati.
Con riferimento ai DPI (dispositivi di protezione individuali), siano essi tradizionali o "smart", è noto come l'art. 77 del D.Lgs. 81/08 imponga al Datore di Lavoro di effettuare analisi e valutazione dei rischi che non possano essere evitati con altri mezzi, di individuare le caratteristiche dei dispositivi, di valutarne le peculiarità e di procedere a un periodico aggiornamento.

Con riguardo agli Smart DPI va segnalato che la loro adozione comporta il sorgere, in capo al Datore di Lavoro, di un ulteriore e duplice obbligo:

- la verifica del pieno rispetto delle tutele in materia di privacy e protezione dei dati personali
- l'osservanza di quanto disposto dall'art. 4 dello Statuto dei Lavoratori in materia di controllo a distanza.

Il primo tema non è nuovo in realtà: esso era già stato affrontato dalla Commissione Europea, la quale, con Raccomandazione del 12 maggio 2009 "sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenze", oltre a fornire degli orientamenti sulla progettazione e l'uso delle applicazioni RFID (Radio Frequency ID Devices, tipologia di dispositivo di IoT) in modo giuridicamente, eticamente, socialmente e politicamente accettabile, ha raccomandato – specularmente a quanto previsto in tema di salute e sicurezza del lavoro, leggasi Valutazione del Rischio – lo svolgimento di una valutazione di impatto preventiva rispetto alla loro adozione.
Ancora, il Gruppo di lavoro 29, già a partire dal 2005, ha analizzato le problematiche relative allo IoT in diversi documenti, fornendo una serie di raccomandazioni con l'intento di realizzare una regolamentazione uniforme, con l'identificazione dei ruoli

e delle responsabilità dei soggetti che si confrontano con tale tecnologia.
Nel nostro ordinamento, infine, il Garante per la protezione dei dati personali ha adottato, in data 9 marzo 2005, un Provvedimento dedicato all'analisi della tecnologia RFID sottocutanea, caldeggiando un utilizzo eccezionale e per comprovate e giustificate esigenze di tutela della salute e nel pieno rispetto del divieto di controllo a distanza del lavoratore (art. 4 della legge 20 maggio 1970, n. 300).

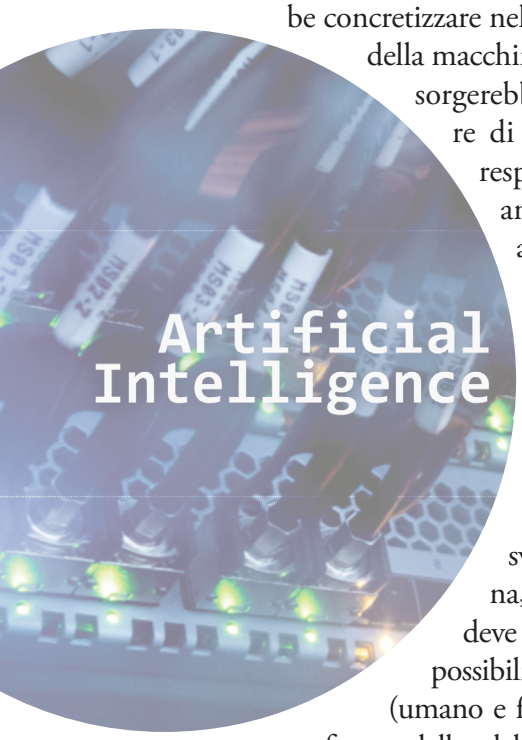
Le tecnologie IoT e i dispositivi wearable

Tutte indicazioni, quelle poc'anzi richiamate, alquanto utili nel presente contesto e, segnatamente, quella afferente la preventiva valutazione di impatto che il titolare del trattamento, allorché sia previsto l'utilizzo di nuove tecnologie, deve svolgere ai sensi dell'art. 35 GDPR: il Garante ha infatti a tal fine specificamente individuato tra le tecnologie IoT i dispositivi wearable, tra i quali rientrano la più parte degli Smart DPI.
Sotto il secondo profilo, così come attualmente strutturata, la tecnologia IoT sembrerebbe conforme all'art. 4 SL.

In altri termini, ascrivere tra i filtri giustificativi di cui al comma 1 dell'art. 4 SL la sicurezza del lavoro attribuisce pienezza legislativa ai controlli effettuati mediante loT, pur inasprendo la loro predisposizione da parte del Datore di Lavoro, il quale, per non incorrere in violazioni normative, deve seguire una procedura di codeterminazione con le rappresentanze sindacali, ovvero, in mancanza di accordo, richiedere un'apposita autorizzazione amministrativa presso la sede territoriale competente dell'INL.

Fermo restando il rispetto della procedura anzidetta, ai sensi del comma terzo della disposizione in esame, i dati raccolti mediante l'utilizzo di dispositivi di sicurezza intelligenti devono essere preceduti, ai fini della loro utilizzabilità nell'ambito del rapporto di lavoro, da un'adeguata informativa e dal pieno rispetto del Codice della privacy e del Reg. (UE) n. 2016/679.
Ma è proprio qui che risiede il *punctum dolens* della tecnologia loT integrata negli Smart DPI in tema di controllo a distanza.
Infatti, se il controllo, previo rispetto delle formalità richieste, parrebbe *prima faciae* essere legittimo ai sensi sia del comma 1 sia del comma 3 dell'art. 4 SL, l'utilizzazione delle informazioni potrebbe in

realtà risultare problematica poiché queste, essendo elaborate autonomamente dallo stesso dispositivo, non sono "gestite" unicamente dal Datore di Lavoro/Titolare del trattamento, ma giungono a quest'ultimo in via mediata.
Non v'è chi non veda come ciò impatti fortemente sul profilo garantistico cui è chiamato il Datore di Lavoro in tema di sicurezza dei lavoratori.
A tal riguardo, infatti, egli potrebbe essere chiamato a rispondere anche di un ulteriore profilo che si potrebbe concretizzare nella *culpa in educando* della macchina. Di conseguenza, sorgerebbe in capo al Datore di Lavoro un dovere/responsabilità che si andrebbe a sommare alle "tradizionali" *culpa in vigilando* e *culpa in eligendo*.



Il Datore di Lavoro, infatti, ad avviso di chi scrive, deve conservare il controllo di quanto svolto dalla macchina, o, quantomeno, deve potersi riservare la possibilità di un intervento (umano e finale) sulle decisioni frutto delle elaborazioni dell'AI, in special modo, ad esempio, con riguardo a quegli Smart DPI che orientano il comportamento del lavoratore.
Nella complessità del quadro sin a qui delineato, il principio di protezione e sicurezza dei dati by design e by default contenuto nell'art. 25 del Reg. (UE) n. 2016/679 potrebbe venire in soccorso del Datore di Lavoro, non solo sotto il profilo della compliance alla normativa sulla protezione dei dati bensì, con i dovuti adeguamenti, anche sotto quello della compliance al TUSIC.

La trasversalità delle due materie è evidente se si considera l'evoluzione dei sistemi di intelligenza artificiale che governano il funzionamento delle tecnologie IoT e, al contempo, l'interrelazione sussistente tra i sistemi di intelligenza artificiale e i dati personali: la connessione tra algoritmi evoluti e dati è, infatti, così profonda che i primi sono alimentati dai secondi.
Ciò implica che errori, imprecisioni o irregolarità nel trattamento e nella elaborazione di dati funzionali all'alimentazione della macchina, potrebbero sfociare in distorsioni del processo decisionale virtuale e condurre a conseguenti indicazioni errate al lavoratore, con pericoloso effetto paradosso.
Il *trait d'union* tra i due ambiti disciplinari – protezione dei dati e sicurezza sul lavoro – potrebbe quindi rinvenirsi nella opportunità/necessità di garantire al Datore di Lavoro, sin dalla progettazione e per impostazione predefinita, la facoltà di controllo e, al contempo, di intervento rispetto ad ogni decisione assunta dalla macchina, onde poter configurare la riferibilità e/o la riconducibilità della decisione finale in capo a un soggetto fisico.
Il dibattito sull'inquadramento giuridico del potere decisionale autonomo delle tecnologie che integrano sistemi di IA nel contesto della sicurezza sul lavoro è ancora timido e agli esordi, così che, pur nella consapevolezza che l'approccio dianzi illustrato non sia scevro da criticità, si reputa utile l'impulso in tale direzione che con il presente scritto si auspica stimolare e approfondire.

In uno scenario tecnico-normativo che possiamo definire "fluido", la strada maestra da percorrere potrebbe essere quella di optare per un utilizzo degli Smart DPI quanto più consapevole possibile e sempre per ottenere il delicato bilanciamento tra gli interessi/obblighi in gioco: le esigenze/obblighi di sicurezza del Datore di Lavoro e la tutela dei dati personali e, dall'altro, dei diritti fondamentali dei lavoratori a essi sottesi.

De iure condendo, questa parrebbe essere una scelta tutelante, non solo nei confronti del prestatore d'opera, ma anche del Datore di Lavoro.