DSL

2-2022

Internet of Things al servizio della salute e della sicurezza dei lavoratori**

di Antonio Ambrosino*

SOMMARIO: 1. Caratteristiche, potenzialità e rischi della tecnologia in oggetto, in specie come strumento di tutela della salute e della sicurezza dei lavoratori. – 2. Intenet delle Cose ed adempimento dell'obbligo datoriale di sicurezza ai sensi dell'art. 2087 c.c. – 3. La compatibilità con la tutela della *privacy* dei dati dei prestatori di lavoro.

1. *Caratteristiche, potenzialità e rischi della tecnologia in oggetto, in specie come strumento di tutela della salute e della sicurezza dei lavoratori*

La massiccia diffusione delle nuove tecnologie negli ambiti più disparati della vita quotidiana ha imposto delle nuove riflessioni nel campo giuslavoristico, dovendosi necessariamente interrogare sulla natura e sulla funzione delle stesse nell'ambito del rapporto di lavoro[1]. Gli ultimi strumenti e le recenti applicazioni, da semplici elementi funzionali alla soluzione di problemi pratici ovvero all'ottimizzazione dei processi produttivi, hanno raggiunto un rilievo ordinamentale inedito: essi non hanno più una finalità ancillare al rapporto giuridico in cui vengono utilizzati, ma la loro operatività assurge ad elemento essenziale delle obbligazioni principali.

Ciò è sicuramente accaduto con lo sviluppo della tecnologia dell'*Internet of Things* (IoT ovvero Internet delle Cose), intendendo con tale locuzione l'insieme di connessioni internet operate da oggetti e da luoghi, senza l'intervento di operatori umani. In particolare, essa viene definita come «*un'infrastruttura globale per la società dell'informazione, che consente di disporre di servizi avanzati interconnettendo oggetti (fisici o virtuali) grazie alle tecnologie dell'informazione e della comunicazione (TIC) interoperabili*

* Antonio Ambrosino è assegnista di ricerca di Diritto del lavoro nell'Università di Modena e Reggio Emilia. *antonio.ambrosino@unimore.it*

** Il saggio è stato preventivamente assoggettato alla procedura di referaggio prevista dalle regole editoriali della Rivista.

[1] Si veda E. DAGNINO, *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Modena, ADAPT University Press, 2019, p. 71 ss., ove l'autore analizza l'incidenza della c.d. Quarta rivoluzione industriale sugli scenari produttivi e giuridici, in particolar modo nei nodi tematici fondamentali della materia giuslavoristica. Un'analoga disamina è effettuata da C. ROMEO, *Le nuove regole del lavoro tra algoritmi e incertezza delle tutele*, in "Il Lavoro nella giurisprudenza", 2021, n. 2, p. 129 ss.

esistenti o in evoluzione»[2]. In questo contesto gli oggetti possono collegarsi alla rete, comunicare il proprio *status* e i dati sul proprio utilizzo, come statistiche ed altro, ed accedere ad informazioni utili per il proprio funzionamento, in modo del tutto automatico[3].

Nello specifico, la IoT si riferisce all'interconnessione di oggetti all'infrastruttura internet attraverso dispositivi informatici incorporati, come *chip* di identificazione a radiofrequenza (*RFID*) e sensori vari. Tale connessione può avvenire, peraltro, tanto tra oggetto e oggetto (*Machine to Machine*), quanto tra essere umano e oggetto (*Machine to Human*) [4].

Le applicazioni nel campo dell'*Internet of Things* sono molteplici, spaziando dal settore della domotica a quello dei trasporti, della logistica e finanche della medicina.

L'Internet delle Cose, indubbiamente, potrebbe altresì giocare un ruolo fondamentale in tema di sicurezza sul lavoro, offrendo una tutela prevenzionistica rafforzata da strumenti di protezione c.d. *smart*: non semplici oggetti, ma "cose" capaci di processare dati ed informazioni del mondo fisico attraverso la digitalizzazione *on line* di essi.

Ciò anche in considerazione dei cambiamenti nello stile di vita imposti dalle note vicende pandemiche, tra cui l'implementazione di forme di lavoro da remoto, forieri di un ripensamento degli assetti e degli strumenti di prevenzione dei rischi precedentemente adottati[5]. Tale aggiornamento non poteva prescindere, in ossequio al principio della massima sicurezza tecnica, organizzativa e procedurale possibile[6], dal saggio delle nuove tecnologie poc'anzi citate.

---

[2] Tale definizione è stata elaborata dall'ITU, l'Agenzia specializzata delle Nazioni Unite per le tecnologie dell'informazione e della comunicazione, nel documento *Recommendation ITU-T Y.2060*, in https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=en, p. 2, nonché adoperata nei documenti istituzionali dell'Unione europea. Cfr. COMMISSIONE EUROPEA, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e di responsabilità*, COM (2020) 64 final, in https://ec.europa.eu/transparency/regdoc/rep/1/2020/IT/COM-2020-64-F1-IT-MAIN-PART-1.PDF, p. 2

[3] In tal senso si vedano F. SARZANA DI S. IPPOLITO, M. NICOTRA, *Diritto della blockchain, intelligenza artificiale e IoT*, Milano, Wolter Kluwer, 2018, p. 281; D. ACEMOGLU, P. RESTREPO, *Artificial intelligence, automation and work*, in "NBER Working paper", gennaio 2018; E. STRADELLA, *La regolazione della robotica e dell'intelligenza artificiale: il dibattito, le proposte, le prospettive. Alcuni spunti di riflessione*, in www.medialaws.eu, 2009, n. 1, p. 73 ss.

[4] Una portata qualificatoria hanno gli scritti di K. ASHTON, *That 'internet of things' thing*, in www.rfid journal.com, 2009; J. CRUMP, I. BROWN, *The societal impact of the internet of things*, in www.bcs.org, 14 febbraio 2013; E. BEVILACQUA, *Internet of Things e sicurezza, come risolvere eventuali problemi*, in www.zerounoweb.it, 5 maggio 2016.

[5] In tale senso G. NATULLO, R. NUNIN, *Introduzione. La tutela della salute e della sicurezza del lavoro alla luce delle sfide del prossimo futuro*, in "Rivista giuridica del lavoro e delle previdenza sociale", 2021, n. 2, I, p. 135.

[6] Linea interpretativa frutto di un orientamento incontrastato nella giurisprudenza, come confermato dalle recenti pronunce di legittimità: Cass. civ., sez. lav., 21 settembre 2021, n. 25597; Cass. civ., sez. lav., 16 dicembre 2019, n. 33133; Cass. civ., sez. lav., 11 dicembre 2019, n. 32382; Cass. civ., sez. lav., 8 ottobre 2018, n. 24741; Cass. civ., sez. lav., 16 maggio 2017, n. 12087, tutte consultabili nelle banca dati "De Jure". La succitata interpretazione è stata avallata anche dalla prevalente dottrina: E. DAGNINO (a cura di), *Il quadro normativo e istituzionale: una rassegna ragionata*

La IoT si articola, attualmente, su tre aree di sviluppo: la "tecnologia indossabile" (*Wearable Computing* ovvero *Wearable devices*), ossia informazioni ricavabili da vestiti, occhiali, orologi che contengono sensori interconnessi tra loro[7]; la "quantificazione del sé" (*Quantified Self*), ossia gestione di informazioni relative al proprio corpo come tracciati del sonno, battiti cardiaci, indicatori dell'attività fisica, delle calorie bruciate in riferimento all'attività svolta; la "domotica" (*Home Automation/Domotics*) ossia connessioni automatiche alla rete internet nelle abitazioni e negli uffici, che avvisano gli utenti di talune circostanze che si realizzano in quegli ambienti, come la rilevazione continuata e in remoto della presenza di individui o cose ed i loro movimenti.

Tutte le possibili aree di sviluppo potrebbero essere utilizzate per scongiurare gli infortuni e le malattie sul lavoro, ma una sicura vocazione prevenzionistica potrebbe essere assunta dalla c.d. tecnologia indossabile[8]. Una declinazione applicativa di tale tecnologia è rappresentata, come riferito, dalla *Radio Frequency ID Devices* (*RFID*), anche nota come "etichette intelligenti"; tale tecnologia è costituita da dispositivi microscopici simili a *microchip* contenenti un identificativo, che è possibile riconoscere attraverso un lettore compatibile e funzionante in radiofrequenza. I predetti dispositivi vengono per lo più utilizzati per l'identificazione e/o il tracciamento automatico degli oggetti mediante radiofrequenza. Ma le etichette intelligenti potrebbero anche fornire informazioni sulle persone e, nel caso di specie, sui lavoratori che le indossano[9].

Quanto sinora illustrato non costituisce una mera illazione teorica o delle ipotesi progettuali future, ma l'utilizzo operativo della tecnologia IoT ai fini prevenzionistici è già in corso, tant'è che l'EU-OSHA, l'agenzia d'informazione dell'Unione europea nel campo della sicurezza e della salute sul lavoro, nelle sue recenti relazioni di ricerca, si è occupata del tema, interrogandosi proprio sui vantaggi e le criticità della tecnologia di monitoraggio incorporata ed indossabile.

---

della letteratura internazionale, in AA.VV., *Il sistema prevenzionistico e le tutele assicurative alla prova della IV Rivoluzione Industriale*, Vol. III, Modena, ADAPT University Press, 2021, p. 246 ss.; G. NATULLO, *Principi generali della prevenzione e «confini» dell'obbligo di sicurezza*, in M. RUSCIANO, G. NATULLO (a cura di), *Ambiente e sicurezza del lavoro*, Torino, Utet giuridica, 2008, p. 77 ss.; L. MONTUSCHI, *La sicurezza nei luoghi di lavoro ovvero l'arte del possibile*, in "Lavoro e diritto", 1995, n. 3, p. 405 ss.: R. ROMEI, *Il campo di applicazione del d.lgs. n. 626/1994 e i soggetti*, in L. MONTUSCHI (a cura di), *Ambiente, salute e sicurezza. Per una gestione integrata dei rischi da lavoro*, Torino, Giappichelli, 1997, p. 64 ss.; R. GUARINIELLO, *Il principio della massima sicurezza tecnologicamente fattibile*, in "Igiene e sicurezza sul lavoro", 1997, p. 339.

[7] Una esemplificazione della tecnologia indossabile viene fornita da V. BRINO, *Wearable devices (voce)*, in S. BORRELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Torino, Giappichelli, 2022, p. 225.

[8] L'utilizzo di tali peculiari dispositivi in funzione prevenzionistica è stato contemplato da M. PERUZZI, *Nuove tecnologie e salute dei lavoratori*, in "Rivista giuridica del lavoro e delle previdenza sociale", 2021, n. 2, I, p. 179 ss.; A. ALLAMPRESE, O. BONARDI, *Studio sulle condizioni di lavoro nella logistica: tempo e salute*, in "Diritto della Sicurezza sul Lavoro", 2020, n. 2, I, p. 49; nonché, di recente, E. DAGNINO, *Diritto del lavoro e nuove tecnologie*, Torino, ADAPT University Press, 2022, p. 85 ss.

[9] È il caso del sistema *IBM Maximo Worker Insights*, che permette, appunto, tramite dispositivi indossati dai dipendenti, di rilevare il loro battito cardiaco ovvero la loro vicinanza ad un luogo pericoloso. In caso di anomalia, quindi, il sensore avvisa sia il dipendente che il responsabile della sicurezza, così da permettere un intervento tempestivo e, nei casi più estremi, salvifico.

Tecnologia indossabile adoperata proprio nell'ambito del rapporto di lavoro al fine di scongiurare possibili infortuni dei dipendenti. Si pensi, ad esempio, all'utilizzo di arnesi potenzialmente pericolosi per l'integrità fisica di chi li maneggia, come i coltelli adottati in macelleria, che vengono "potenziati" attraverso la tecnologia IoT e divengono capaci di localizzare la loro posizione e, eventualmente, segnalare all'utilizzatore la presenza dell'utensile in luogo fisico diverso dall'ordinaria postazione di lavoro al fine di evitare ferimenti involontari[10]; oppure, si pensi ancora, agli occhiali dotati di schermi e funzionalità di realtà virtuale da adoperare lungo le catene di montaggio[11] in grado di poter indurre i lavoratori a cambiare volontariamente i loro atteggiamenti o comportamenti, indirizzandoli verso percorsi e/o luoghi sicuri, attraverso la persuasione posta in essere con luci o altri impulsi[12].

L'utilizzo dei predetti dispositivi di protezione individuale intelligenti (*smart PPE personal protective equipment*), come evidenziato, costringe a rivedere gli attuali modelli organizzativi adottati[13] poiché l'innovazione tecnologica se, da un lato, è capace in astratto di potenziare il cordone di sicurezza intorno alla persona del lavoratore[14], dall'altro, è essa stessa foriera di altrettanti potenziali rischi psicosociali in capo al prestatore[15], come il rischio di ambiguità e carenza di informazioni sul ruolo, sulle responsabilità, sui compiti da eseguire[16], sino ad invadere la sfera di riservatezza personale del dipendente, di cui si dirà nel corso della trattazione.

---

[10] Cfr. *Tecnologia di monitoraggio: la ricerca del benessere nel XXI secolo?*, EU-OSHA Discussion Paper, luglio 2017, p. 7, consultabile su https://osha.europa.eu/it/publications.

[11] Si veda il documento di riflessione, *La SSL e il lavoro del futuro vantaggi e rischi degli strumenti di intelligenza artificiale nei luoghi di lavoro*, EU-OSHA, luglio 2019, p. 8, consultabile su https://osha.europa.eu/it/publications.

[12] Si rimanda ancora alla relazione *Tecnologia di monitoraggio: la ricerca del benessere nel XXI secolo?*, cit., p. 8 in cui si fa riferimento alla tecnologia di monitoraggio persuasiva.

[13] Le nuove possibilità quanto i nuovi rischi connessi all'introduzione di specifiche tecnologie in materia di salute e sicurezza dei lavoratori sono state compiutamente illustrate da: M. TIRABOSCHI, *Nuovi modelli della organizzazione del lavoro e nuovi rischi*, in "Diritto della Sicurezza sul Lavoro", 2022, n. 1, I, p. 145 ss. E. DAGNINO, *Le tecnologie per la tutela della salute e sicurezza dei lavoratori tra garanzie e vincoli*, in "Il Lavoro nella giurisprudenza", 2021, n. 6, p. 591 ss.; G. PIGLIALARMI, *5G e nuovi ambienti di lavoro: appunti per una ricerca giuslavoristica*, in "Diritto delle relazioni industriali", 2020, n. 4, p. 1055.

[14] Sulla ridotta pericolosità del lavoro garantita dall'evoluzione dei processi tecnologici F. CARNEVALE, *La salute e la sicurezza dei lavoratori in Italia. Continuità e trasformazioni dalla Prima Rivoluzione industriale a quella digitale*, in A. CIPRIANI, A. GRAMOLATI, G. MARI (a cura di), *Il lavoro 4.0. la quarta rivoluzione industriale e le trasformazioni delle attività lavorative*, Firenze University Press, 2018, p. 117 ss.

[15] Sui rischi psicosociali e Quarta rivoluzione industriale si rinvia a M. TIRABOSCHI (a cura di), *Bilancio e prospettive di una ricerca*, in AA.VV., *Il sistema prevenzionistico e le tutele assicurative alla prova della IV Rivoluzione Industriale*, Vol. I, Modena, ADAPT University Press, 2021, p. 230 ss., nonché a L.M. PELUSI (a cura di), *Le tutele assicurative: il caso italiano nel confronto comparato*, in AA.VV., *Il sistema prevenzionistico e le tutele assicurative alla prova della IV Rivoluzione Industriale*, Vol. IV, Modena, ADAPT University Press, 2021, p. 15 ss.

[16] Si veda ancora M. PERUZZI, *Nuove tecnologie e salute dei lavoratori*, cit., p. 181; nonché V. CANGEMI, *L'infortunio sul lavoro. Persona, tecnologia, tutele*, Modena, ADAPT University Press, 2020, p. 30, il quale afferma che l'interazione tra intelligenza artificiale, IoT e robotica permette di coniugare «*connettività, autonomia e dipendenza dai dati*», rendendo questi sistemi capaci di svolgere compiti in autonomia o con basso coinvolgimento di un operatore umano.

A tali rischi indiretti, infine, possono esserne aggiunti altri prettamente "fisici" legati all'utilizzo di tali nuove tecnologie. Si pensi alle patologie riguardanti l'apparato muscolo-scheletrico derivanti dai rischi ergonomici, all'esposizione alle onde elettromagnetiche emesse dai telefoni cellulari e da qualunque dispositivo dotato di connessione *wireless*[17], nonché al sovraccarico informativo e della mancanza di separazione tra vita privata e vita professionale[18].

Potenzialità e rischi connessi alle nuove tecnologie richiedono giocoforza una mappatura delle fonti di pericolo e di ricostruzione dei ruoli giuridici inedita poiché taluni dispositivi di sicurezza, stante la loro intrinseca capacità di processare informazioni e dati, potrebbero autonomamente inibire taluni comportamenti del lavoratore al fine di scongiurare situazioni pericolose rilevate, sostituendosi di fatto al datore di lavoro.

2. *Internet delle Cose ed adempimento dell'obbligo datoriale di sicurezza ai sensi dell'art. 2087 c.c.*

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. mediante l'utilizzo della tecnologia dell'*Internet of Things*: in pratica, va verificato se l'affidamento all'IoT possa concretamente garantire e salvaguardare l'integrità fisica e la personalità morale dei prestatori di lavoro. Una tale verifica circa l'idoneità dell'Internet delle Cose quale strumento di adempimento 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. Verificazione resasi ulteriormente necessaria in considerazione delle recenti 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[19]. Il succitato art. 20, tra le soluzioni tecnologiche da sperimentare, annovera segnatamente

---

[17] Cfr. M. TIRABOSCHI, *Esposizione a campi elettromagnetici prodotti da telefoni cellulari, malattia professionale a eziologia multifattoriale, tutele del lavoro* (nota a App. Torino, 13 gennaio 2020, n. 904 e altre), in "Diritto delle relazioni industriali", 2020, n. 2, p. 558 ss.

[18] In questo senso va ricordato un report dell'Inail del 2016, *ICT e lavoro: nuove prospettive di analisi per la salute e la sicurezza sul lavoro*, in www.inail.it.

[19] Tale facoltà è stata immediatamente esercitata dall'INAIL che ha, nell'aprile 2022, siglato con il Gruppo Ferrovie dello Stato l'accordo pilota destinato a fare da apripista per ulteriori collaborazioni con altri grandi gruppi industriali. Di tale circostanza e della funzione strategica dei protocolli di cui all'art. 20 del d.l. n. 36/2022 se ne da conto nella Relazione annuale del Presidente dell'INAIL, Franco Bettini, del 25 luglio 2022, reperibile su https://www.inail.it/cs/internet/docs/alg-relazione-annuale-anno-2021.pdf.

«*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*.

Ed invero, nel merito, la prospettiva di un adempimento "disumano" dell'obbligazione di sicurezza[20], grazie alle connessioni telematiche di cui all'*Internet of Things*, genererebbe, in prima battuta, delle forti criticità in relazione all'imputazione di responsabilità in caso di infortunio o nocumento alla persona del lavoratore.

Taluni dispositivi intelligenti potrebbero avocare a sé alcune valutazioni ed adottare delle misure che ordinariamente spetterebbero al datore di lavoro. È opportuno ovviamente effettuare una precisazione, distinguendo 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*. La differenza non è di poco conto, poiché, come ha avuto modo di affermare di recente anche la giurisprudenza amministrativa[21], 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[22]. Differentemente, 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[23].

In buona sostanza, 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. Un possibile argine alla deriva algoritmica del dovere di tutela della persona del lavoratore risiede 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

---

[20] Cfr. M. TIRABOSCHI, F. SEGHEZZI, *Il Piano nazionale Industria 4.0: una lettura lavoristica*, in "Labour & Law Issues", 2016, n. 2, p. 2, e F. SEGHEZZI, *La nuova grande trasformazione. Lavoro e persona nella quarta rivoluzione industriale*, Modena, ADAPT University Press, 2017, p. 1 ss.

[21] Cfr. Cons. Stato, sez. III, 25 novembre 2021, n. 7891 in "Foro Amministrativo", 2021, 11, p. 1721.

[22] Si veda L. ZAPPALÀ, *Algoritmo (voce)*, in S. BORRELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Torino, Giappichelli, 2022, p. 17 ss.

[23] La descrizione delle caratteristiche tra algoritmo tradizionale e quello evoluto artificialmente intelligente è analiticamente fornita da A. DONINI, A. INGRAO (a cura di), *Algoritmi e lavoro*, 25 maggio 2022, in https://www.labourlawcommunity.org/ricerca/algoritmi-e-lavoro/, nonché da L. ZAPPALÀ, *Intelligenza artificiale (voce)*, in S. BORRELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Giappichelli, 2022, p. 133 ss.

frutto delle elaborazioni dell'intelligenza artificiale[24]. Il rispetto del predetto principio 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. Ne consegue che, a seguito dell'utilizzo di dispositivi di sicurezza dotati di intelligenza artificiale e di capacità di autoapprendimento, il datore di lavoro sarà tenuto a valutare anche l'ulteriore rischio di concretizzazione di una *culpa in educando* della macchina[25], come anche i rischi da interferenza tra l'agire dei lavoratori e le iniziative prese in autonomia dai dispositivi algoritmici.

Il controllo umano, quale elemento essenziale di gestione delle nuove tecnologie di *machine learning*[26], è stato invocato anche dalle maggiori confederazioni sindacali e imprenditoriali europee nell'accordo quadro europeo sulla digitalizzazione[27]. Infatti, nel predetto 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*". La vera sfida lanciata agli attori pubblici e privati delle relazioni industriali non è 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 concepire una verifica istantanea dei meccanismi decisionali della macchina. 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*"[28].

---

[24] L'utilità e la garanzia del principio del c.d. *human in control principle* vengono riconosciute da: E. DAGNINO, *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, cit., p. 198 ss.; M. PERUZZI, *Nuove tecnologie e salute dei lavoratori*, cit., p. 185; nonché T. TREU, *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in "federalismi.it", 2022, n. 9, p. 205 ss.

[25] In tal senso L.M. PELUSI, *Nuove competenze per la prevenzione dei rischi nella IV rivoluzione industriale*, in "Working Paper ADAPT Salus", n. 1/2020, p. 10, in http://salus.adapt.it e V. MAIO, *Il diritto del lavoro e le nuove sfide della rivoluzione robotica*, in "Argomenti di diritto del lavoro", 2018, n. 6, p. 1433.

[26] Si rimanda per approfondimenti a L. ZAPPALÀ, *Machine learning (voce)*, in S. BORRELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Torino, Giappichelli, 2022, p. 147 ss.

[27] Nel giugno 2020, le parti sociali europee (Ces, BusinessEurope, SMEunited, CEEP) hanno sottoscritto un accordo quadro autonomo in tema di digitalizzazione. Tale accordo era previsto nel Programma di lavoro delle parti sociali europee relativo al triennio 2019-2021; tra i commenti si rinvia a M. PERUZZI, *Il dialogo sociale europeo di fronte alle sfide della digitalizzazione*, in "Diritto delle relazioni industriali", 2020, n. 4, p. 1213 ss.; A. ROTA, *Sull'Accordo quadro europeo in tema di digitalizzazione del lavoro*, in "Labour & Law Issues", 2020, vol. 6, n. 2, p. 23 ss.

[28] Sul meccanismo della delega di funzioni si rinvia a P. PASCUCCI, *Dopo la legge n. 123 del 2007. Titolo I del d.lgs. 9 aprile 2008, n. 81 in materia di tutela della salute e della sicurezza nei luoghi di lavoro*, in "WP C.S.D.L.E. "Massimo D'Antona".IT", n. 73/2008, p. 103 ss.; R. BRUNELLI, *La delega di funzioni e l'esercizio di fatto di poteri direttivi*, in L. ZOPPOLI, P. PASCUCCI, G. NATULLO (a cura di), *Le nuove regole per la salute e la sicurezza dei lavoratori. Commentario al D.Lgs. 9 aprile 2008 n. 81. Aggiornato al D.Lgs. 3 agosto 2009, n. 106*, Milano, Ipsoa, 2010, p. 215 ss.; A. RUSSO, *La delega di funzioni e gli obblighi del datore non delegabili*, in M. TIRABOSCHI (a cura di), *Il testo unico della salute e sicurezza nei luoghi di lavoro. Commentario al decreto legislativo 9 aprile 2008, n. 81*, Milano, Giuffrè, 2008, p. 219.

L'istituzione concettuale del rapporto di mandato tra delegante umano e delegato digitale 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[29].

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. Ed invero, basti 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.[30] Orbene, l'utilizzo di dispositivi di sicurezza intelligenti capaci di elaborare dati ed assumere decisioni al posto del datore in un'ottica prevenzionistica - come ad esempio inibire talune attività al lavoratore - sfumerebbe, sempre in astratto, 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. Tale circostanza, minando la capacità di incidenza dell'agire umano sulla macchina, renderebbe ancora più difficoltosa l'individuazione dei contorni dell'obbligazione di sicurezza del datore, nonché il titolo giuridico delle responsabilità a quest'ultimo ascrivibili. Infatti, 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. Diversamente, 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

---

[29] Sul tema P. AGHION, B.F. JONES, C.I. JONES, *Artificial Intelligence and Economic Growth*, in "NBER", ottobre 2017, p. 1 ss.; A. KORINEK, J.E. STIGLITZ, *Artificial Intelligence and its implications for income distribution and unemployment*, in "NBER", dicembre 2017, p. 1 ss.; C. TUCKER, *Privacy, Algorithms and Artificial Intelligence*, in "NBER", maggio 2019, p. 1 ss.

[30] Cfr. Cass. civ., sez. III, 21 settembre 2021, n. 25512, in "Il Lavoro nella giurisprudenza", 2022, n. 6, p. 604 con nota di G. PISTORE, *Delega di funzioni e responsabilità civile in materia prevenzionistica.*

atipica, andrebbero individuati dei nuovi profili di responsabilità non necessariamente rispondenti ai canoni degli artt. 1228 e 2049 c.c.[31]

In sintesi, l'impiego attuale (e la diffusione futura) della tecnologia dell'*Internet of Things* in materia di sicurezza, stante il carattere evoluto ed evolvente dei dispositivi intelligenti, 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 - *docendi causa* - della delega, nonostante le precauzioni iniziali che il datore metterebbe in campo prima del suo utilizzo, potrebbe risultare inidoneo a contenere la macchina "pensante".

L'unico vero argine, a prescindere dalla veste giuridica che viene attribuita al *machine learning*, è la capacità di monitoraggio ed intervento da parte del datore, intervento umano assoluto e radicale sul dispositivo, idoneo ad interrompere *ad nutum* l'azione digitale. Così ragionando, qualsiasi operazione di surrogazione che avvenga tra datore di lavoro e macchina dovrà essere caratterizzata da una reversibilità unidirezionale verso il soggetto datoriale, limitando fortemente l'autonomia "meccanica" di esecuzione delle attività previamente trasferite ed esercitate in sostituzione.

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[32], 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.

Il 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

---

[31] L'inadeguatezza degli ordinari criteri di imputazione delle responsabilità *ex* art. 2049 c.c. in un contesto di forte digitalizzazione, di de-piramidalizzazione delle strutture, di allentamento dei confini spazio-temporali dell'adempimento, ma anche di maggiore tecnicismo del contenuto della prestazione viene illustrata da E. GUARDIGLI, *La responsabilità vicaria: una rilettura alla luce dei modelli di lavoro della rivoluzione digitale*, in "Lavoro Diritti Europa", 2022, n. 1, p. 12 ss., ove l'autrice ritiene che la responsabilità vicaria non può essere comunque sganciata dalla prevedibilità del rischio *ex ante* da parte del preponente.

[32] Cfr. G. PISTORE, *Delega di funzioni e responsabilità civile in materia prevenzionistica*, cit., p. 607, nonché P. PASCUCCI, *Salute e sicurezza sul lavoro, responsabilità degli enti, modelli organizzativi e gestionali*, in "Rivista giuridica del lavoro e delle previdenza sociale", 2021, n. 4, I, p. 537 ss., ove l'autore evidenzia il ruolo dei modelli organizzativi anche sotto il profilo partecipativo del sistema di prevenzione aziendale di cui al d.lgs. n. 81/2008.

finalizzati alla tutela dell'"*integrità fisica*" e della "*personalità morale*" dei prestatori di lavoro *ex* art. 2087 c.c.[33] Proprio tale carattere intrinseco dei modelli di gestione dei rischi garantisce (ed impone) al datore di governare, sul piano organizzativo, ogni risvolto tecnologico.

La predetta soluzione - che contempla la possibilità di vigilare sullo "operato" del dispositivo intelligente unitamente alla capacità di intervenire istantaneamente - sembra essere stata accolta dalla recente Proposta 2021/0106 (COD) di Regolamento del Parlamento Europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione[34]. D'altronde, già il Parlamento europeo aveva stilato delle linee-guida per l'uso dell'intelligenza artificiale in campo militare e civile, in cui si sottolineava l'espressa necessità di un controllo umano sui sistemi di intelligenza artificiale[35].

Se tale soluzione ricevesse dignità normativa consentirebbe di non rinunciare alle potenzialità dei nuovi dispositivi di protezione, anche improntati sulla tecnologia dell'*Internet of Things*, superando le criticità esposte e relative all'individuazioni dei ruoli, delle responsabilità ed al contenimento dei rischi derivanti dagli automatismi algoritmici.

3. *La compatibilità con la tutela della* privacy *dei dati dei prestatori di lavoro*

Le innovazioni tecnologiche applicate al rapporto del lavoro, seppur ricche di potenzialità e soprattutto di efficientamento di entrambe le prestazioni del sinallagma contrattuale, potrebbero alterare gli ordinari meccanismi di esercizio dei rispettivi diritti del lavoratore e le prerogative del datore.

---

[33] In tal senso G. ZAMPINI, *Sicurezza sul lavoro e modello organizzativo: quali responsabilità per il datore di lavoro?*, in "Il Lavoro nella giurisprudenza", 2018, n. 2, p. 123.

[34] Tale documento del 21 aprile 2021 è reperibile su https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52021PC0206&from=IT. Tra i primi commenti alla proposta di Regolamento si segnalano: F. COSTANTINI, *Intelligenza artificiale, design tecnologico e futuro del lavoro nella UE: i presupposti ed il contesto*, in "Il Lavoro nella giurisprudenza", 2021, nn. 9-10, p. 807 ss.; F. COSTANTINI, *Intelligenza artificiale, design tecnologico e futuro del lavoro nella UE: il caso dei platform workers*, in "Il Lavoro nella giurisprudenza", 2021, n. 12, p. 1124 ss.; A. ALOISI, V. DE STEFANO, *La Commissione europea ha pubblicato la proposta di Regolamento Ue sull'«Approccio europeo all'Intelligenza artificiale»: a un primo esame, la proposta è del tutto insufficiente ad assicurare una protezione ai lavoratori*, in www.rivistailmulino.it, 4 maggio 2021.

[35] Cfr. Risoluzione del Parlamento europeo del 20 gennaio 2021 sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI)), consultabile su https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52021IP0009&from=EN, ove viene affermato che «*l'IA utilizzata in un contesto militare e civile debba essere soggetta ad un significativo controllo umano, in modo tale che in qualsiasi momento un umano abbia i mezzi per correggerla, bloccarla o disattivarla in caso di comportamento imprevisto, intervento accidentale, attacchi informatici o interferenza di terzi con tecnologie basate sull'IA o qualora terzi acquisiscano tale tecnologia*».

Talune criticità interpretative, connesse alla smaterializzazione delle prestazioni contrattuali, già sono state evidenziate nel corso della disamina delle singole tecnologie descritte.

La loro trazione digitale sposta sensibilmente l'attenzione dell'interprete che, anziché ragionare su questioni aventi ricadute sul piano materiale, si trova a disputare su dati ed *asset* intangibili.

Tale vocazione computazionale delle nuove tecnologie, tra cui ovviamente l'*Internet of Things*, contribuisce ad accrescere la loro operatività, al punto tale da rafforzare i meccanismi decisionali della "macchina" in uso nel rapporto di lavoro. La tecnologia, così, da mero strumento al servizio di un decisore umano, all'esito dell'acquisizione di un vasto flusso di dati, inizia ad impattare sui lavoratori e sui modelli organizzativi in tutte le fasi nevralgiche del rapporto, concependo essa stessa decisioni di spettanza imprenditoriale. Tale peculiare caratteristica delle nuove tecnologie aziendali, fondata sull'elaborazione massiva di dati, viene qualificata come *workforce* o *people analytics* o, ancora, di *HR analytics*[36]. Fornire il *management* aziendale di tale ulteriore metodo decisionale significa assumere determinazioni relative alla persona dei lavoratori sulla base di modelli statistici stilati con i dati personali dei lavoratori stessi: una sorta di *loop*, un circolo in cui l'azienda incamera mediante *software* i dati dei lavoratori, che vengono elaborati, sempre automaticamente, per concepire scelte di gestione del personale. Più è accurato il meccanismo di analisi dei dati più è marginale il ruolo del datore, in buona sostanza maggiore è l'utilizzo del dispositivo tecnologico minore sarà il margine decisionale dell'utilizzatore.

Le decisioni "suggerite" (e, talvolta o per lo più, "assunte" direttamente) dallo strumento tecnologico possono ovviamente riguardate la salute e la sicurezza dei lavoratori[37], ove la tecnologia per preservare la salute del dipendente si "alimenta" dei dati di quest'ultimi, in altre ipotesi, il dispositivo tecnologico potrebbe attingere direttamente ai dati del processo produttivo senza riferibilità a persone fisiche identificate o identificabili, ma, anche in tali occasioni, vanno

---

[36] Sul tema si vedano: E. DAGNINO, *People Analytics: lavoro e tutele al tempo del management tramite big data*, in "Labour & Law Issues", 2017, vol. 3, n. 1, p. 7 ss.; E. DAGNINO, *Big data e lavoro: le sfide della workforce analytics*, in E. DAGNINO, F. NESPOLI, F. SEGHEZZI (a cura di), *La nuova grande trasformazione del lavoro. Lavoro futuro: analisi e proposte dei ricercatori Adapt*, Modena, ADAPT University Press, 2017, p. 135 ss.; F. COSTANTINI, *Profilazione e "automated decision making" in ambito lavorativo nella giurisprudenza italiana*, in "Il Lavoro nella giurisprudenza", 2019, n. 11, p. 986 ss.; L. CASANO, F. SEGHEZZI (a cura di), *Le trasformazioni del lavoro: un percorso di lettura*, in AA. VV., *Il sistema prevenzionistico e le tutele assicurative alla prova della IV Rivoluzione Industriale*, Vol. II, Modena, ADAPT University Press, 2021, p. 16.

[37] Un tale utilizzo del principio del *people analytics* viene riferito da A. ROTA, *Rapporto di lavoro e big data analytcs: profili critici e risposte possibili*, in "Labour & Law Issues", 2017, vol. 3, n. 1, p. 35, che ha evidenziato come il patrimonio di dati messo a disposizione dalle tecniche di analisi avanzata è stato valorizzato anche dall'Inail nelle indagini sulla correlazione fra infortuni/malattie professionali e contesto locale, comportamenti aziendali, generatori di stress, stile di vita del lavoro ed azioni di prevenzione. Ad analoga conclusione si giunge in M. TIRABOSCHI (a cura di), *Bilancio e prospettive di una ricerca*, cit., pp. 237-238.

preservate comunque le possibili distorsioni che possono incidere sulla salute e sicurezza delle persone o avere un impatto negativo sui diritti fondamentali[38].

Appuntando l'interesse sui profili esclusivi di *data protection*, appare evidente, ad ogni modo, che anche l'utilizzo di tali nuove tecnologie nell'ambito del rapporto di lavoro non può trascurare la verifica del pieno rispetto delle tutele in materia di *privacy* e dati personali dei prestatori, che, ancor prima delle loro energie fisiche e materiali, assumono rilievo preponderante nella gestione dei rapporti giuridici tecnologicamente innovati[39].

Ed è altrettanto evidente che ogni nuova tecnologia, avendo proprie caratteristiche e peculiari ambiti di utilizzo, avrà differenti problematiche interpretative da dipanare in materia di *privacy*, che richiederanno un'attenta verifica della conformità e praticabilità dei singoli risvolti applicativi in relazione all'attuale sistema di protezione concepito dal Reg. (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 ("Regolamento generale sulla protezione dei dati") [40].

Le preoccupazioni in tema di trattamento dei dati personali involgono ovviamente anche le ipotesi di utilizzo della tecnologia dell'*Internet of Things* nell'ambito del rapporto di lavoro[41]. Il tema già era stato affrontato dalla Commissione europea, la quale, con la Raccomandazione del 12 maggio 2009 «*sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza*», oltre a fornire degli orientamenti sulla progettazione e l'uso delle applicazioni *RFID* (tipologia di dispositivo di IoT) in modo giuridicamente, eticamente, socialmente e politicamente accettabile nel rispetto del diritto alla vita privata e garantendo la

---

[38] Le esigenze di tutela e sicurezza delle persone hanno assunto rilievo anche nelle ipotesi di utilizzo dei dati per l'addestramento dei modelli sui cui si basano i sistemi di IA, come testimoniato dagli emendamenti proposti alla proposta di Regolamento europeo sull'intelligenza artificiale consultabili su https://www.europarl.europa.eu/doceo/document/ITRE-AD-719801_IT.pdf.

[39] Le preoccupazioni in tema di *privacy* connesse all'utilizzo delle nuove tecnologie sono compiutamente illustrate da R. SANTUCCI, *La quarta rivoluzione industriale e il controllo a distanza dei lavoratori*, in "Il Lavoro nella giurisprudenza", 2021, n. 1, p. 19 ss.

[40] Sul Reg. (UE) n. 2016/679 si segnalano i seguenti commenti di F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, p. 1 ss.; C. OGRISEG, *Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in "Labour & Law Issues", 2016, n. 2, p. 29 ss.; G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, p. 21; G. FINOCCHIARO, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in "Le nuove leggi civili commentate", 2017, n. 1, p. 2 ss.; C. DEL FEDERICO, *Trattamento dei dati nell'ambito dei rapporti di lavoro*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, p. 629 ed ancora C. DEL FEDERICO, *Il trattamento dei dati personali dei lavoratori e il Regolamento 2016/679/UE. Implicazioni e prospettive*, in P. TULLINI (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, Giappichelli, 2017, p. 61; F. COSTANTINI, *Il Regolamento (UE) 679/2016 sulla protezione dei dati personali*, in "Il Lavoro nella giurisprudenza", 2018, n. 6, p. 545.

[41] I principali profili problematici sono stati evidenziati da A. SITZIA, B. LOPEZ, *Le più avanzate modalità di controllo sul lavoratore: machine learning e social media*, in C. PISANI, G. PROIA, A. TOPO (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022, p. 385 ss.

protezione dei dati personali, suggeriva ai gestori di *RFID* di eseguire «*valutazioni dell'impatto sulla protezione della vita privata e dei dati*» prima dell'utilizzo effettivo del dispositivo e di sottoporre la valutazione a disposizione dell'Autorità competenti[42].

Nella scia interpretativa della predetta Raccomandazione, si inserivano i pareri offerti dall'allora "Gruppo di lavoro sulla protezione dei dati", spesso indicato come "Gruppo di lavoro Articolo 29" in onore della norma della Direttiva 95/46/CE del 24 ottobre 1995 che lo istituiva[43].

Il Gruppo di lavoro analizzava le problematiche relative all'IoT in diversi documenti, fornendo una serie di raccomandazioni agli operatori del settore con l'intento di realizzare una regolamentazione uniforme, con l'identificazione dei ruoli e delle responsabilità dei soggetti che adoperano tale tecnologia[44]. Il Gruppo esaminava, così, i principali timori per la *privacy* connessi alla possibilità dei dispositivi di IoT di essere associati ai dati personali del soggetto utilizzatore, che - come visto - potrebbe essere un lavoratore dipendente nell'ipotesi in cui lo strumento venga adoperato per motivi di salute e sicurezza. Le informazioni personali raccolte dall'*Internet of Things* dovrebbero essere cancellate o rese anonime ovvero bisognerebbe garantire un consenso informato. Se ciò non accadesse i rischi sarebbero tra i più vari, come la profilazione del prestatore, sino al furto di identità.

L'attenzione verso le tecnologie IoT non si è avuta solo al livello europeo, ma anche nel nostro ordinamento, in cui si sono registrati, forse anche anticipando taluni approdi interpretativi sovranazionali, degli interventi da parte dell'autorità competente. Ed invero, il Garante per la protezione dei dati personali adottava, in data 9 marzo 2005, un Provvedimento dedicato all'analisi della tecnologia *RFID*, accentuando gli aspetti di allarme[45].

In tale documento, oltre a ribadire che l'uso di tecniche *RFID* doveva in particolare rispettare il divieto di controllo a distanza del lavoratore (art. 4 della legge 20 maggio 1970, n. 300), il Garante, con riferimento ai sistemi a radiofrequenza destinati all'impianto sottocutaneo attraverso etichette intelligenti, predicava che il loro uso avvenisse solo in casi eccezionali e per comprovate e giustificate esigenze di tutela della salute ed in stretta adesione con il principio di proporzionalità.

---

[42] Documento reperibile su https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:IT:PDF.

[43] Tale organismo era composto dai rappresentanti delle autorità competenti per la protezione dei dati nei diversi Stati membri. In data 25 maggio 2018, il Gruppo di lavoro Articolo 29 ha cessato di esistere ed è stato sostituito dall'attuale Comitato europeo per la protezione dei dati (*EDPB*).

[44] Cfr. il parere n. 104/2005 del 19 gennaio 2005, il parere n. 5/2010 del 13 luglio 2010, il parere 9/2011 dell'11 febbraio 2011 e il parere n. 8/2014 del 16 settembre 2014, tutti consultabili su https://ec.europa.eu.

[45] Provvedimento generale [doc. web n. 1109493] del 9 marzo 2005, «*'Etichette intelligenti' (Rfid): il Garante individua le garanzie per il loro uso*», su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1109493.

Tali modalità di utilizzo venivano, poi, confermate sempre dal Garante della *privacy* con riferimento questa volta ai bracciali muniti di sensori che consentivano la rilevazione a distanza delle condizioni cliniche dei soggetti che li indossavano[46].

L'Autorità garante permetteva l'utilizzo di tale tecnologia a condizione che fossero rispettate in maniera precisa le condizioni previste dal Codice della *privacy* (decreto legislativo 30 giugno 2003, n. 196, oggi riformulato dal decreto legislativo 10 agosto 2018, n. 101 di adeguamento della normativa italiana al Regolamento europeo sulla *privacy*), quali il necessario consenso in forma scritta da parte del soggetto utilizzatore e la localizzazione effettuata non in modo sistematico.

Le indicazioni sinora illustrate risultano utili anche alla luce del Regolamento europeo, segnatamente per quanto attiene alla valutazione preventiva di impatto del trattamento sulla protezione dei dati personali che il titolare deve svolgere, ai sensi dell'art. 35 del Reg. (UE) n. 2016/679, quando un tipo di trattamento, allorché preveda l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La valutazione di cui all'art. 35 del Reg. (UE) n. 2016/679 non è, come noto, un mero adempimento formale, ma, al contrario, obbliga i titolari del trattamento a svolgere un'approfondita stima dell'impatto prima di darvi inizio, consultando l'autorità di controllo nel caso in cui le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato. Il Regolamento europeo contempla proprio l'utilizzo delle nuove tecnologie come occasione per procedere alla predetta valutazione ed i trattamenti di dati mediante la tecnologia *Internet of Things*, proprio per la sua specialità ed il carattere di novità, sono stati indicati tra le tipologie di trattamenti soggetti al requisito di una valutazione di impatto sulla protezione dei dati da parte del Gruppo di lavoro Articolo 29 nelle linee-guida adottate sul tema, con l'intento dichiarato di preservare l'interessato nelle seguenti ipotesi di rischio: valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*"; processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; monitoraggio sistematico; trattamento di dati sensibili o dati aventi carattere altamente personale; trattamento di dati su larga scala; creazione di corrispondenze o combinazione di insiemi di dati; trattamento di dati relativi a interessati vulnerabili; uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; quando il trattamento in sé "*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*"[47].

---

[46] Provvedimento n. 29 [doc. web n. 7810766] del 25 gennaio 2018, «*Verifica preliminare. Raccolta di dati attraverso il monitoraggio a distanza di pazienti non autosufficienti*», su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/7810766.

[47] Si vedano le Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del

Le istruzioni fornite dall'allora Gruppo di lavoro Articolo 29 sono state raccolte anche dal Garante della *privacy*, che ha, in pratica, aggiornato le proprie coordinate interpretative sul tema, fondate, nei precedenti provvedimenti emessi, sia su riferimenti normativi pregressi e parzialmente modificati sia sui primissimi dispositivi di tecnologia indossabile (*Wearable Computing*)[48]. Il Garante per la protezione dei dati personali, infatti, ha prontamente inserito, sulla scorta delle linee-guida del Gruppo di lavoro Articolo 29, tra i trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Reg. (UE) n. 2016/679, quelli «*effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking)*[49]».

Di recente, l'*Internet of Things* ha fortemente innovato e sviluppato gli originari dispositivi esaminati dal Garante, i quali stanno lentamente acquisendo sempre di più una marcata capacità di elaborazione dei dati e di adozione di decisioni automatiche, sostituendosi talvolta, nell'ambito del rapporto di lavoro, al datore. La predetta sostituzione, preliminarmente, genera commistioni difficili da risolvere sul piano della gestione del rapporto di lavoro e, secondariamente, potrebbe porre in crisi le attuali prescrizioni in materia di *privacy*, che necessitano, quindi, di una verifica della loro idoneità e validità.

Così come attualmente strutturata, la tecnologia IoT appare pienamente conforme alle attuali disposizioni dell'art. 4 della legge n. 300/1970, novellate dall'art. 23 del decreto legislativo 14 settembre 2015, n. 151[50], come, d'altronde,

---

regolamento 2016/679 - WP248rev.01, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017 e consultabili su https://ec.europa.eu/newsroom/article29/items/611236/en.

[48] Sul dibattito scaturito dall'utilizzo del braccialetto Amazon si vedano E. DAGNINO, *Il braccialetto di Amazon, facciamo chiarezza*, in @bollettinoADAPT del 5 febbraio 2018, n. 5; R. DI MEO, *Tecnologie e poteri datoriali: commento a margine del cd. braccialetto Amazon*, in "Labour & Law Issues", 2018, vol. 4, n. 1, p. 1 ss.; A. INGRAO, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in "Diritto delle relazioni industriali", 2019, n. 3, p. 895 ss.

[49] Cfr. l'Allegato 1 del Provvedimento n. 467 [doc. web n. 9058979] dell'11 ottobre 2018, «*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*», su https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9059358.

[50] Sulla nuova versione della norma si rimanda ai contributi dottrinali di A. SARTORI, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Torino, Giappichelli, 2020, p. 1 ss.; A. INGRAO, *Il controllo a distanza dei lavoratori e la nuova disciplina privacy. Una lettura integrata*, Bari, Cacucci, 2018, p. 1 ss.; O. DESSÌ, *Il controllo a distanza sui lavoratori. Il nuovo art. 4 Stat. lav.*, Napoli, Edizioni Scientifiche Italiane, 2017, p. 1 ss.; M.T. SALIMBENI, *Commento all'art. 4 St. lav.*, in R. DE LUCA TAMAJO, O. MAZZOTTA (a cura di), *Commentario breve alle leggi sul lavoro*, Padova, Cedam, 2017, p. 819 ss.; A. SITIZIA, *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in "Argomenti di diritto del lavoro", 2017, n. 3, p. 829 ss.; I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in "Labour & Law Issues", 2016, n. 1, p. 1 ss.; E. BALLETTI, *I poteri del datore di lavoro tra legge e contratto*, in AA.VV., *Legge contrattazione collettiva nel diritto del lavoro post-statutario*, Milano,Giuffrè, 2016, p. 67 ss.; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 d.lgs. n. 151/2016)*, in "Rivista italiana di diritto del lavoro", 2016, n. 1, I, p. 77 ss.; C. GAMBA, *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, in "Labour & Law Issues", 2016, n. 1, p. 122 ss.; A. LEVI, *La ridefinizione dell'assetto regolativo dei controlli a distanza, quale*

sarebbe stata altrettanto compatibile con le previgenti prescrizioni della medesima norma statutaria. Ed invero, l'inserimento, tra le esigenze che consentono l'installazione di strumenti dai quali possa derivare anche indirettamente un controllo a distanza dell'attività lavorativa, della sicurezza del lavoro sembrerebbe dare piena legittimità ai controlli effettuati mediante l'*Internet of Things*, sottoponendoli alle prescrizioni dell'art. 4 St. lav. nella sua nuova formulazione: l'accordo sindacale o, in mancanza, l'autorizzazione amministrativa e le informazioni ai lavoratori[51].

È evidente che annoverare tra i filtri giustificativi di cui al comma 1 dell'art. 4 St. lav. la sicurezza del lavoro conferirebbe pienezza legislativa alla categoria dei controlli effettuati mediante IoT, ma comunque irrigidirebbe la loro predisposizione da parte del datore, il quale, per non incorrere in possibili 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'Ispettorato nazionale del lavoro, per poter adoperare gli strumenti di controllo di cui al comma 1 della norma statutaria. Fermo restando il rispetto della procedura anzidetta, i dati raccolti mediante l'utilizzo di dispositivi di sicurezza intelligenti, basati sulla tecnologia dell'Intenet delle Cose, devono essere preceduti, ai fini della loro utilizzabilità nell'ambito del rapporto di lavoro, da un'adeguata informativa e dal pieno rispetto del Codice delle *privacy*[52], nonché ovviamente del Reg. (UE) n. 2016/679.

Questo forse potrebbe essere il vero punto di caduta della tecnologia IoT in tema di controllo a distanza poiché se il controllo potrebbe essere legittimo, previo rispetto delle formalità richieste, ai sensi sia del comma 1 che del comma 3,

---

tassello di una più complessiva riforma del diritto del lavoro, in A. LEVI (a cura), *Il nuovo art. 4 sui controlli a distanza. Lo Statuto dei Lavoratori dopo il Jobs Act*, Milano, Giuffrè, 2016, p. 1 ss.; M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza)e del trattamento dei dati (del lavoratore)*, in "WP C.S.D.L.E. "Massimo D'Antona".IT", n. 300/2016, p. 14 ss.; A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in "Rivista italiana di diritto del lavoro", 2016, n. 1, I, p. 513; A. TROJSI, *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in "Variazioni su Temi di Diritto del lavoro", 2016, n. 4, p. 667 ss.; A. TROJSI, *Controllo a distanza e protezione dei dati del lavoratore: legge, contratto collettivo e codice di deontologia*, in AA.VV., *Legge contrattazione collettiva nel diritto del lavoro post-statutario*, Milano Giuffrè, 2016, p. 385 ss.; E. VILLA, *Accordo sindacale e procedura amministrativa nei controlli a distanza dei lavoratori*, in "Variazioni su Temi di Diritto del lavoro", 2016, n. 4, p. 707 ss.; C. ZOLI, *Il controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970*, in "Variazioni su Temi di Diritto del lavoro", 2016, n. 4, p. 636 ss.; E. DAGNINO, *Tecnologia e controlli a distanza*, in "Diritto delle relazioni industriali", 2015, n. 4, p. 988 ss.; V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in "Argomenti di diritto del lavoro", 2015, n. 6, p. 1186 ss.

[51] Sull'applicazione delle nuove prescrizioni dell'art. 4 Statuto dei lavoratori alla tecnologia *RFID* (*Radio Frequency ID Devices*), seppur adoperata non in funzione prevenzionistica, ma come strumento di controllo a distanza, si rinvia a A. TROJSI, A. MELLACE, *Badge e Gps: strumenti di controllo (e probatori), prima e dopo il Jobs Act* (nota a Cass. civ., sez. lav., 5 ottobre 2016, n. 19922, nonché a Cass. civ., sez. lav., 13 maggio, 2016, n. 9904), in "Rivista giuridica del lavoro e delle previdenza sociale", 2017, n. 1, II, p. 34 ss.

[52] Informativa ritenuta superflua da Cass. civ., sez. II, 26 gennaio 2016, n. 1422, in "De Jure", quando il meccanismo di rilevazione dei dati, che utilizza la tecnologia delle etichette intelligenti *RFID*, sia azionabile ad iniziativa dell'utilizzatore.

l'utilizzazione delle informazioni potrebbe risultare problematica poiché esse non sono "gestite" unicamente dal datore di lavoro, ma sono elaborate dallo stesso dispositivo e giungono al datore solo in via mediata. La mediazione algoritmica rappresenta, quindi, una possibile disfunzione in relazione alle tutele statutarie, ma, in verità, tutte le nuove applicazioni basate sulla tecnologia IoT posseggono, o per un verso o per un altro, delle peculiarità tecniche che rendono gravoso il lavoro dell'interprete in materia di protezione dei dati personali, anche e, soprattutto, in relazione all'applicazione del Regolamento europeo n. 2016/679.

Una siffatta difficoltà, però, non significa che esse non siano conformi alle prescrizioni del Regolamento sulla *privacy* in quanto lo stesso contiene una sorta di clausola di salvezza: il principio di *privacy by design* o anche di *security by design*[53].

Il predetto principio, contenuto all'art. 25 del Reg. (UE) n. 2016/679, può essere sintetizzato nella necessità che i trattamenti, sia nel momento della progettazione dei sistemi sia in occasione del loro uso, vengano effettuati nel rispetto delle previsioni e dei principi del Regolamento e, in particolare, seguendo possibilmente il metodo della pseudonimizzazione e minimizzazione dei dati personali[54]. I mezzi e le misure tecnico-organizzative adoperate dal titolare devono però – sempre secondo i dettami dell'art. 25 – confrontarsi con lo stato dell'arte ed i costi di attuazione, nonché con la natura dell'ambito di applicazione e del contesto, con le finalità del trattamento, come anche con i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Le tecnologie descritte avrebbero anche la possibilità, in alcune circostanze, di agevolare la pseudonimizzazione dei dati raccolti e di minimizzare il trattamento, però vi sono comunque molte operazioni assolutamente al di fuori della sfera di controllo del titolare del trattamento, rimesse esclusivamente a processi algoritmici capaci di minare le tutele predisposte dal Regolamento europeo sulla *privacy*. Infatti, se, da un lato, i dispositivi IoT potrebbero essi stessi mascherare e cifrare i dati personali trattati in modo da non risalire all'identità della persona dell'utilizzatore, dall'altro, stante gli automatismi meccanici che li governano, potrebbero effettuare operazioni sui dati non autorizzate o illecite e, soprattutto, non sempre imputabili al titolare del trattamento, in netto contrasto con i fondamentali principi dell'art. 5 del Reg. (UE) n. 2016/679, tra cui, ovviamente, quelli dell'integrità e riservatezza, nonché della responsabilizzazione del titolare. Alla luce di tali considerazioni, è possibile affermare che il trattamento dei dati mediante le nuove tecnologie illustrate possa difficilmente

---

[53] Cfr. F. LORÈ, *Blockchain e privacy, un rapporto ancora da definire*, in "Dirittifondamentali.it", 2020, n. 3, p. 63.

[54] Una compiuta descrizione del principio viene compiuta da V. BRINO, *Privacy by design (voce)*, in S. BORRELLI, V. BRINO, C. FALERI, L. LAZZERONI, L. TEBANO, L. ZAPPALÀ, *Lavoro e tecnologie. Dizionario del diritto del lavoro che cambia*, Torino, Giappichelli, 2022, p. 173 ss. ove l'autrice, in relazione al predetto principio, ritine che esso sottende inoltre, un monitoraggio costante sui tipi di rischi i quali, tenuto conto dell'evoluzione della tecnologia, sono suscettibili di modificarsi e differenziarsi nel corso del tempo.

conformarsi alle previsioni e rispondere alle esigenze di tutela del Reg. (UE) n. 2016/679.

La tassonomia dei divieti e dei gradi di rischiosità dei nuovi sistemi digitali in tema di protezione dei dati personali, anche alla luce della proposta di Regolamento europeo sull'intelligenza artificiale, ha spinto quindi il Garante della *privacy* a fornire delle prospettive di intervento nella recente Memoria presentata in data 9 marzo 2022 alle Commissioni IX e X riunite della Camera dei Deputati[55].

L'Autorità ha, preliminarmente, sottolineato l'interrelazione sussistente tra i sistemi di intelligenza artificiale e la protezione dei dati personali, tant'è che ha considerato entrambe le materie «*trasversali, certamente, ma accomunate dal rappresentare la sfida, attuale e futura, lanciata dalla tecnica al diritto e alla sua possibilità di regolamentare anche ciò che appare, nella sua evoluzione incessante, più refrattario alla norma*». La connessione tra algoritmi evoluti e trattamento dei dati è così profonda che il Garante ha evidenziato che i primi sono alimentati dal secondo.

Infatti, errori, imprecisioni o irregolarità nel trattamento dei dati, funzionali all'alimentazione della macchina (sia in fase iniziale sia in fase esecutiva), si riflettono in altrettante distorsioni del processo algoritmico.

Nel merito, il Garante per la protezione dei dati personali, attingendo a diversi risultati interpretativi forniti dal parere congiunto n. 5/2021 del Garante europeo della protezione dei dati (*EDPS*) e del Comitato europeo per la protezione dei dati (*EDPB*)[56], oltre a ribadire la centralità della normativa europea in materia di *privacy* e, in particolare, i principi di minimizzazione e *privacy by design* ai fini dell'immissione nel mercato dei nuovi sistemi tecnologici, ha espressamente suggerito di vietare qualsiasi sistema di intelligenza artificiale funzionale all'attribuzione di punteggi sociali, in qualsiasi ambito utilizzati, o alla deduzione delle emozioni, nonché quelli volti a categorizzare le persone in insiemi, sulla base di dati biometrici, dell'etnia, del genere, dell'orientamento politico o sessuale ovvero in base ad altri motivi di discriminazione di cui all'articolo 21 della Carta dei diritti fondamentali dell'Unione europea.

Il monito espresso dal Garante delle *privacy*, in uno scenario tecnico-normativo "liquido", ove, ad eccezione del Reg. (UE) n. 2016/679, non si registrano delle prescrizioni formali capaci di frenare l'ascesa algoritmica dei nuovi sistemi tecnologici utilizzati dal datore, appare di estremo conforto per il futuro, non solo per la tutela della persona del prestatore, ma anche per la conservazione delle prerogative del datore.

---

[55] Memoria del Garante per la protezione dei dati personali - COM 2021(206) Proposta di regolamento (UE) sull'intelligenza artificiale del 9 marzo 2022, su https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751565.

[56] Parere congiunto 5/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) del 18 giugno 2021, su https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_it.pdf. Sul ruolo strategico delle Autorità garanti per la protezione dei dati personali si veda F. LAMBERTI, *La proposta di Regolamento UE sull'Intelligenza Artificiale alla prova delle privacy*, in "federalismi.it", *focus* Lavoro Persona Tecnologia, *Paper* 29 giugno 2022, p. 5.

Abstract

*Il contributo esamina il ruolo dei dispositivi di protezione individuale evoluti nell'ambito del rapporto di lavoro, appuntando l'interesse sull'impiego della c.d. "tecnologia indossabile", che rappresenta un'area di sviluppo dell'*Internet of Things. *A tal proposito, è stata indagata la 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. *Ulteriore ambito di ricerca approfondito nell'articolo ha riguardato, poi, la verifica del pieno rispetto delle tutele in materia di privacy e dati personali dei prestatori nelle ipotesi di utilizzo delle nuove tecnologie in funzione prevenzionistica e, segnatamente, dell'*Internet of Things.

The paper deals with the role of smart personal protective equipment in the work relationship, noting the interest in the use of the so-called "wearable devices", that represents a development area in the Internet of Things. In this regard, we investigate the capacity of the employer to fulfil the safety obligation according to art. 2087 c.c. through the use of Internet of Things. Moreover, a further in-depth research topic in the paper regards the check of the full compliance with data protection and privacy of providers in case of using new technologies for preventionist purposes, and, in particular, Internet of Things.

Parole chiave

Internet delle Cose, Intelligenza artificiale, Salute e sicurezza sul lavoro, Datore di lavoro, Controllo umano, Riservatezza

Keywords

Internet of Things, Artificial Intelligence, Health and Safety at Work, Employer, Human Control, Privacy