



FOCUS LAVORO, PERSONA, TECNOLOGIA
13 DICEMBRE 2023

Lavoro e tecnologia: connubio tra opportunità e rischi

di Elena Signorini

Professoressa associata di Diritto del lavoro
Università degli Studi di Bergamo



Lavoro e tecnologia: connubio tra opportunità e rischi*

di Elena Signorini

Professoressa associata di Diritto del lavoro
Università degli Studi di Bergamo

Abstract [It]: L'accelerazione della digitalizzazione richiede una riflessione sulle insidie che l'accompagnano. Tra le difficoltà ravvisabili vi è il delicato rapporto tra le potenzialità che la transizione tecnologica offre e il diritto alla riservatezza del lavoratore nell'esercizio del diritto di controllo da parte del datore di lavoro anche domestico. Allo stato attuale questo sistema, ancora privo di una adeguata regolamentazione, impatta sulle condizioni di lavoro che sono messe in pericolo da un uso non controllato della tecnologia evidenziando la necessità di attuare un adeguato bilanciamento tra i contrapposti interessi dei lavoratori e delle imprese.

Title: Work and technology: a combination of opportunities and risks

Abstract [En]: The acceleration of digitalisation calls for reflection on the pitfalls that accompany it. Among the difficulties that can be identified is the delicate relationship between the potential that the technological transition offers and the employee's right to privacy in the exercise of his or her right to control by the employer, including domestic employees. At present, this system, which still lacks adequate regulation, impacts on working conditions that are endangered by an uncontrolled use of technology, highlighting the need to implement an appropriate balance between the opposing interests of workers and companies.

Parole chiave: Controllo a distanza; Intelligenza artificiale; Monitoraggio; Fondato sospetto; Privacy

Keywords: Remote control; Artificial intelligence; Monitoring; Grounded suspicion; Privacy

Sommario: 1. Introduzione. 2. La trasformazione digitale del lavoro: le insidie derivanti dall'ingresso della IA. 3. Le nuove manifestazioni del potere di controllo del datore di lavoro. 4. Il lavoro domestico e le modalità di controllo. 5. La geolocalizzazione. 6. Considerazioni conclusive.

1. Introduzione

Il rapporto tra nuove tecnologie e lavoro ha messo in evidenza come la relazione lavorativa (sia *pre* che *post covid*) è stata intensamente interessata dagli stravolgimenti che le nuove metodologie, a volte facilitative del lavoro, producono su di esso. Il tema in esame, ponendosi a cavallo tra le modalità di controllo datoriale (gemmato dal contenuto dell'art. 4 dello Statuto dei lavoratori e successive modifiche)¹ e le ricadute sul sistema della *privacy*, rappresenta l'occasione per soffermarsi su alcune delle soluzioni

* Articolo sottoposto a referaggio.

¹ In argomento si segnalano le modifiche apportate dal d.lgs. n. 151 del 2015 e dal d.lgs. n. 185 del 2016 precedute dall'art. 8 del d.l. n. 138 del 2011 in materia di contrattazione di prossimità con cui viene ampliata la platea dei soggetti titolari e legittimati alla stipula degli accordi sindacali quale strumento di autorizzazione privilegiato per la legittima installazione di impianti da cui derivi anche il controllo a distanza ai sensi dell'art. 4 dello Statuto dei Lavoratori portando un elemento di disomogeneità tra le disposizioni di legge. In argomento successivamente si segnala l'Ispettorato del lavoro, Nota n. 4619 del 24 maggio 2017, ha fornito chiarimenti sulle parti legittimate a stipulare gli accordi sindacali ai sensi del combinato disposto degli artt. art. 8 d.l. 138 cit. art. 4 dello Statuto.

applicative adottate per affrontare le esigenze del quotidiano dai cui impatti non risultano immuni i lavoratori². La questione va analizzata unitamente inoltre al monito della UE che vuole e pone “la persona al centro”³ sottolineando come “*le tecnologie digitali dovrebbero tutelare i diritti delle persone, sostenere la democrazia e garantire che tutti gli operatori digitali agiscano in modo responsabile e sicuro. L’UE promuove questi valori in tutto il mondo*”⁴, collocando gli obiettivi digitali al centro del percorso verso il 2030⁵.

La riflessione odierna prende lo spunto dai numerosi studi più o meno recenti⁶, che già hanno sviscerato il tema, dando voce all’operato propulsivo e pionieristico del legislatore sin dagli anni ’70, oltre che della

² A. BELLAVISTA, *Il controllo sui lavoratori*, Torino, Giappichelli, 1995

³ Relazione 2023 sullo stato del decennio digitale, 2023, in <https://digital-strategy.ec.europa.eu/it/library/2023-report-state-digital-decade>; SPECIAL EUROBAROMETER 532, *The Digital Decade, Report Fieldwork*, 2023, testo consultabile sul sito <https://europa.eu>; *Bussola per il digitale 2030: il modello europeo per il decennio digitale*, testo consultabile sul sito della <https://commission.europa.eu/>; Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell’intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL));

⁴ Testo consultabile sul sito <https://commission.europa.eu>

⁵ *Decennio digitale europeo: obiettivi digitali per il 2030*, testo consultabile sul sito <https://commission.europa.eu>

⁶ In questo contributo non sarà possibile approfondire tutte le questioni legate all’impianto dell’art. 4 dello Statuto dei lavoratori, già ampiamente oggetto dell’attenzione della dottrina, e per le quali si vedano: A. BELLAVISTA, *Sorveglianza elettronica, protezione dei dati personali e tutela dei lavoratori*, in LDE, 2023, 1, p. 1; A. BELLAVISTA, *Controlli tecnologici e privacy del lavoratore*, in A. BELLAVISTA, R. SANTUCCI (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Giappichelli, 2022, p. 99, ss; T. COELHO MOREIRA, *The Electronic Control of the Employer in Portugal*, in LLI, 2016, 2, p. 1; C. COLOSIMO, *La moderna declinazione del potere di controllo*, in P. CURZIO, L. DI PAOLA, R. ROMEI (a cura di), *Diritti e doveri nel rapporto di lavoro*, Giuffrè, vol. II, 2018, p.75 ss.; A. DONINI, M. NOVELLA, M.L. VALLAURI, *Prime riflessioni sul lavoro nel metaverso*, in LLI, 2022, 8, 2; A. INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci, 2018; A. INGRAO, *Il braccialelettronico tra privacy e sicurezza del lavoratore*, in DRI, 2019, 3, 895; A.INGRAO, *Il controllo a distanza sulla prestazione dei ciclofattorini tra Scoober App e GPS*, in LLI, 2021, 7, 1, 165; A.INGRAO, *Il potere di controllo a distanza sull’attività lavorativa e la nuova disciplina della privacy nella sfida delle nuove tecnologie*, in *Nuove tecnologie e diritto del lavoro. Un’analisi comparata degli ordinamenti italiano, spagnolo e brasiliano*, a cura di G. LUDOVICO - F. FITA ORTEGA - T. CHRISTINA NAHAS, Milano University Press, 2021, 111; M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, WP CSDLE, It., n. 300/2016; M. MARAZZA, *Social Media e Relazioni industriali. Repertorio di questioni*, in LLI, vol. 5, n. 2/2019, I ss.; A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. TULLINI, Giappichelli, 2017, 1; M. MARAZZA, *I controlli a distanza del lavoratore di natura “difensiva”*, in P. TULLINI (a cura di), *Controlli a distanza cit.*, a cura di P. TULLINI, Giappichelli, 2017, p. 27; M. NOVELLA, *Poteri del datore di lavoro nell’impresa digitale: fenomenologia e limiti*, in LD, 2021, 3-4, 451;; V. MAIO, *I controlli difensivi e la tutela del patrimonio aziendale*, in C. PISANI, G. PROIA, A. TOPO, *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022, p. 416; I. PICCININI, M. ISCERI, *Questioni attuali sul potere di vigilanza e controllo del datore*, in LDE, 2021, n. 4; PISANI C., PROIA G., TOPO A. (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giappichelli, 2022; A. PIZZOFERRATO, *I limiti al potere di controllo datoriale nell’era digitale*, in LDE, 2023, 1, p. 2; D. PIZZONIA, D. POLETTI, *Gli intermediari dei dati*, in EJPLT, 2022, 1; U. ROMAGNOLI, *Sub art. 8*, in G. GHEZZI - F. MANCINI - L. MONTUSCHI - U. ROMAGNOLI, *Statuto dei diritti dei lavoratori*, Bologna, Zanichelli, 1979; E. C. SCHIAVONI, *Gli obblighi informativi in caso di sistemi decisionali o di monitoraggio automatizzati (art. 4, co. 1, lett. a, d.lgs. n. 104/2022) (art. 1, co. 1, lett. s, e art. 1-bis, d.lgs. n. 152/1997, inserito dall’art. 4, co. 1, lett. b, d.lgs. n. 104/2022)*, in *Trasparenza e attività di cura nei contratti di lavoro. Commentario ai decreti legislativi n. 104 e n. 105 del 2022*, a cura di D. GAROFALO - M. TIRABOSCHI - V. FILÌ - A. TROJSI, Adapt University Press, 2022, 211; A. SITZIA, M. I. RAMOS QUINTANA, *Sorveglianza difensiva “occulta” sui luoghi di lavoro e dignità nella prospettiva della Grande Camera della Corte EDU: la Sentenza López*, in LDE, 2019, 3; A. SITZIA, *Il controllo (del datore di lavoro) sull’attività dei lavoratori: il nuovo articolo 4 st. lav. e il consenso (del lavoratore)*, in LLI, n. 1/2016, 83 ss.; L. TEBANO, *La digitalizzazione del lavoro tra intelligenza artificiale e gestione algoritmica*, in *Ianus*, 2021, 24, 43.

dottrina⁷ e non ultima della giurisprudenza⁸. Prendendo pertanto le mosse da tali ricostruzioni⁹, il presente lavoro intraprende un viaggio¹⁰ in questo panorama affascinante¹¹ ed ancora in gran parte sconosciuto e povero di regolamentazione. Ciò che va sondato in particolare è la necessità di coniugare lo scollamento di percezione della realtà offerta dall'intelligenza artificiale (da qui IA)¹² (con tutte le implicazioni che ne derivano in termini di raccolta ed utilizzo di informazioni e dati personali) con il sistema di controllo dei lavoratori¹³ vigente.

⁷ S. LAFORGIA, *I poteri del datore di lavoro, oggi. Opacità e rifrazioni sotto la lente del giurista*, in *Le conquiste legislative degli anni '70 e il ruolo del movimento sindacale in Puglia*, a cura di V. LECCESE - V. PINTO, Edizione Radici Future, 2022, 237.

⁸ S. CIRIELLO, F. ARIANTE, *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c. Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo*, in *LDE*, 2019, p. 3; C. CARTA, *Corte europea dei diritti dell'uomo: la Grande camera torna sul (e difende il) diritto alla privacy del lavoratore*, in *Labor*, 2017; C. COLAPIETRO, A. GIUBILEI, *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione*, in *LLI*, 2021, p. 187; G. CONSONNI, *Il caso Bărbulescu vs. Romania e il potere di controllo a distanza dopo il Jobs Act: normativa europea e italiana a confronto*, in *Dir. Rel. Ind.*, 2016, p. 1771 ss; V. NUZZO, *Il ragionevole sospetto di illecito e la possibilità di controlli difensivi occulti all'esame della Grande Camera della Corte Europea dei diritti dell'uomo*, in *Labor*, 2020, 2, 208; A. INGRAO, *Il "cyberslacking" e i diritti del lavoratore "catturato nella rete informatica". Note critiche a margine della sentenza della Corte Europea dei diritti dell'uomo, sez. IV, 12 gennaio 2016, n. 61496, Bărbulescu vs. Romania, in attesa della pronuncia della Grande Camera*, in *Osservatorio AIC*, 2016, 3, 621; A. INGRAO, *Controllo a distanza e privacy alla luce dei principi di finalità e proporzionalità*, in *LLI*, Vol. 9, No. 1, 2023, p. 103 ss, ISSN2421-2695; L. TEBANO, *I confini dei controlli difensivi e gli equilibri della Corte Edu*, in *RIDL*, 2020, II, 211; 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*, 2016, *LLI*, 2(1), 1-45; P. LAMBERTUCCI, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act)*, in *CSDLE, It.*, n. 255/2015.

⁹ I. ALVINO, *I nuovi limiti controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto i lavoratori e quelle del Codice della privacy*, in *LLI*, 2016, p. 2, 1; M. BARBIERI, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. TULLINI, Giappichelli, 2017, p.183; ; M. T.CARINCI, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. TULLINI, Giappichelli, 2017, p. 45; L. CAIRO, *Controlli a distanza: passato e presente in un tema ancora controverso*, in *Lav. Giur.*, 2018, p. 2; C. GAMBA, *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, in *LLI*, 2016, 2, 1, 122; A. GARILLI, *Tutela della persona e tutela della sfera privata nel rapporto di lavoro*, in *RCDP*, 1992, II, 321 ss.; R. DEL PUNTA, *La nuova disciplina del controllo a distanza sul lavoro (art. 23 D.Lgs. n. 151/2015)*, *RIDL*, 2016, I, 77 ss; R. DI MEO, *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *LLI*, 2018, 4, p. 1; F. LISO, *Computer e controllo dei lavoratori*, in *DLRI*, 1986, 366 ss.; C. OGRISEG, *Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente*, in *LLI*, n. 2/2016, R.27-64.; F. PERRONE, *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei Diritti dell'Uomo e giurisdizione nazionale dopo la sentenza Bărbulescu 2*, in *Labor*, 2018, 3, 283; A. STOLFA, *La tutela della privacy sul luogo di lavoro: gli orientamenti della Corte Europea dei Diritti dell'Uomo*, in *LG*, 2018, 5, 530; L. TEBANO, *Employees' Privacy and Employers' control between the Italian and European system*, in *LLI*, 2017, 3, 2, 3; TULLINI P., *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione possibile?* in *Controlli a distanza e tutela dei dati personali del lavoratore*, a cura di P. TULLINI, Giappichelli, 2017, p. 97; P. TULLINI, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *Riv. It. Dir. Lav.*, 2009, I, p.323, G. ZICCARDI, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *LLI*, 2016, 2, 1, p. 48.

¹⁰ A. ALOISI, N. COUNTOURIS, V. DE STEFANO, *Quando il metaverso è un luogo di lavoro*, 2019, in www.lavoce.it

¹¹ Per IA si intende la disciplina che abbraccia teorie e tecniche pratiche per lo sviluppo di algoritmi che consentano alle macchine (in particolare ai 'calcolatori') di mostrare attività intelligente, per lo meno in specifici domini e ambiti applicativi. Si tratta di quell'insieme di tecnologie e di macchinari dotati - attraverso specifici algoritmi - della possibilità di analizzare ed elaborare una serie massiccia di dati (machine learning) traducendoli in azioni semplici o via via sempre più complesse.

¹² S. RANSBOTHAM, P. GERGERT, M. REEVES, D. KIRON, M. SPIRA, *Artificial intelligence in business*, cit. p. 35 ss.

¹³ S. RANSBOTHAM, P. GERGERT, M. REEVES, D. KIRON, M. SPIRA, *Artificial intelligence in business gets real, Pioneering Companies Aim for AI*, in <https://sloanreview.mit.edu>

Uno tra gli aspetti che il ricorso alle modalità di controllo tecnologico ha, infatti, reso evidente è il cambio di rotta nel rapporto fiduciario¹⁴ che contraddistingue la relazione lavorativa. Questa è una conseguenza del ricorso in maniera preponderante a mezzi di sorveglianza la cui pervasività (derivante anche da una incessante innovazione tecnologica delle modalità con cui può essere perpetrato il controllo a distanza¹⁵) caratterizza oramai il lavoro¹⁶ al punto che i lavoratori si sentono costantemente sorvegliati dalle tecniche distopiche di vigilanza¹⁷. Con la IA la quotidianità dei luoghi di lavoro si mostra, infatti, sempre più contraddistinta da modalità e misure di controllo rappresentate da *webcam*, *badge*, *GPS* oltre che da sistemi di monitoraggio dei movimenti e della posta elettronica¹⁸ che richiedono un temperamento delle «esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore» focalizzando l'attenzione sulla dimensione di trasparenza e proporzionalità dei controlli (art. 4, co. 3)¹⁹. Si tratta di applicazioni di IA talvolta sofisticate ravvisabili anche nel consueto svolgimento del lavoro domestico, contesto nel quale esse sollevano alcune questioni relativi ai risvolti probatori dell'utilizzo delle informazioni assunte tramite tali strumenti.

Punto fermo dal quale occorre partire per ogni riflessione è che, quantunque il controllo a distanza inglobi e rappresenti uno speciale trattamento dei dati personali del lavoratore, questo non lo sottrae alla disciplina generale in materia di *privacy*: senza una adeguata regolamentazione della videosorveglianza i diritti dei lavoratori rischiano, infatti, di soccombere ad una epidemia cibernetica²⁰.

Nella parte conclusiva il contributo svilupperà alcune considerazioni sull'impegno umano che richiede l'approccio tecnologico basato sulla IA. Si tratta, infatti, di maturare una consapevolezza sulle indubbe opportunità che essa apporta esplorandone anche pericoli e limiti. L'integrazione delle nuove tecnologie nei luoghi di lavoro, quali produzione additiva, realtà aumentata o *robot* presuppone un percorso di implementazione che consenta di accompagnare i lavoratori e allo stesso tempo i datori di lavoro a gestire

¹⁴ COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia* (COM(2020) 65 final), in <https://eur-lex.europa.eu>

¹⁵ A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, cit. p. 4.

¹⁶ H. PARKES, *Dystopian worker surveillance techniques likely to disproportionately affect young people says IPPR* (Institute for public policy research), 2023, in www.ippr.org

¹⁷ Un richiamo va ad esempio a quei dispositivi che nella pratica consentono anche una rilevazione e registrazione puntuale dell'attività lavorativa: attraverso il salvataggio automatico della cronologia il datore di lavoro può acquisire una enorme quantità di informazioni sui modi ed i tempi di lavoro ma anche di non lavoro. Controlli a distanza: Ministero del Lavoro, nessuna liberalizzazione; norma in linea con le indicazioni del Garante della Privacy, Nota n. 20, 18 giugno 2015, Ministero del Lavoro e delle Politiche Sociali, in <https://www.lavoro.gov.it>

¹⁸ A. SITZIA, *Il controllo del datore di lavoro su Internet e posta elettronica: quale riservatezza sul luogo di lavoro?* in NGCC, 2016, 6, 1, 901.

¹⁹ A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, cit. p. 4.

²⁰ C. DELLA GIUSTINA - P. DE GIOIACARABELLESE, *Le scelte tragiche durante l'emergenza sanitaria: quando le risorse sono scarse, chi curare? Una riflessione comparatistica*, in Stato, Chiese e pluralismo confessionale, n. 2/2023, 82, not. 59 «il rischio è che si possa passare da uno stato di emergenza sanitaria a uno stato di emergenza cibernetica, o informatica, che potrebbe determinare, quale conseguenza ultima, la scomparsa del genere umano».

nella maniera più idonea il cambiamento, fronteggiando in particolare anche i nuovi rischi, soprattutto psicosociali, che ne possono derivare.

2. La trasformazione digitale del lavoro: le insidie derivanti dall'ingresso della IA

Come noto la trasformazione digitale ha prodotto i suoi effetti su diversi aspetti della relazione lavorativa impattando sul lavoro (inteso nelle sue varie accezioni dalle tipologie, alle competenze, alla formazione, al divario digitale ecc.), sul contratto di lavoro (tempi, luoghi, durata, carichi di lavoro), sulle condizioni dello stesso e sui rapporti di lavoro (conciliazione, *work life balance*, telelavoro, *smart working*) e sulle modalità organizzative dell'impresa (in termini di gestione, monitoraggio dei carichi di lavoro, lavoro a distanza ecc.).

Oltre che nelle fasi di ingresso nel lavoro (colloqui attraverso *chatbots* o anche tramite il riconoscimento emotivo), essa ha assunto un ruolo determinante anche in quelle di valutazione e gestione del personale, ad esempio nel caso degli eventuali esuberanti²¹, oltre che nell'esplicazione del potere di controllo datoriale inducendo ad interrogarsi sulle insidie che essa nasconde giacché, nella convivenza tra “dipendenti umani” e “dipendenti artificiali”, taluni dei poteri tipicamente datoriali sono stati delegati a nuove entità inanimate, ma non per questo neutre.

Si tratta di un aspetto che richiede una riflessione riguardo le modalità, limiti e contorni con cui le IA (sotto forma di applicazioni, di strumenti che utilizzano algoritmi) dovranno essere programmate²², trovandosi ad affiancare ed a sostituire gli uomini in talune frazioni dei processi aziendali. Quella della IA è una ingerenza che concorre al cambiamento dei modelli organizzativi aziendali apportando assistenza, supporto, ausilio nella gestione e velocizzazione delle attività aziendali, ma che al contempo potrebbe inficiare l'impianto che supporta la gestione dell'azienda, dando vita a trattamenti discriminatori o in violazione dei diritti fondamentali quali la dignità o la *privacy* del lavoratore.

Rileva in questo contesto il profilo dei risvolti etici e sociali legati al lavoro ed all'occupazione²³. Si tratta di risvolti legati ai timori che l'intensificazione del ricorso a queste metodologie possa portare entro il

²¹ L. FAILLA, *Intelligenza artificiale e lavoro. Una sfida giuridica, ma anche etica*, 2023, in www.ipsoa.it con riguardo alle notizie relative ai licenziamenti annunciati - (oltre 150.000 dipendenti stando alle ultime stime) pare realizzati in pochissimo tempo, utilizzando sistemi di intelligenza artificiale - da parte di alcune delle Big Tech della Silicon Valley (Meta, Google, Amazon, Microsoft, Twitter e Netflix fra gli altri). Appare sempre più esteso il ricorso, nei piani di esuberanti, a metodi e parametri di individuazione del personale interessato da tali procedure espulsive nelle quali protagonisti sono test di intelligenza artificiale. Tale metodo per quanto nel nostro paese si scontrerebbe con le previsioni della L. n. 223 del 1991 attuativo della Direttiva UE in tema dimostra la deriva e la direzione che sta caratterizzando il mondo del lavoro sollevando il datore di lavoro da tutta una serie di manifestazioni dei suoi poteri che in tal maniera vengono delegati alla IA esimendosi da ogni responsabilità che viene attribuita al funzionamento dell'algoritmo.

²² A. TULLIO, *L'intelligenza artificiale cambia i modelli organizzativi aziendali. Attenzione ai limiti*, 2023, in www.ipsoa.it

²³ I. FERRARI, *Indagine comparata sulla giurisprudenza in materia di responsabilità civile per i danni arrecati dall'uso dei sistemi di intelligenza artificiale*, in LDE, n. 3, 2022.

2055 a dimezzare le attività lavorative sostituendole con una automazione parziale, circostanza questa che avrebbe effetti deflagranti sul mercato del lavoro²⁴. Il tema è stato oggetto di molti studi che variamente hanno valutato l'impatto dell'ingresso della tecnologia nei luoghi di lavoro. Da una parte vi sono quelli che stimano come circa la metà dell'attuale forza lavoro verrà investita dall'automazione grazie alle tecnologie già note e in uso attualmente²⁵; dall'altra vi sono quelli che ridimensionano la responsabilità distruttiva della IA, evidenziando le potenzialità che possono scaturire da una adeguata gestione del rapporto macchina uomo²⁶. In questo scenario in continuo mutamento va altresì segnalato come troppe realtà non essendo ancora in grado di sviluppare ed applicare metodologie domestiche di IA si affidino esclusivamente a prodotti di terze parti²⁷. La mancanza di tecnologie sviluppate internamente aggrava ulteriormente la situazione esponendo i fruitori di questi servizi a rischi spesso non controllati né prevedibili.

Tra le aree di attenzione che la tecnologia porta con sé vi è anche quella riferita al concetto di IA generativa riferita alla sua capacità di analizzare i dati e di creare dei contenuti fondati su tale analisi²⁸ - si pensi agli algoritmi come *ChatGPT*, *Dall-E2*, *Midjourney* tutti sistemi che utilizzano dati di addestramento per generare dati realistici o apparentemente realistici, testi, immagini, audio e li rende poi noti. Oltre a quest'area vanno segnalati altri rischi derivanti da un uso incontrollato della stessa quali il rischio reputazionale difficile da monitorare²⁹, il rischio di generare informazioni sbagliate, cd. di "allucinazione"³⁰ conseguenti alla errata elaborazione delle informazioni dando vita a nuove informazioni; oppure quello di divulgare dati sensibili inconsapevolmente³¹. Questi sono solo alcuni³² dei motivi, tra cui

²⁴ Report *A Future That Works: Automation, Employment and Productivity*, McKinsey Global Institute – MGI, in https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf

²⁵ *Report di The Boston Consulting Group e MIT Sloan Management Review* dimostra che la riduzione della forza lavoro è temuta solo da meno della metà dei manager (47%), convinti invece delle potenzialità (l'85% degli interpellati pensa che permetterà alle aziende di guadagnare e mantenere un vantaggio competitivo); Ricerca di Accenture, *Reworking the revolution: are you ready to compete as intelligent technology meets human ingenuity to create the future workforce*, Forum dell'Economia di Davos nella quale si stima che i ricavi delle imprese potrebbero crescere del 38% entro il 2020, a patto che investano sull'Intelligenza Artificiale e su un'efficace cooperazione uomo-macchina.

²⁶ CAPGEMINI, *Turning AI into concrete value: the successful implementers' toolkit*, in <https://www.capgemini.com>, secondo cui l'83% delle imprese intervistate conferma la creazione di nuove posizioni all'interno dell'azienda, inoltre, i tre quarti delle società intervistate hanno registrato un aumento delle vendite del 10% proprio in seguito all'implementazione dell'Intelligenza Artificiale.

²⁷ E. M RENIERIS, D. KIRON, S. MILLS, *Building Robust RAI Programs as Third-Party AI Tools Proliferate*, 20 June 2023, in <https://sloanreview.mit.edu>

²⁸ Si pensi a ChatGPT- che il Garante della Privacy ha deciso di bloccare in Italia a causa di alcune criticità sulla gestione dei dati degli utenti, oltre a sistemi analoghi capaci della creazione di contenuti video, Garante per la protezione dei dati personali, Provvedimento 11 aprile 2023.

²⁹ BCG, *Generative AI*, 2023, in www.bcg.com; España se encuentra entre los países que lideran la adopción de la Inteligencia Artificial en el entorno laboral, in <https://www.bcg.com/>

³⁰ A. CATALETA, *AI generativa, ecco i rischi dell'uso scorretto dei dati*, 20 settembre 2023, in <https://www.agendadigitale.eu>

³¹ P. LICATA, *AI generativa una grana per le aziende: balza al secondo posto nella classifica dei rischi*, 2023, in <https://www.corrierecomunicazioni.it>

³² OECD, P. LORENZ, K. PERSET, J. BERRYHILL, *Initial Policy considerations for generative artificial intelligence*, 2023.

anche il rischio di perpetrare pregiudizi attraverso la disinformazione, che inducono ad un approccio moderato e responsabile all'espansione dei programmi di IA, che deve essere accompagnata da una maggior consapevolezza³³.

Il processo di transizione digitale che interessa il mondo del lavoro evidenzia l'importanza del mantenimento della cooperazione tra persone e IA. La dimensione operativa ricercata dovrà evitare la sovrapposizione e la sostituzione tra i protagonisti delle nuove relazioni che si stanno intessendo in questo nuovo contesto relazionale, mirando alla creazione di un sistema etico di relazioni reciproche pensato per concretizzare il punto di equilibrio tra uomo e tecnologia. L'IA rappresenta sempre più il cuore pulsante delle aziende ed è determinante valutare se i risultati del ricorso a tali sistemi (operanti tramite gli algoritmi) saranno accettati acriticamente e passivamente o se saranno oggetto di una attività umana di valutazione (etica e giuridica),³⁴ onde valutare la decisione finale e gli impatti che la stessa potrebbe avere sugli individui coinvolti³⁵.

Come accennato in apertura di questa riflessione uno dei rischi è quello cd. di allucinazione derivante dal fatto che la IA non ha un cervello biologico ma opera attraverso algoritmi e modelli di apprendimento e le allucinazioni possono essere una conseguenza di come le macchine elaborano ed interpretano i dati. In questo suo operare può accadere che la realtà venga distorta dall'algoritmo che, se non trova le risposte adeguate al quesito posto, potrebbe appunto falsare, inventare e creare realtà di diverso tipo³⁶. Questo effetto si verifica soprattutto nel momento della elaborazione dei dati e delle informazioni. In questa fase, infatti, le IA elaborano i dati in base ai modelli di apprendimento automatico (rete neurali artificiali) ed alle tendenze che le stesse hanno appreso e che derivano da *input*. Anche la fase dell'addestramento, pertanto, è importante perché se i dati utilizzati per addestrarla sono troppo "rumorosi", o contengono informazioni etichettate in maniera errata, può accadere che nel loro processo di elaborazione l'algoritmo non riesca ad interpretarle correttamente, generando rappresentazioni alterate della realtà. La conseguenza che ne deriva è che nel caso in cui le informazioni da elaborare risultino ambigue, incomplete o non rappresentative, oppure si presentino in grande quantità, l'IA potrebbe trovarsi in difficoltà a comprendere il contesto nel quale calare tali dati, e si potrebbe generare un effetto che l'uomo identifica

³³ Il tema va affrontato anche sotto il profilo dei sistemi intelligenti che acquisiscono dati per alimentare gli algoritmi e che ci sollecitano risposte all'interrogativo etico e giuridico sul futuro che ci attende, poiché molte delle attività un tempo gestite esclusivamente dall'uomo sia in termini intellettuali sia in termini emozionali (o creativi), vengono oggi affidati a delle macchine che danno vita a prodotti (frutto di analisi con sistemi probabilistici della questione presentata) che sono il frutto dell'analisi effettuata che però è ben diversa da una risposta umana.

³⁴ Risoluzione del Parlamento europeo del 20 ottobre 2020 recante raccomandazioni alla Commissione concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2020/2012(INL)), in https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_IT.html

³⁵ L. FAILLA, *Intelligenza Artificiale e gestione degli esuberanti in Italia: la rilevanza del fattore umano*, 2023, in <https://www.quotidianopiu.it/>; nonché dello stesso A. *Intelligenza artificiale e lavoro. Una sfida giuridica, ma anche etica*, cit.

³⁶ A. ALOISI, V. DE STEFANO, *Il tuo capo è un algoritmo*, Laterza, 2020.

come allucinazioni che corrispondono a risultati, gemmati proprio dalla IA, che possono essere, come detto, erronei, frutto di connessioni bizzarre o slegate dai dati degli *input* o prodotto della inventiva estrema generata dall'algoritmo.

I fenomeni che abbiamo delineato sino ad ora prendono il nome di a) *overfitting*, quando l'IA tende ad adattarsi eccessivamente ai dati degli addestramenti specifici, con la conseguenza che il modello partendo dai dati-campione osservati, si dimostra meno capace di generalizzare quando deve affrontare nuove situazioni che si discostano da quelle degli addestramenti (questo deriva dal fatto che, dinnanzi ad un numero eccessivo di parametri rispetto al numero delle osservazioni, l'IA tenderebbe a perdere il controllo con la realtà dei dati); l'altro fenomeno è b) l'*overgeneration* che si manifesta nel momento in cui l'IA generalizza invece eccessivamente, dando vita a connessioni singolari o erronee tra i dati degli *input*³⁷. Si tratta di rischi reali che possono essere mitigati adottando un approccio di addestramento e verifica rigorosi, ricorrendo a dati di alta qualità associati allo sviluppo di meccanismi di controllo capaci di rilevare e correggere eventuali rappresentazioni inverosimili o distorte.

Appare fondamentale dotarsi di una lettura critica giacché per le caratteristiche che la contraddistinguono (opacità, complessità, dipendenza dai dati e comportamento autonomo) il pericolo è la compromissione dei diritti fondamentali degli individui³⁸.

Ne consegue che è opportuno approntare un sistema di gestione del rischio, di monitoraggio e di supervisione umana per ridurre al minimo il pericolo di decisioni errate o distorte assistite dalla IA in settori critici quali il lavoro³⁹ (si pensi ai rischi che potrebbero derivare nel caso di sistemi di guida autonoma se l'IA presentasse delle allucinazioni mettendo in serio pericolo la sicurezza degli individui coinvolti). Per fare questo sarà necessario individuare delle linee guida da comunicare ai produttori degli algoritmi favorendo una programmazione adeguata.

Un ruolo determinante in questo scenario in continuo divenire spetta al diritto ed ai giuristi a cui compete la regolamentazione e la gestione dei nuovi sistemi coniugandoli con i tradizionali coadiuvati, in questo, anche dallo sforzo dell'UE.

A tal riguardo va richiamato l'*Artificial Intelligence Act Proposal* del 2021 approvato dal Parlamento Europeo il 14 giugno 2023 volto a dar vita ad un quadro normativo comune capace di regolamentare i *software* di IA la cui approvazione definitiva dall'UE "dovrebbe" giungere a fine anno consentendo così la sua entrata in vigore nel 2024. Si tratta del primo tentativo di regolamentazione generale dell'IA nato da numerosi

³⁷ C. GALLESE NOBILE, *Legal Aspects of the Use Artificial Intelligence in Telemedicine*, in *Journal of Digital Technologies and Law*, 2023;1(2):314–336.

³⁸ E. FALLETTI, *Discriminazione algoritmica*, Giappichelli, 2022, p. 260 ss.

³⁹ E. FALLETTI, *Discriminazione algoritmica*, cit., p. 200.



atti di impulso e *soft laws*⁴⁰ con l'intento di bilanciare e rappresentare una “quadratura del cerchio” sullo sviluppo della IA a livello globale⁴¹, concretizzando l'obiettivo di un mercato unico digitale efficiente ed equo, oltre che capace di incrementare fino al 2030 tra 1 e 1,4 milioni di posti di lavoro⁴². Tra le ragioni e gli obiettivi della proposta viene sottolineato come l'uso della tecnologia informatica possa favorire risultati vantaggiosi dal punto di vista sociale e ambientale, fornendo vantaggi competitivi fondamentali alle aziende e all'economia europea⁴³.

Concorrono in questo arduo compito oltre all'*Artificial Intelligence Act Proposal* anche altre iniziative dirette a realizzare il progetto di un mercato unico europeo dei dati quali il *Digital Service Act* (DSA)⁴⁴, tra i cui obiettivi vi è la tutela della situazione dei lavoratori delle piattaforme *online* i cui diritti rischiano di essere compromessi e riguardo ai quali sarebbe opportuno che le piattaforme, (richiamando ed ispirandoci alla materia del *crowdfunding*), ricoprissero un ruolo da *gatekeeper* concorrendo nella certificazione delle realtà lavorative digitali filtrando e scartando quelle non virtuose⁴⁵. Affiancano il DSA, nella regolamentazione delle piattaforme digitali per il perseguimento della maggior trasparenza e concorrenza nel mercato europeo digitale dei dati che sia competitivo ed affidabile, anche il *Digital Market Act*⁴⁶, nonché il *Data Act* e il *Data Governance Act*⁴⁷ sui quali il Parlamento UE e Consiglio europeo stanno ancora lavorando⁴⁸. A tal riguardo va segnalato come il 9 dicembre 2023 l'Europarlamento, la Commissione e il Consiglio hanno stato raggiunto un accordo sull'AI Act, ovverosia, la legge europea sull'intelligenza artificiale. Si tratta del primo quadro normativo sui sistemi di intelligenza artificiale nel mondo destinata a dare “un contributo sostanziale allo sviluppo di regole e principi globali per un'IA incentrata sull'uomo”⁴⁹.

⁴⁰ C. CASONATO, B. MARCETTI, *Primeosservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, 2021, consultabile in <https://teseo.unitn.it/biolaw>; E. FALLETTI, *Discriminazione algoritmica*, cit., p. 301.

⁴¹ G. RESTA, *Cosa c'è di 'europeo' nella proposta di regolamento UE sull'intelligenza artificiale?* in *il diritto dell'informazione e dell'informatica*, n. 2/2022, p. 323

⁴² Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), Bruxelles, 15.12.2020, COM(2020) 842 final, 2020/0374 (COD), {SEC(2020) 437 final} - {SWD(2020) 363 final} - {SWD(2020) 364 final}, p. 63, in <https://ec.europa.eu/>

⁴³ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

⁴⁴ Il DSA è stato pubblicato nella Gazzetta ufficiale il 27 ottobre 2022 ed è entrato in vigore il 16 novembre 2022 <https://digital-strategy.ec.europa.eu/>

⁴⁵ E. SIGNORINI, *New paths of protection in the digital labyrinth*, in *Actes de la 30e Journée de droit international privé Le droit international privé dans le labyrinthe des plateformes digitales du 28 juin 2018*, Istituto Svizzero di Diritto Comparato, in *Publication de l'Institut de droit comparé*, Losanna, 2018, pp. 325-334, ISBN/ISSN 978-3-7255-8525-0.

⁴⁶ Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali), cit.

⁴⁷ A. TROJSI, *Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, 2022, 4, p. 276.

⁴⁸ Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), in <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R0868>

⁴⁹ <https://www.europarl.europa.eu/news/it/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai>

L'*excursus* delineato offre l'occasione di osservare come la tecnologia si sia insinuata anche in un aspetto già affrontato dal diritto quale è quello del controllo a distanza. Si tratta di un contesto nel quale ci si deve interrogare sulla capacità dell'impianto normativo esistente di rispondere alle sollecitazioni di un mondo tecnologico in crescita senza che questo porti il datore di lavoro ad abdicare ai poteri oltre che ai valori che ne sono la concreta espressione sociale ed etica. Nel percorso verso un sistema di relazioni che non veda la predominanza di una delle due componenti (tecnologia e potere di controllo), ma una convivenza con scambi reciproci, emerge con prepotenza l'esigenza di disegnare nuovi confini entro i quali il potere di controllo datoriale possa esser esercitato senza tradursi in una violazione dei diritti dei lavoratori.

3. Le nuove manifestazioni del potere di controllo del datore di lavoro

Come già detto nell'introduzione, la nostra dottrina vanta una vasta produzione di contributi sul tema del potere di controllo datoriale analizzato sotto il profilo dei limiti che lo contraddistinguono⁵⁰, alla quale si rimanda per una panoramica.

Le riflessioni odierne non intendono riproporre una ricostruzione del sistema che già è stato ben tratteggiato da cotanta dottrina coadiuvato dalla ricca produzione giurisprudenziale cui si farà riferimento nel prosieguo. L'intento di queste riflessioni è quello di partire da tali ricostruzioni per osservare che ruolo in tale struttura ricoprano le tecniche distopiche di sorveglianza dei lavoratori adottate in misura sempre maggiore dalla azienda, misure divenute sempre più popolari dopo la pandemia, normalizzandosi e diffondendosi in un numero crescente di settori. Se da un lato, infatti, si assiste ad un'intensificazione ed una diversificazione delle modalità di controllo, dall'altro emerge come la regolamentazione a tutela dei dipendenti non sia stata in grado di seguire la stessa velocità nel predisporre nuove forme di tutela dei lavoratori, infrangendosi contro le barriere delle norme a tutela della *privacy*, della riservatezza ed in generale dei valori costituzionali dei lavoratori.

Alcuni studi hanno inoltre evidenziato come la transizione digitale osservata dal punto di vista della prospettiva disciplinare possa andare a discapito di particolari categorie di lavoratori quali i giovani, le donne e lavoratori appartenenti a minoranze straniere⁵¹ (rischio *bias* algoritmici) che rischiano di essere colpiti in modo sproporzionato e negativo dalla sorveglianza dei lavoratori così come attuale, circostanza questa che è acuita dal fatto che ad oggi, la legge non è al passo con la realtà e che questo potrebbe produrre conseguenze disastrose per il benessere mentale e fisico della forza lavoro oltre a far da motrice di pregiudizi in base al genere o all'etnia e non solo.

⁵⁰ A. PIZZOFERRATO, *I limiti al potere* cit. p. 2.

⁵¹ H. PARKES, *Dystopian worker surveillance techniques likely to disproportionately affect young people* says IPPR, 2023, cit.

La sensazione che, inoltre, contraddistingue oramai la stragrande maggioranza dei lavoratori è di essere costantemente sorvegliati attraverso il tracciamento dei movimenti fisici, attraverso la tecnologia *webcam* che può monitorare il tempo trascorso davanti allo schermo, la concentrazione e le espressioni facciali⁵² dei lavoratori sia in ufficio che a casa, attraverso il ricorso al monitoraggio dei veicoli tramite l'uso di telecamere sui cruscotti (nel caso di auto aziendali), sino ad arrivare a pratiche quali quelle che analizzano la pressione dei tasti dei *computer*, o *software* che a intervalli temporali scattano un'immagine dello schermo. Quelle richiamate sono, invero, solo alcune delle tecniche cui le aziende ricorrono per video sorvegliare i propri dipendenti.

Appare di tutta evidenza come questa sia una deriva del sistema che, se non regolamentata, può portare a conseguenze gravi per la salute del lavoratore, non escluso la possibilità di ravvisare comportamenti che si avvicinano alle molestie nei confronti dei lavoratori e negative per l'azienda aumentando inevitabilmente il *turnover* del personale la cui produttività, la cui professionalità viene determinata e calcolata dalla misura arbitraria, ad esempio, di quanto digita e muove il *mouse*⁵³.

Non v'è dubbio che lo scenario del sistema pensato negli anni '70 sia evoluto discostandosi però dall'idea originaria del controllo a distanza, poiché essa mostra un nuovo risvolto del potere datoriale esercitato e talvolta percepito come punitivo.

Come evidenziato in dottrina, è difficile immaginare che strumenti normativi risalenti agli anni '70 possano ancora oggi mantenere la loro forza protettiva intatta. E' indispensabile che il modello regolatorio venga aggiornato, anche alla luce delle recenti riforme e che si riveda urgentemente ciò che è accettabilmente idoneo a coniugare le soluzioni di monitoraggio adottate dal datore di lavoro con le esigenze informative dei lavoratori, soprattutto riguardo ai rischi ed ai livelli di rischio, al grado di pervasività del controllo realizzato, alla indicazione puntuale degli strumenti adottati dall'impresa (specificandone le modalità di funzionamento, le logiche che li supportano), offrendo ogni riferimento utile a comprendere quali dati sono oggetto di raccolta, come siano elaborati e quali azioni vengano assunte dagli algoritmi insiti nell'IA che li governano⁵⁴.

Con lo Statuto dei lavoratori nel 1970 il legislatore era intervenuto pionieristicamente con l'art. 4, rubricato "*Impianti audiovisivi e altri strumenti di controllo*", prevedendo una specifica tipologia di controllo datoriale, ossia il c.d. controllo a distanza. Con tale espressione si intende il controllo effettuato tramite strumenti tecnologici che permettono la vigilanza a distanza sia spaziale che temporale sul lavoratore.

⁵² A. D. SIGNORELLI, *Il riconoscimento facciale sta creando un mondo distopico*, 2019, testo consultabile in www.wired.it

⁵³ C. SKOPELITI, *I feel constantly watched: the employees working under surveillance*, in www.theguardian.com

⁵⁴ G. PROIA, *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione)*, 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*, Giuffrè, 2022.

È di tutta evidenza come questo scenario sia oggi amplificato dall'impatto della transizione tecnologica, al punto che la potenzialità del controllo effettuato tramite le originarie videocamere, posizionate nelle aree lavorative, è giunto ad interessare la quasi la totalità degli strumenti utilizzati dal lavoratore per compiere la propria prestazione lavorativa, (*computer*, telefoni aziendali). Questa condizione ha inevitabilmente accentuato l'eventualità di violazione della dignità e della *privacy*⁵⁵ che accompagnano le modalità di controllo e che nel caso del lavoro presentano tutta una serie di risvolti che meritano una apposita attenzione. Come noto l'originaria stesura dell'art. 4 è stata oggetto di una serie di rivisitazioni rese necessarie per ovviare alla insoddisfazione che accompagnava il disposto statutario sempre più lontano dal contesto produttivo nel quale avrebbe dovuto esprimere le sue potenzialità. All'intervento realizzato nel 2011 con il d.l. n. 138 (art.8) con cui il legislatore abilita il contratto collettivo aziendale di prossimità⁵⁶ alla adozione di soluzioni derogatorie alla previsione statutaria proprio in relazione all'impatto nelle nuove tecnologie è seguito nel 2015 la riforma contenuta nel Jobs Act con cui si è inciso sul tenore letterale della norma, aggiornandolo nel contesto di una realtà organizzativa pervasa dalle implementazioni e dalla incidenza della tecnologia.

L'impianto realizzato in risposta alle istanze della evoluzione tecnologica si discosta inevitabilmente dalla struttura originaria evidenziandone i limiti manifestati nella sua quarantennale applicazione. Oltre, infatti, ad assistere ad una proliferazione di deroghe, pur nel permanere del divieto generalizzato del controllo a distanza della prestazione lavorativa, la giurisprudenza⁵⁷ mette in evidenza tutta una serie di incongruenze in merito alla utilizzabilità delle prove raccolte quantunque in presenza di comportamenti integranti illeciti civili e penali⁵⁸.

Pur permanendo, come detto, il divieto di controllo a distanza della prestazione lavorativa generalizzato e preventivo (controllo diretto) l'impianto che ne deriva richiama la struttura originaria che distingueva da un lato i controlli realizzabili legittimamente solo a seguito di un'autorizzazione sindacale o, in mancanza, amministrativa, giustificati da esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Si tratta dei cd. controlli preterintenzionali (art. 4, c. 1), già teorizzati da dottrina e giurisprudenza prima dell'avvento della riscrittura del 2015, per i quali la finalità per la quale sarà impiegato lo strumento di controllo costituisce essa stessa il presupposto per renderne legittima l'installazione. A seguito della riforma del 2015 tale assetto venne arricchito da quella categoria di controlli che possono essere attuati o attraverso strumenti con cui si rende la prestazione lavorativa oppure attraverso i controlli degli accessi e delle presenze, per i quali non si applica il regime autorizzatorio

⁵⁵ G. FINOCCHIARO, *I limiti posti dal Codice in materia di protezione dei dati personali al controllo del datore di lavoro* in *Diritti e Libertà in Internet*, 2017.

⁵⁶ P. LAMBERTUCCI, *Potere di controllo* cit., p.13.

⁵⁷ Cass.5 ottobre 2016, n. 19922e Cass. 1° ottobre 2012, n. 16622 in <https://www.certifico.com>

⁵⁸ Sul nuovo assetto A. PIZZOFERRATO, *I limiti al potere* cit. p. 3 ss.

da parte sindacale o amministrativa (controllo diretto ex art. 4, c. 2)⁵⁹. Per entrambe le categorie la legittimità del controllo deriva dal rispetto dell'onere di fornire una adeguata informazione ai lavoratori, ed in alcuni casi alle rappresentanze sindacali in azienda, circa le modalità di effettuazione dei controlli. È, infatti, fondamentale che il lavoratore acquisisca consapevolezza delle possibilità di controllo in ossequio al principio di trasparenza e proporzionalità⁶⁰.

Alle ipotesi richiamate di controllo a distanza, effettuato in forma generalizzata e in via preventiva, si è andato ad aggiungere, dall'altro lato, quello del controllo a distanza personalizzato e specifico, operato *ex post* e fuori dall'ambito di azione dell'art. 4, anche in via occulta per scopi difensivi da parte datoriale. La legittimità di questi controlli anche dopo la riforma del 2015 è stata riconosciuta dalla Cassazione anche in sede penale⁶¹. Va attribuito a questo strumento d'origine giurisprudenziale "*aver fatto giustizia*"⁶² riguardo le preclusioni probatorie derivanti dalla norma statutaria.

Con riguardo ai controlli difensivi la giurisprudenza distingue, "*tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio, controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell'art. 4 novellato in tutti i suoi aspetti e "controlli difensivi" in senso stretto, diretti ad accertare specificamente condotte illecite ascrivibili - in base a concreti indizi - a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro*", puntualizzando come tali "*controlli, anche se effettuati con strumenti tecnologici, non avendo ad oggetto la normale attività del lavoratore*", debbano esser posizionati, "*all'esterno del perimetro applicativo dell'art. 4*"⁶³.

⁵⁹ A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, cit. p. 14.

⁶⁰ I. ALVINO, *I nuovi limiti*, cit. p. 43

⁶¹ Nel vigore del testo dell'art. 4 precedente alla riforma la Cassazione penale aveva sancito (Cass. Pen. Sez. III, 15 dicembre 2006, n. 8042) in [www https://olympus.uniurb.it](https://olympus.uniurb.it) in tema di utilizzabilità "*come prove nel processo penale dei risultati delle videoriprese effettuate sul luogo di lavoro a tutela del patrimonio aziendale, in assenza di previo accordo con le rappresentanze sindacali competenti e di previa autorizzazione dell'Ispettorato del lavoro, che "sono utilizzabili nel processo penale, ancorché imputato sia il lavoratore subordinato, i risultati delle videoriprese effettuate con telecamere installate all'interno dei luoghi di lavoro ad opera del datore di lavoro per esercitare un controllo per tutelare il patrimonio aziendale messo a rischio da possibili comportamenti infedeli dei lavoratori, in quanto le norme dello Statuto dei lavoratori poste a presidio della loro riservatezza non proibiscono i cosiddetti controlli difensivi del patrimonio aziendale e non giustificano pertanto l'esistenza di un divieto probatorio"*; Cass. pen., sez. V, 12 luglio 2011, n. 34842 per la quale «*sono utilizzabili nel processo penale le prove di reato acquisite nei confronti di un dipendente mediante videoriprese effettuate con telecamere installate all'interno del luogo di lavoro, ad opera del datore di lavoro, per esercitare un controllo a beneficio del patrimonio aziendale messo a rischio da possibili comportamenti infedeli dei lavoratori, perché le norme dello statuto dei lavoratori poste a presidio della loro riservatezza, non fanno divieto dei c.d. controlli difensivi del patrimonio aziendale e non giustificano, pertanto, l'esistenza di un divieto probatorio*»; ancora v. Cass. Pen. Sez. III, 12 novembre 2013, n. 4331, in [www https://olympus.uniurb.it](https://olympus.uniurb.it). Successivamente alla riforma del 2015 v. Cass. Pen. Sez. III, 6 dicembre 2016, n. 51897, in Foro It., 2017, 2, II, 89; Cass. Pen. Sez. III, 08 settembre 2016, n.51897, in <https://www.eius.it/giurisprudenza/>; Cass. Pen. Sez. II, 12 maggio 2016, n.33567, [www https://olympus.uniurb.it](https://olympus.uniurb.it); Cass. Pen. Sez. III, 7 aprile 2016, n. 45198, in <https://www.puntodidiritto.it/>; Cass. Pen. Sez. II, 30 novembre 2017, n.4367, in <https://www.adlabor.it/interpretazioni/>; Cass. Pen. Sez. III, 31 gennaio 2017, n.22148, in <https://www.altalex.com/>; Cass. Pen. Sez. III, 10 aprile 2018, n.38882 in [www https://olympus.uniurb.it](https://olympus.uniurb.it); Cass. Pen. Sez. III, 27 gennaio 2021, n. 3255, in [www https://olympus.uniurb.it](https://olympus.uniurb.it); Cass. Pen. Sez. III, 15 luglio 2019, n.50919 in [www https://olympus.uniurb.it](https://olympus.uniurb.it); Cass. Pen. Sez., III, 17 gennaio 2020, n. 1733, in [www https://olympus.uniurb.it](https://olympus.uniurb.it); Cass. Pen. Sez. III, 16 novembre 2023, n. 46188, in <https://www.dirittoegiustizia.it/>

⁶² A. MARESCA, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, cit. p. 2, 7 ss.

⁶³ Cass. 22 settembre 2021, n. 25732, punto 31 e 32, consultabile in [www https://olympus.uniurb.it](https://olympus.uniurb.it)

Oltre a tale presupposto tali controlli richiedono anche un posizionamento temporale giacché, a differenza dei controlli preventivi quelli di tipo difensivo in senso stretto devono essere mirati ed attuati *ex post*, ossia "a seguito del comportamento illecito di uno o più lavoratori del cui avvenuto compimento il datore abbia avuto il fondato sospetto", perché solo a partire da quel preciso momento il datore può provvedere alla raccolta di informazioni utilizzabili⁶⁴.

La presenza di un ragionevole sospetto⁶⁵ circa l'esistenza di condotte illecite commesse dal lavoratore concorre a legittimare il controllo a distanza personalizzato e specifico, attuato a posteriori, sebbene in via occulta con scopo difensivo del datore di lavoro. Su questo ultimo aspetto è intervenuta la giurisprudenza che ha puntualizzato come anche "in presenza di un sospetto di attività illecita", occorrerà, nell'osservanza della disciplina a tutela della riservatezza del lavoratore, e segnatamente dell'art. 8 della Convenzione Europea dei diritti dell'uomo come interpretato dalla giurisprudenza della Corte EDU, "assicurare un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, con un contemperamento che non può prescindere dalle circostanze del caso concreto"⁶⁶.

L'aspetto della legittima utilizzazione delle informazioni e dei dati raccolti a tutti i fini connessi al rapporto di lavoro soggiace pertanto ai presupposti compendati nel principio di diritto elaborato recentemente dalla Suprema Corte⁶⁷ (pur rifacendosi alla pronuncia n. 25732 del 2021) contraddistinti da una estensione temporale del controllo. Secondo infatti la giurisprudenza "sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, 1) in presenza di un fondato sospetto circa la commissione di un illecito, purché 2) sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore, 3) sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto"⁶⁸.

La competenza che sta maturando la dottrina verso la IA dovrebbe soffermarsi anche a "considerare la qualità dei dati", nel senso che l'esperienza fornita sta ponendo in evidenza che il metodo usato sino ad oggi di raccolta dei dati (di cui si sia già in possesso) e loro preparazione (perché già a disposizione) per il trattamento forse dovrebbe essere oggetto di un mutamento di approccio. Questo dovrebbe consentire di vedere i dati come qualcosa da cui partire, come informazioni non più modificabili che debbono essere abilitate per l'analisi preventiva all'avvio di un modello, o di un progetto o di una azienda. Questo metodo

⁶⁴ Cass. 22 settembre 2021, n. 25732, punto 40, 44, consultabile in www.olympus.uniurb.it

⁶⁵ R. ROMEI, *Il "ragionevole sospetto" in Cassazione*, in LDE, 2023, 1.

⁶⁶ Cass. 22 settembre 2021, n. 25732, punto 36e 38, consultabile in www.olympus.uniurb.it, ove si richiama Cass. 10 novembre 2017, n. 26682, consultabile in <https://www.defensis.it>

⁶⁷ Cass. 26 giugno 2023, n. 18168 consultabile in www.olympus.uniurb.it

⁶⁸ Cass. 22 settembre 2021, n. 25732, punto 51, consultabile in www.olympus.uniurb.it

consentirebbe di fornire agli algoritmi delle informazioni dettagliate per ideare e fornire misure di contrasto (come nel caso in esame verso potenziali comportamenti riconducibili a illeciti), o prodotti ed azioni mirate ed ottimizzate perché più rispondenti alle esigenze ed alle finalità dei fruitori.

Da quanto delineato emerge come la giurisprudenza circoscrive il controllo ai dati di cui si sia acquisita conoscenza a seguito all'insorgenza del sospetto, espressione questa su cui la dottrina si è a lungo interrogata⁶⁹ giungendo alla conclusione che non si può legittimare a posteriori, neppure ricorrendo a questa tipologia di controllo, una eventuale pratica di acquisizione generalizzata *ex ante* di dati attuata violando la previsione dell'art. 4 dello Statuto. Merita rammentare, infatti, che deve esser garantito il rispetto dell'art. 8 della Convenzione Europea dei diritti dell'uomo, citato, laddove impone di assicurare un corretto bilanciamento tra le esigenze di salvaguardia della dignità e riservatezza del dipendente e quelle di protezione da parte datoriale degli interessi e dei beni aziendali, nel rispetto dei canoni generali di correttezza e buona fede contrattuale.

La stessa dottrina ha peraltro evidenziato la miopia dimostrata talvolta dalla Corte; la finalità del controllo non deve essere solo funzionalizzata alla prevenzione della commissione di ulteriori illeciti, ma è opportuno che esso possa estendersi anche alle condotte pregresse già realizzate dal lavoratore, in un'ottica riabilitativa, ma soprattutto finalizzata all'accertamento fattuale ai fini probatori in sede processuale⁷⁰.

Sul punto la Corte puntualizza che allegazione e prove debbono riguardare *“circostanze temporalmente collocate, atteso che le stesse segnano il momento a partire dal quale i dati acquisiti possono essere utilizzati nel procedimento disciplinare e, successivamente, in giudizio, non essendo possibile l'esame e l'analisi di informazioni precedentemente assunte in violazione delle prescrizioni di cui all'art. 4 St. lav., estendendo "a dismisura" l'area del controllo difensivo lecito, considerato che non può essere reso retroattivamente lecito un comportamento che tale non era al momento in cui fu tenuto”*⁷¹.

Altro aspetto su cui la giurisprudenza è intervenuta è quello dedicato all'onere della prova precisando come incomba sul datore di lavoro l'onere di allegare prima e provare poi le specifiche circostanze che lo hanno indotto ad attivare un controllo tecnologico *ex post*, onere che deriva dal combinato disposto tra la necessaria sussistenza di un fondato sospetto che consente al datore di porre la sua azione fuori

⁶⁹ V. NUZZO, *Il ragionevole sospetto di illecito e la possibilità di controlli difensivi occulti all'esame della Grande Camera della Corte Europea dei diritti dell'uomo*, cit.

⁷⁰ A. BELLAVISTA, *Sorveglianza elettronica*, cit. 183.

⁷¹ Cass. 22 settembre 2021, n. 25732, punto 41, consultabile in www.olympus.uniurb.it in argomento anche Cass. Pen. 27 gennaio 2021, n. 3255 che è intervenuta in argomento sancendo che *“Non è configurabile la violazione della disciplina di cui alla L. n. 300 del 1970, artt. 4 e 38 - tuttora penalmente sanzionata in forza del D.Lgs. n. 196 del 2003, art. 171 come modificato dalla L. n. 101 del 2018 - quando l'impianto audiovisivo o di controllo a distanza, sebbene installato sul luogo di lavoro in difetto di accordo con le rappresentanze sindacali legittimate o di autorizzazione dell'Ispettorato del lavoro, sia strettamente funzionale alla tutela del patrimonio aziendale, sempre che il suo utilizzo non implichi un significativo controllo sull'ordinario svolgimento dell'attività lavorativa dei dipendenti o resti necessariamente "riservato" per consentire l'accertamento di gravi condotte illecite degli stessi”*. Analogamente Cass. pen. Sez. III, 14 dicembre 2020, n. 3255, consultabile in <https://www.altalex.com>

dall'ambito di applicazione diretta dell'art. 4 Stat. e il criterio generale dell'art. 5, della legge n. 604 del 1966 sui licenziamenti individuali che fa ricadere sulla parte datoriale l'onere di provare il complesso di elementi che giustificano il licenziamento⁷². Nel caso in cui il datore di lavoro non riesca a fornire la prova che i dati di matrice tecnologica posti a fondamento della procedura disciplinare siano stati legittimamente acquisiti, la sanzione prevista dall'ordinamento discende dalla previsione generale in materia di protezione della *privacy* secondo cui "*i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*" (D. Lgs. n. 196 del 2003, art. 11, comma 2).

L'onere informativo, ravvisabile in capo al datore di lavoro, va ad intersecarsi con le recenti previsioni del Decreto Trasparenza⁷³, infatti, gli obblighi informativi nel lavoro e l'utilizzo di sistemi di monitoraggio automatizzati debbono essere oggetto di coordinamento con il GDPR. Il decreto lavoro interviene in materia di trasparenza nei contratti di lavoro ridimensionando l'obbligo informativo a carico del datore di lavoro nel caso di utilizzo di sistemi decisionali o di monitoraggio, riferendolo ai soli casi in cui questi siano "integralmente automatizzati"⁷⁴. Tuttavia, occorre considerare le norme in materia previste dal GDPR, secondo il quale gli obblighi informativi non sono solo limitati agli strumenti integralmente automatizzati⁷⁵.

4. Il lavoro domestico e le modalità di controllo

Uno dei contesti nel quale il tema del controllo manifesta le sue tante debolezze è quello legato al lavoro domestico di cui alla l. 339 del 1958 che, come noto, è sottratto all'applicazione dei limiti e dei divieti previsti dall'art. 4 dello Statuto dei lavoratori. In argomento va però segnalato l'intervento della Nota 1004 dell'8 febbraio 2017 dell'INL che ha fornito un parere positivo in merito alla possibilità di autorizzare l'installazione di un impianto di videosorveglianza collocato in una abitazione privata all'interno della quale è presente un lavoratore domestico⁷⁶, questo purché il datore di lavoro informi il lavoratore della volontà di procedere alla videosorveglianza acquisendone il relativo e preventivo consenso.

Nel 1987 la Corte Costituzionale con sentenza n. 585 si era già pronunciata sulle peculiarità che contraddistinguono il lavoro domestico specificando che "*Non v'è dubbio che il rapporto di lavoro domestico per la sua particolare natura si differenzia, sia in relazione all'oggetto, sia in relazione ai soggetti coinvolti, da ogni altro rapporto*

⁷² Cass. 26 giugno 2023, n. 18168, consultabile in [www.https://olympus.uniurb.it](https://olympus.uniurb.it)

⁷³ B. ROSSILLI, *Gli obblighi informativi relativi all'utilizzo di sistemi decisionali e di monitoraggio automatizzati indicati nel decreto "Trasparenza"*, in *Federalismi.it, focus LPT*, 5 ottobre 2022;

⁷⁴ Art. 5, 12, 13 e 15 del Regolamento Ue sulla *privacy* n. 2016/679 (GDPR).

⁷⁵ Art. 1-bis. Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati, D.Lgs. n. 152/1997.

⁷⁶ INL, Nota 1004, dell'8 febbraio 2017, in www.ispettorato.gov.it

di lavoro: esso, infatti, non è prestato a favore di un'impresa avente, nella prevalenza dei casi, un sistema di lavoro organizzato in forma plurima e differenziata, con possibilità di ricambio o di sostituzione di soggetti, sebbene di un nucleo familiare ristretto ed omogeneo; destinato, quindi, a svolgersi nell'ambito della vita privata quotidiana di una limitata convivenza. In ragione di tali caratteristiche, proprie al rapporto, la Corte ha già evidenziato, in via di principio, la legittimità di una disciplina speciale anche derogatoria ad alcuni aspetti di quella generale" (sentenza n. 27 del 1974)."

Quantunque l'esclusione dalla applicazione dell'art. 4 Statuto dei lavoratori derivi pertanto dal fatto che il datore di lavoro domestico è un soggetto privato, che non organizza il lavoro in forma d'impresa come avviene invece per i soggetti presi in esame dallo Statuto dei lavoratori, ciò non lo sottrae al rispetto della ordinaria disciplina sul trattamento dei dati personali, dovendosi confermare la tutela della riservatezza al d.lgs. n. 196 del 2003 e ss. modifiche in ordine al consenso preventivo ed agli obblighi informativi⁷⁷.

Dal quadro delineato esula la questione riferibile al fatto che le apparecchiature sono installate con lo scopo di evitare possibili attività criminali, come il furto di oggetti preziosi o comportamenti violenti nei confronti della persona assistita; in questo particolare caso, infatti, non è necessario il consenso del collaboratore e nonostante la mancanza di questo, le prove ricavate dalla registrazione degli impianti possano essere validamente utilizzate in sede processuale.

Il tema è complesso. Soprattutto è da comprendere se i controlli a distanza, attuati anche attraverso strumenti tecnologici, siano da considerarsi legittimi in questo particolare tipo di rapporto; per rispondere a questo quesito occorre considerare pertanto che, anche nel lavoro domestico, il controllo a distanza soggiace ai limiti dettati dal nostro ordinamento, sia in ordine alla tutela della dignità del lavoratore, sia in ordine al rispetto dell'aspettativa di *privacy* del lavoratore. L'installazione di apparecchi di videosorveglianza potrà essere quindi liberamente effettuata ma solo nel rispetto della dignità e della *privacy* del prestatore a cui sarà, quindi, dovuta adeguata informazione, come previsto dal GDPR, e dovrà essere fornita specifica informativa in merito a modalità e tempistiche dei controlli che devono essere palesi e non possono essere continuativi o vessatori.

Altro aspetto su cui porre l'attenzione è l'oggetto del controllo che nel caso in esame potrebbe esser destinato non tanto a valutare la correttezza della prestazione ed i possibili inadempimenti aventi una rilevanza disciplinare, bensì ad accertare che durante lo svolgimento di questa il prestatore non commetta illeciti penali (che potrebbero sostanziarsi nella commissione di un reato con funzione di deterrente) contro il patrimonio del datore oppure nei confronti dei soggetti, nella maggior parte dei casi deboli o incapaci, di cui è chiamato a prendersi cura. In tali circostanze, infatti, occorre operare come anticipato un diverso bilanciamento di interessi, poiché alla necessità di tutelare la dignità e la *privacy* del lavoratore,

⁷⁷ Resta comunque applicabile l'art. 8 dello Statuto che disciplina il divieto di effettuare indagini sul profilo del lavoratore che non riguardino in modo diretto l'attività lavorativa svolta.

va a contrapporsi il diritto, primario, alla tutela di soggetti particolarmente bisognosi quali anziani o bambini, di cui potrebbe essere necessario garantire la sicurezza. Si ritorna in questo caso all'ipotesi affrontata dalla giurisprudenza in materia di controlli occulti⁷⁸ contraddistinti dal carattere occasionale, non sistematico, oltre che costituenti l'*estrema ratio*, essendo tecnicamente indispensabili e non sostituibili ed implicando, per la loro stessa legittimità, che vi sia un fondato sospetto.

Sul tema la Suprema Corte si è recentemente pronunciata⁷⁹ confermando un orientamento già delineato nel 2021 secondo cui *"in nessun caso può essere giustificato un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore"* (punto 37), e che anche nel caso di controllo difensivo *"in senso stretto"* lecito, occorre comunque sia *"assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore"*. La pronuncia ha operato un contemperamento che intesse la trama della disciplina dei controlli anche nel concorrere multilivello di fonti interne e sovranazionali derivanti dal combinato tra la previsione statutaria novellata dell'art. 4, il Codice della privacy (art. 13), il Regolamento UE 2016/679 e ss. modifiche.

Con riguardo specifico ai reati verificabili in ambito domestico che potrebbero essere contrastati tramite il ricorso alla videosorveglianza si segnalano il furto in casa (art. 624 cc), appropriazione indebita (art. 646 cp); ricettazione (art. 642 cp); la circonvenzione di incapace (art. 643 cp), lo *stalking*, delitto di atti persecutori (art. 612 bis cp); ricatti ed estorsione, (art. 629 cp); abbandono e maltrattamenti (art. 591 cp); sequestro (art. 605 cp) e schiavitù (art. 600 cp); omicidio (art. 575 cp)⁸⁰. Si tratta di un panorama assai vasto ed in questo contesto occorre affrontare l'aspetto della utilizzabilità delle risultanze probatorie ottenute a seguito del controllo occulto, posto in essere per valutare la possibile illiceità delle condotte.

⁷⁸ Tra gli altri casi affrontati dalla giurisprudenza in tema di controlli occulti quantunque non in ambito domestico si citano Cass. 8 giugno 2011, n. 12489: controlli occulti tramite agenzie investigative - basta il sospetto o la mera ipotesi degli illeciti in corso di esecuzione; Cass. 22 dicembre 2009, n. 26991 del 2009: controlli svolti da guardie giurate per accertare che un lavoratore ometta la consegna dello scontrino fiscale ai clienti; Cass. 18 settembre 1995, n. 9836: utilizzo di un istituto di vigilanza sull'incasso del prezzo e rilascio dello scontrino fiscale da parte di un dipendente in <https://sentenze.laleggepertutti.it> La Corte di Cassazione n. 12489 del 2011 cit. nel decidere in merito alla legittimità del licenziamento effettuato a seguito della investigazione commissionata dal datore di lavoro puntualizzava che il limite posto dall'art. 2 dello Statuto dei lavoratori in merito all'intervento di soggetti preposti dal datore a tutela del patrimonio aziendale, non esclude che il datore possa incaricare agenzie per svolgere indagini su illeciti, penali o fiscali, integranti violazioni di obblighi extracontrattuali, già commessi o in via di esecuzione, da parte del lavoratore dipendente. Nel caso in esame il controllo esercitato dal datore risultava lecito non essendo diretto a valutare l'eventuale inadempimento dell'obbligazione lavorativa, bensì a valutare le condotte attuate dal lavoratore, di carattere fiscale o penale che in ogni modo esulano dal contenuto della prestazione lavorativa. Nel giudicare la Corte altresì dichiara ammissibile escutere i dipendenti dell'agenzia di investigazione in qualità di testi e conferma l'ammissibilità della prova operata dal giudice di appello, in quanto i dipendenti della suddetta agenzia non avevano alcun interesse diretto nella lite.

⁷⁹ Cass. 26 giugno 2023, n. 18168, Cass. 22 settembre 2021, n. 25732; Cass. 12 novembre 2021, n. 34092 consultabile in www.olympus.it

⁸⁰ DOMINA, *Il valore del lavoro domestico, il ruolo economico e sociale delle famiglie datori di lavoro, reati penali verificabili nel lavoro domestico*, Dossier 7, 2017.

Questo interrogativo è fondamentale poiché solo e limitatamente a questo fine potrebbe essere utilizzato quanto ottenuto tramite controllo occulto, mentre tali risultanze non potranno essere invece utilizzate per fondare un procedimento disciplinare basato su possibili inadempimenti contrattuali venuti alla luce attraverso il medesimo controllo.

Volendo esplicitare quanto detto va segnalato che nel caso venga realizzato un controllo occulto per verificare un sospetto abuso nei confronti del soggetto devoluto alle cure di un/una badante, le risultanze probatorie potranno essere utilizzate esclusivamente a fondamento della prova del procedimento penale finalizzato alla condanna della/o stessa/o per il maltrattamento del soggetto per il cui benessere era stato stipulato il contratto. Laddove dal medesimo controllo, invece, fosse stato possibile venire a conoscenza di un inadempimento contrattuale, questa prova non sarà utilizzabile a fini disciplinari e resterà esclusa da un possibile giudizio del lavoro. La forte limitazione che deriva da quanto delineato viene mitigata dal regime del licenziamento vigente in ambito domestico: in questo contesto, infatti, in ogni caso il datore di lavoro può recedere liberamente, purché venga dato il preavviso, senza dare una giusta causa o giustificato motivo al lavoratore. Nei fatti, quindi, il datore di lavoro potrà licenziare per giusta causa il lavoratore che realizzi un illecito penale mentre potrà, in ogni caso, licenziare il lavoratore inadempiente, ex art. 2118 c.c., senza che sia data evidenza del controllo occulto effettuato e da cui si è potuto evincere l'inadempimento attuato.

Anche le fasi di estinzione del rapporto di lavoro domestico traggono la loro origine in un corollario normativo che “*quasi fisiologicamente si allontana dalle regole generali che assistono ordinariamente il momento di interruzione del legame negoziale tra le parti interessate*”⁸¹. La giustificazione di una tale distinzione deriva dal diverso perimetro normativo nel quale questo rapporto si incardina e scaturisce dalla particolare natura del soggetto datoriale, nonché dalle speciali caratteristiche che contraddistinguono la prestazione lavorativa resa dal lavoratore, e inoltre dall’ambiente di lavoro in cui esso si sviluppa.

5. La geolocalizzazione

Da quanto tratteggiato il tema presenta svariate sfaccettature e tra gli ulteriori aspetti che meritano di essere affrontati vi è quello del rapporto tra l’esplicazione del controllo e la tutela della *privacy* del lavoratore nel caso della geolocalizzazione. Sul tema è intervenuta la Corte Europea dei diritti dell’uomo in ordine alla legittimità del tracciamento GPS dei veicoli aziendali⁸² soffermandosi sui confini tra liceità

⁸¹ NOTA INL n. 1004 del 2017 cit.

⁸² Sentenza CEDU Sez. IV del 15 dicembre 2022 n. 26968/16, testo consultabile in <https://www.certifico.com>

ed illiceità sull'utilizzo degli strumenti in esame che, seppur consentiti dalle norme, possono trasformarsi, a causa di particolari condotte, in abusi⁸³ e vessazioni.

L'autorità garante per la protezione dei dati personali si è dimostrata particolarmente intransigente riguardo alla geolocalizzazione dei mezzi aziendali, ponendosi in linea con le previsioni dello Statuto dei lavoratori che vieta il controllo dei lavoratori a distanza, pur coniugandolo con una serie di indicazioni che contengono precauzioni e cautele da adottare laddove i datori di lavoro utilizzino mezzi aziendali con installati a bordo sistemi di geolocalizzazione finalizzati alla tutela del patrimonio. In particolare tre sono le precauzioni indicate per la legittimazione del metodo di controllo: in primo luogo si ammette che la geolocalizzazione dei mezzi guidati dal personale aziendale sia adottata solo al fine di garantire la sicurezza dei veicoli e l'ottimizzazione dei carichi di lavoro; in secondo luogo si prescrive la presenza sui dispositivi, che geolocalizzano, di una icona che indichi quando la localizzazione è attiva, in ultimo si prevede la possibilità di disattivazione della stessa durante le pause (pranzo e altre pause lavorative contrattuali) previa informazione dei dipendenti dei casi in cui è consentito disattivare il GPS⁸⁴.

Il tema si è arricchito, a seguito dell'entrata in vigore del GDPR nel 2018, dell'ulteriore criterio della *minimizzazione*, in ossequio al *principio di privacy by design e by default*. Il GDPR ha, infatti, imposto al titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti. Il principio di *privacy by design*, contenuto nell'art. 25 offre un diverso approccio concettuale finalizzato alla predisposizione di un sistema di protezione sostanziale e non meramente formale poggiato su un progetto corredato sin dalla sua ideazione dalla valutazione dei rischi, degli strumenti e delle corrette modalità previste al fine di tutelare nella concretezza gli utenti. I principi cui esso si ispira sono “*prevenire non correggere*” (inteso nel senso che i problemi vanno valutati nella fase di progettazione e l'applicativo deve prevenire il verificarsi dei rischi); *privacy come impostazione di default* (inteso nel senso della non obbligatorietà della compilazione di un campo o di un *format* il cui conferimento di dati è facoltativo); *privacy incorporata nel progetto* (inteso nel senso dell'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati); *massima funzionalità, in maniera da rispettare tutte le esigenze* (inteso nel senso di rifiutare le false antitesi come quelle che ad una maggior *privacy* corrisponderebbe una minore sicurezza); *sicurezza durante tutto il ciclo del prodotto o servizio; visibilità e trasparenza del trattamento*, (riferita cioè a tutte le fasi operative che debbono essere trasparenti in modo che sia verificabile la tutela dei dati); *centralità dell'utente* (inteso nel senso del rispetto dei diritti e della necessità di offrire tempestive e chiare risposte alle richieste di accesso)⁸⁵. La valutazione dovrà esser fatta preventivamente all'avvio del

⁸³ L. DI GIACOMO, *Geolocalizzazione dei lavoratori: pronuncia CGUE*, 2023, testo consultabile in www.diritto.it sul Caso Florindo de Almeida Vasconcelos Gramaxo/Portogallo (pronuncia n. 26968/2016 depositata il 13 dicembre 2022).

⁸⁴ <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9936174>

⁸⁵ B. SAETTA, *Principi fondamentali*, 2018, in <https://protezionedatipersonali.it>



trattamento e l'approccio del GDPR è proprio quello di evitare la progettazione di un sistema rispondente alla norma ma svuotato di efficacia nella quotidianità⁸⁶.

Quanto al principio di *privacy by default* (protezione per impostazione predefinita), esso sollecita le imprese a trattare i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Si tratta di una misura precauzionale, di un approccio prudente riferito non solo alla quantità e qualità dei dati, ma anche alla durata del loro trattamento ed alle persone che possono accedere agli stessi⁸⁷.

Sull'impianto così delineato si è andata a porre la pronuncia della Corte Europea dei diritti dell'uomo⁸⁸ sancendo la legittimità del licenziamento intimato ad un dipendente, basato sulle risultanze del sistema di geolocalizzazione GPS dell'auto aziendale in uso al medesimo, sancendo che la raccolta e il trattamento dei relativi dati così effettuata non comportano una violazione dei diritti del lavoratore come sanciti dalla Convenzione dei diritti dell'uomo. Centro dell'analisi è stato il tipo e il livello di sorveglianza progettato e attuato dal datore di lavoro, livello che la Corte ha ritenuto accettabile fissando dei criteri per il giusto bilanciamento tra diritti del lavoratore al rispetto della sua vita privata e le prerogative datoriali in termini di controllo sul corretto impiego dei beni aziendali, bilanciamento che va fatto caso per caso. Il tema della difesa della *privacy* individuale da interferenze arbitrarie e illegittime in un contesto professionale (ex art. 8 della Convenzione Cedu) si coniuga con il diritto del datore di lavoro di gestire razionalmente i mezzi messi a disposizione dei dipendenti, accertandosi che essi siano destinati all'effettivo svolgimento delle mansioni professionali e non ad altri scopi, onde evitare che un uso inappropriato si traduca in un pregiudizio significativo per il datore. Oltre a disporre la legittimità del controllo tramite dispositivo GPS la pronuncia ha evidenziato come nel bilanciamento degli interessi in gioco sono prevalsi gli interessi del datore di lavoro a non subire danni economici o sprechi derivanti da un uso scorretto dei veicoli in un periodo di difficoltà economica.

Sempre in argomento va segnalato il recente provvedimento emanato dal Garante della *privacy*⁸⁹ nel 2023 con il quale è stata comminata una sanzione di 20.000 euro ad una società incaricata della lettura dei contatori gas, acqua e luce per condotta illecita non avendo (la società datrice di lavoro) fornito idoneo riscontro alle istanze di accesso presentate dai dipendenti riguardo ai dati raccolti attraverso lo *smartphone*

⁸⁶ <https://protezionedatipersonali.it>

⁸⁷ European Data Protection Board, *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, 2019, in https://edpb.europa.eu/our-work-tools/documents/public-consultations/2019/guidelines-42019-article-25-data-protection_en

⁸⁸ A. ABBASCIANO, *Il controllo a distanza del datore di lavoro e il rispetto del diritto alla vita privata del lavoratore (ancora) sotto i riflettori della Corte Edu: il caso Gramaxo c. Portugal*, in LLI, 2023, 9(1), C.1-C.25; C. DELLA GIUSTINA, *La videosorveglianza 'reale' del lavoratore approda alla Corte EDU. Il caso Affaire Florindo de Almeyda Vasconcelos Gramaxo c. Portugal*, in <https://www.nomos-leattualitaneldiritto.it>

⁸⁹ <https://www.cybersecurity360.it>

aziendale, su cui era stato installato un sistema di geolocalizzazione idoneo a individuare il tragitto da effettuare per raggiungere i contatori, al fine di chiarire le modalità di quantificazione dei corrispondenti rimborsi chilometrici. Due sono i profili dai quali il Garante fa derivare il suo giudizio di illiceità del comportamento datoriale. Con riguardo al primo profilo va evidenziato come dal testo del provvedimento emerga come la società datrice di lavoro ricavasse dal GPS, di cui erano dotati i mezzi aziendali, tutta una serie di dati personali riferiti ai lavoratori. I sistemi di GPS consentono, infatti, di registrare dati relativi alla posizione, ovvero latitudine, longitudine, altitudine, direzione di marcia e ora di registrazione della posizione riferita al luogo presso i quali gli operatori effettuano i loro servizi. Nel caso specifico la geolocalizzazione risultava necessaria al fine di permettere all'operatore l'individuazione del tragitto da effettuare per giungere ai contatori, posizione che il terminale indica come luogo ove effettuare le rilevazioni. Il sistema di geolocalizzazione noto anche come RTLS (*Real Time Location Systems – Sistemi di Localizzazione in Tempo Reale*) consente in generale l'identificazione della posizione geografica ben definita di un oggetto o di un individuo, in un determinato momento, indipendentemente dal fatto che sia fermo o in movimento.

In secondo luogo, il provvedimento fa riferimento al sistema progettato per trattare i dati personali dei dipendenti che svolgono mansioni di tecnico dei contatori. Come noto il sistema di geolocalizzazione può essere utilizzato per attestare svariate attività collegate ai lavoratori quali ad esempio la presenza giornaliera, la quantificazione delle ore e dei servizi effettuati accertando lo svolgimento dei compiti assegnati (come nel caso in esame), ma svolge anche un ruolo di supporto per la tutela del patrimonio aziendale e per l'accertamento di illeciti.

Nel caso portato all'attenzione del Garante viene sottolineato dai ricorrenti *“l'impossibilità di esercitare in modo pieno e completo il diritto di accesso ex art. 15 del Regolamento relativamente al “trattamento dei dati personali e [al]le informazioni utilizzate al fine di elaborare i rimborsi chilometrici e la retribuzione mensile oraria nonché la logica di elaborazione”*. Altresì essi contestavano come la società non avesse dato riscontro alla loro richiesta dei *“documenti di autorizzazione in [...] possesso [della Società] con i quali viene formulata una informativa sul trattamento dei dati e del terminalino”*; nonché del *“contenuto del fascicolo personale, comprensivo del monitoraggio chilometrico della prestazione lavorativa, durata giornaliera della geolocalizzazione, nonché gli atti tutti che hanno riguardato la prestazione lavorativa in qualunque modo trattati e conservati”*. Al termine di una complessa istruttoria l'Autorità Garante contesta alla società datrice di lavoro di non aver fornito idoneo riscontro alle istanze di accesso realizzando una condotta illecita ex artt. 12 e 15 del Regolamento, sottolineando come *“la Società avrebbe dovuto fornire un completo riscontro alle istanze di esercizio del diritto di accesso anche comunicando i dati relativi alla geolocalizzazione dei reclamanti nonché le informazioni espressamente richieste”* e che *“neppure durante l'istruttoria condotta dall'Autorità la Società ha invece fornito un riscontro completo”*. Ne deriva la condanna della datrice di

lavoro al soddisfacimento delle richieste dei ricorrenti e la condanna della stessa ad una sanzione amministrativa ex art. 58, par. 2, lett. c) ed i) del Regolamento, quantificata in euro 20.000.

Il provvedimento citato evidenzia come la tecnologia digitale abbia inciso ridisegnando i modelli operativi delle imprese. Questa tendenza va però letta con “lenti bifocali” giacché permette di soddisfare vari interessi. Da un lato il ricorso agli strumenti digitali consente certamente di avere una maggior visibilità e, di conseguenza un controllo, sulle modalità operative dei propri lavoratori (purché nel rispetto del giusto bilanciamento dei diritti delle parti già richiamato), determinante in un frangente come l’attuale dove la tendenza è al posizionamento dei lavoratori fuori dagli spazi aziendali. Dall’altro non va sottaciuto che le informazioni aggiuntive reperibili con questi strumenti possono, allo stesso tempo, portare ad un miglioramento del servizio fornito dalle stesse imprese che, seppur a distanza possono esser in grado di intervenire se necessario, reimpostando il lavoro dei propri dipendenti, regolando ed affrontando i diversi problemi che si possono verificare, ovvero individuando o anticipando potenziali *fault*.

Il caso pone in evidenza come i sistemi di localizzazione dei veicoli nell’ambito del rapporto di lavoro coniugano esigenze organizzative, produttive, di sicurezza sul lavoro ed al contempo di protezione dei dati personali, all’interno di un perimetro contraddistinto da principi quali la necessità, la pertinenza e la non eccedenza⁹⁰.

Al tempo stesso l’atteggiamento della società datrice di lavoro richiama alla mente quello emerso nelle vicende affrontate nel caso Deliveroo dal Tribunale di Bologna, con la sentenza 31 dicembre 2020⁹¹. In quella occasione il giudicante sviluppò il suo ragionamento, rifacendosi a quanto contenuto del GDPR relativamente alla necessità, in sede di programmazione di un algoritmo, di valutare non solo l’efficacia del modello di calcolo, ma anche una serie di ulteriori elementi contingenti che possano condurre ad un pregiudizio nel corso dell’utilizzo di tale sistema automatizzato. Il richiamo è al *principio di privacy by design* citato all’art. 25 par. 1 ed in particolare ai diritti all’autodeterminazione informativa del singolo, quali, il diritto di accesso ai propri dati, il diritto di opposizione al loro trattamento, nonché il diritto alla cancellazione degli stessi.

Alla base del ragionamento vi è l’esigenza di garantire la conoscenza dello schema operativo dell’algoritmo (che vede e segue i lavoratori nell’esecuzione delle loro prestazioni), oltre che degli elementi di cui esso si compone, giacché solo questa conoscenza (fornita dal datore di lavoro) consente di concretizzare quel diritto di informativa dei lavoratori garantendo l’esigenza di trasparenza⁹² ed il bilanciamento degli

⁹⁰ <https://www.fiscoetasse.com/files/17119/garanteprivacy-9936174.pdf>

⁹¹ G. Fava, L’ordinanza del Tribunale di Bologna in merito alla possibile discriminatorietà dell’algoritmo utilizzato da Deliveroo, in *Lavoro Diritti Europa*, 2021, 1, in <https://www.lavorodirittieuropa.it/>

⁹² Cass. 25 maggio 2021, n. 14381, in I. FERRARI, *Indagine comparata sulla giurisprudenza in materia di responsabilità civile per i danni arrecati dall’uso dei sistemi di intelligenza artificiale*, in *LDE*, 2022, 3, 10; F. CASTAGNA, *Trasparenza Algoritmica e Validità del Consenso al Trattamento dei Dati Personali*, in *Responsabilità civile e Previdenza*, 2022, fasc. 1-2, p. 501; E.

interessi delle parti interessate. L'aspetto è cruciale poiché nel caso portato alla attenzione del giudice bolognese rilevò che il rifiuto di produrre il concreto meccanismo di funzionamento dell'algoritmo precludeva una più asserita disamina della questione non ottemperando al dovere di trasparenza previsto dall'art. 22 del GDPR⁹³.

6. Considerazioni conclusive

Volendo tracciare brevi considerazioni conclusive va evidenziato come questa riflessione intendesse soffermarsi a riflettere solo e limitatamente su alcuni aspetti delle sfide ed opportunità associate all'uso della IA⁹⁴ focalizzandosi sul delicato bilanciamento degli interessi contrapposti. Non v'è dubbio che questa influenzi i lavoratori che temono⁹⁵ lo spettro di macchine intelligenti⁹⁶. Prima di demonizzare questi sistemi sarebbe opportuno maturare una comprensione ed una conoscenza della IA⁹⁷ e delle modalità di incorporazione nei processi aziendali⁹⁸, poiché vi è la consapevolezza (nonostante i timori) che tale strumentazione migliori la produttività⁹⁹.

È pertanto fondamentale implementare un processo di formazione che avvicini ed accompagni gli operatori nell'uso aziendale quotidiano di queste applicazioni (tramite esperienze dirette con strumenti e tecniche di IA su problemi aziendali reali; istruendo e offrendo formazione ai talenti già esistenti; organizzando immersioni intensive per periodi ristretti; stimolando la comprensione delle basi di apprendimento automatico per esser in grado di identificare problemi, opportunità). Solo maturando un nuovo approccio verso le potenzialità organizzative sarà possibile attingere a piene mani dai benefici che essa (sostituendo a volte parti delle mansioni che i lavoratori vivono come banali e ripetitive) offre, consentendo il miglioramento delle prestazioni (proponendo mansioni più creative) grazie anche al cambiamento dei modelli esistenti¹⁰⁰.

Le esperienze sull'uso di tali strumenti hanno dimostrato come l'ingresso di meccanismi di automazione parziale per migliorare la produttività consenta di innescare processi di mutamento delle mansioni dei

MATTIOLI, *Dati personali: consenso validamente prestato solo se riferito a un trattamento specifico*, in *Diritto & Giustizia*, 2022, fasc. 105, p. 1.

⁹³ E. FALLETTI, *Discriminazione algoritmica*, cit., p. 274.

⁹⁴ S. RANSBOTHAM, P. GERBERT, M. REEVES, D. KIRON, M. SPIRA, *Artificial intelligence in business gets real, Pioneering Companies Aim for AI at Scale*, 2018, testo consultabile in <https://sloanreview.mit.edu/>

⁹⁵ OECD, *What happened to jobs at high risk of automation?* 2021, in <http://www.oecd.org/future-of-work/>

⁹⁶ A. SMITH, J. ANDERSON, *AI, Robotics, and the Future of Jobs*, Pew Research Center, 6 Agosto, 2014, testo consultabile in www.pewinternet.org.

⁹⁷ OECD, *Artificial Intelligence in Science: Challenges, Opportunities and the Future of Research*, OECD Publishing, 2023, Paris.

⁹⁸ S. RANSBOTHAM, D. KIRON, P. GERBERT, M. REEVES, *Reshaping business with artificial intelligence, Closing the Gap Between Ambition and Action*, 2017, testo consultabile in <https://sloanreview.mit.edu/>

⁹⁹ S. RANSBOTHAM, P. GERBERT, M. REEVES, D. KIRON, M. SPIRA, *Artificial intelligence in business*, cit. p. 31, con riguardo al caso Daimler.

¹⁰⁰ G. JOLLY, *Role of artificial intelligence the development of innovation*, testo consultabile in <https://www.theajhssr.com>



lavoratori attribuendo loro compiti diversi e di maggior valore supportati, appunto dalla tecnologia, oppure mansioni nuove abilitate proprio dall'innovazione¹⁰¹. Le incognite che accompagnano i lavoratori sono comprensibili ed occorre un periodo di maturazione degli aspetti ancora sconosciuti del fenomeno perché questo possa divenire il trampolino per proiettarsi verso il futuro. Si tratta di “automatizzare il facile” (affidando i compiti corrispondenti alla strumentazione digitale), “aumentando il difficile” (coniugando IA e lavoratori e portando ad una riqualificazione per migliorare le competenze dei lavoratori soddisfacendo la domanda di ruoli più qualificati). L'introduzione di un approccio attento a quanto delineato fino ad ora potrebbe avere positivi riguardo alla qualità del lavoro, gestendo i fattori di *stress* che l'ingresso dei nuovi strumenti comporta e soddisfacendo così nel contempo interessi economici, sociali ed anche ambientali¹⁰².

¹⁰¹ Vedi il caso dei bancari e l'avvio degli sportelli automatici in J. CONDEMI, *Che fine fa il diritto del lavoro se il tuo capo è un algoritmo*, in <https://valori.it/>

¹⁰² CENTRE CANADIENNE DE L'HYGIENE ET DE SECURITE AU TRAVAIL, *Intégration de nouvelles technologies en milieu de travail*, 2023, in www.cchst.ca