CENTRE FOR THE STUDY OF EUROPEAN LABOUR LAW "MASSIMO D'ANTONA"

Working Papers

Capitalismo digitale e controlli sulle attività telematiche dei lavoratori

WP CSDLE "Massimo D'Antona".IT – 458/2022

Università di Palermo
alessandro.riccobono@unipa.it

WP CSDLE MASSIMO D'ANTONA.IT - ISSN 1594-817X
Centre for the Study of European Labour Law "MASSIMO D'ANTONA" , University of Catania
On line journal, registered at Tribunale di Catania n. 1/2012 – 12.1.2012
Via Gallo, 25 – 95124 Catania (Italy)
Tel: +39 095230855 – Fax: +39 0952507020
csdle@lex.unict.it
http://csdle.lex.unict.it/workingpapers.aspx

Capitalismo digitale e controlli sulle attività telematiche dei lavoratori[α]

Alessandro Riccobono
Università di Palermo

[α] Il presente scritto è in corso di pubblicazione in M. Ricci, A. Olivieri (a cura di), *La tutela dei dati del lavoratore. Visibile e invisibile in una prospettiva comparata*, Cacucci, Bari, 2022.

1. Tecnica, tecnologia e controllo tecnologico nel capitalismo digitale.

L'impiego delle tecnologie avanzate al servizio dei rapporti di produzione è un elemento costante nel modello di sviluppo dei sistemi capitalistici contemporanei[1].

La «quarta rivoluzione industriale»[2], come la si suole chiamare, ha consentito di integrare gli oggetti fisici nelle reti informatiche: *internet* viene associato a macchine intelligenti che formano un *network* sofisticato, e ciò ha reso «il mondo reale un sistema informativo esteso», che permette di collegare le unità produttive in un unico sistema economico digitalizzato[3].

Non vi sono dubbi sul fatto che l'industrializzazione basata sull'*information and communication technology* (ICT) sia da considerare un fenomeno rivoluzionario e periodizzante.

Eppure la società civile ne ha rapidamente metabolizzato le coordinate essenziali, a partire dai riflessi sui modi di lavorare, che cominciano ad essere considerati parte integrante di una nuova modernità[4].

Termini come «internet delle cose», «*computer clouding*», «*machine learning*», «algoritmi» e «piattaforme digitali», fanno parte del lessico quotidiano di tutti i consociati[5]. E la percezione che i più moderni ritrovati della tecnica possano immagazzinare una enorme quantità di informazioni sulle persone che li adoperano appartiene alle dotazioni di senso comune di chiunque abbia maneggiato il più semplice degli *smartphone*.

Nel contesto delle relazioni di lavoro, l'avvento di nuovi modelli di *business* generati dal progresso tecnologico ha accentuato gli squilibri di potere socio-economico, consentendo un esercizio più intenso delle prerogative imprenditoriali[6]. L'integrazione tra il lavoro umano e le risorse

[1] R. BALDWIN, *Rivoluzione globotica. Globalizzazione, robotica e futuro del lavoro*, Bologna, 2020; A. CASILLI, *Schiavi del clic. Perché lavoriamo tutti per il nuovo capitalismo?*, Milano, 2020.
[2] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.
[3] Così M. WEISS, *Digitalizzazione: sfide e prospettive per il diritto del lavoro*, in *Dir. Rel. Ind.*, 2016, I, 251 ss.
[4] S. DHONDT, P. OEIJ, F.D. POT, *Digital transformation of work: spillover effects of workplace innovation on social innovation*, in U. HOWALDT, C. KALETKA, A. SCHRÖDER, *A Research Agenda for Social Innovation*, *Elgaronline*, 2021, 99 ss.
[5] R. SANTUCCI, *La quarta rivoluzione industriale e il controllo sui lavoratori*, in *Lav. Giur.*, 2021, 19 ss.
[6] T. TREU, *La digitalizzazione del lavoro: proposte europee e piste di ricerca*, in *Federalismi.it*, 2022, 190 ss.; A. PIZZOFERRATO, *Digitalisation of work: new challenges to labour law*, in *ADL*, 2021, 1329 ss.; S. MAINARDI, *Rivoluzione digitale e diritto del lavoro*, in *Mass. Giur. Lav.*, 2020, 341 ss.; E. BALLETTI, *I poteri del datore di lavoro tra legge e contratto,* in *Dir. Merc. Lav.*, 2018, 63 ss.

telematiche è così stretta che può arrivare a «catturare la vita della persona dentro il processo produttivo»[7].

Per dirla con *Shoshana Zuboff*, si assiste all'avanzata del «capitalismo digitale della sorveglianza», costruito sulle diseguaglianze sociali che la vasta gamma di strumenti capaci di estrarre informazioni e dati comportamentali sugli individui ha smisuratamente allargato[8].

All'interno di questo panorama è possibile cogliere una pluralità di aspetti che meritano attenzione, specialmente per le ricadute che presentano sulla regolazione dei rapporti di lavoro e sulle modalità di esercizio dei poteri tipici dell'imprenditore.

Un primo punto problematico è che i dati fluiscono comunemente tra dispositivi che possono prestarsi al tempo stesso a funzioni di lavoro, a funzioni di controllo, o a scopi di intrattenimento personale. Paradigmatico è il caso dei *social network*, che sono divenuti l'emblema di un'epoca in cui è possibile tenere una finestra sempre aperta sulla vita che i dipendenti conducono al di fuori dell'ambito professionale. La narrazione più benevola li considera strumenti di emancipazione avanzata per l'esercizio delle libertà democratiche, ma più spesso si tratta di «non-luoghi» in cui il principio della spersonalizzazione dei rapporti di lavoro è perennemente messo in discussione[9].

In seconda battuta occorre considerare che le tecnologie digitali hanno aperto la strada alla frammentazione multidimensionale di lavoro, consentendo il monitoraggio a distanza al di fuori degli ambienti fisici e attribuendovi carattere ubiquo[10]. L'esperienza del lavoro da remoto, che ha costituito la principale contromisura per fronteggiare l'emergenza pandemica[11], prelude allo sviluppo di un nuovo modello ibrido in cui trovarsi perennemente sotto controllo potrebbe essere il prezzo da pagare per la

[7] P. TULLINI, *La salvaguardia dei diritti fondamentali della persona che lavora nella gig-economy*, in *Costituzionalismo.it*, 2020, I, 41 ss.
[8] S. ZUBOFF, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019. Da ultimo l'espressione è stata ripresa da M.W. FINKIN, *The surveillance capitalism controversy*, 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*, Padova, 2022, 279 ss.
[9] A. TOPO, *Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore*, in C. PISANI, G. PROIA, A. TOPO (a cura di), *Privacy e lavoro*, cit., 439 ss., nonché, se si vuole, A. RICCOBONO, S. BOLOGNA, *What are you thinking about? freedom of expression and labour law in times of social networks*, in M. PALMA RAMALHO, C. CARVALHO, J. NUNES VICENTE, *Work in a digital era: legal challenges*, Lisbona, 2022, 627 ss.
[10] P. BOZZAO, *Lavoro subordinato, tempi e luoghi digitali*, in *Federalismi.it*, 2022, 106 ss.; M.T. CARINCI, A. INGRAO, *Il lavoro agile: criticità emergenti e proposte per una riforma*, in *Lab. & Law Issues*, 2021, 12 ss.; C. SPINELLI, *Tecnologie digitali e lavoro agile*, Cacucci, Bari, 2018.
[11] M. NICOLOSI, *Le sfide del lavoro agile dopo l'emergenza pandemica*, in A. GARILLI (a cura di) *Dall'emergenza al rilancio*, Torino, 2020, 91 ss.

flessibilità di lavorare da casa o da qualunque altra parte del mondo[12].

Vi è poi il variegato mondo del lavoro su piattaforma (*gig economy*, *sharing economy*, *on demand economy*)[13], dove le implicazioni del tracciamento *end-to-end* sono assai significative per via della fusione, in un unico dispositivo automatizzato, del centro di organizzazione, decisione e controllo della prestazione lavorativa[14]. Anche su questo versante le ricadute sono molteplici, a partire dal fatto che l'elaborazione algoritmica, sulla quale si basano la ripartizione delle occasioni di lavoro e le opportunità di guadagno, può alterare la giustizia distributiva negli scambi e facilitare le pratiche discriminatorie, occultandole dietro l'apparente neutralità delle formule matematiche[15].

Sarebbe tuttavia riduttivo considerare la digitalizzazione dell'economia un fenomeno limitato ai settori produttivi più sensibili all'innovazione tecnologica. I dati sono immanenti in ogni attività e le capacità rigenerative delle ICT hanno carattere universale: tale potenziale viene sfruttato in tutti i contesti e per tutte le tipologie di lavoro, fino a lambire anche i mestieri più tradizionali e meno qualificati[16]. Proprio in quest'ultimo ambito, peraltro, emerge il lato più insidioso della digitalizzazione: il progresso tecnologico può essere *skill based*, cioè correlato positivamente con la domanda di lavoro altamente qualificato, ma anche divenire un formidabile mezzo per parcellizzare l'attività umana e costringerla all'interno di schemi autoritativi e gerarchizzati. Quando ciò accade, come nel caso dei *rider* o dei «*mechanical turker*», si ripropongono modelli di divisione del lavoro di tipo neo-tayloristico, di cui il monitoraggio intensivo costituisce un ingranaggio tanto essenziale quanto minaccioso[17].

---

[12] R. DONNELLY, J. JOHNS, *Recontextualising remote working and its HRM in the digital economy: An integrated framework for theory and practice*, in *Int. Jour. of Human Resource Management*, 2021, 85 ss.

[13] C. CROUCH, *Se il lavoro si fa gig*, Bologna, 2019; A. DONINI, *Il lavoro attraverso le piattaforme digitali*, Bologna, 2019; J. PRASSL, *Humans as a Service. The Promise and Perils of Work in the Gig Economy*, Oxford University Press, 2018; D. WEIL, T. GOLDMAN, *Labor Standards, the Fissured Workplace, and the On-Demand Economy*, in *Perspectives on work*, 2016, 26 ss.

[14] V. DE STEFANO, A. ALOISI, *Il tuo capo è un algoritmo*, Bologna, 2020; E. DAGNINO, *Dalla fisica all'algoritmo: una prospettiva di analisi giuslavoristica*, Adapt University press, 2019.

[15] V. Trib. Bologna, 31 dicembre 2020, in *Dir. rel. ind.*, 2021, 204 ss., con nota di M. FAIOLI, *Discriminazioni digitali e tutela giudiziaria su iniziativa delle organizzazioni sindacali*, che ha qualificato come antisindacale il comportamento di una nota piattaforma del *food delivery* che penalizzava nell'elaborazione del *ranking* reputazionale i ciclofattorini indisponibili a rispondere alle chiamate, perché impegnati in manifestazioni di protesta sindacale. Da ultimo. Trib. Palermo 12 aprile 2021, in *Lav. giur.*, 2021, 859 ss., con nota di S. BATTISTELLI, *Discriminazione per ragioni di affiliazione sindacale: il caso dei rider*.

[16] J. CRUZ VILLALÒN, *Le trasformazioni delle relazioni industriali di fronte alla digitalizzazione dell'economia*, in *Giorn. Dir. Lav. Rel. Ind*., 2018, 465 ss.

[17] G. RITZER, *La McDonaldizzazione del mondo nella società digitale,* Milano, 2020; A. BELLAVISTA, *Sorveglianza sui lavoratori, protezione dei dati personali ed azione collettiva*

2. I controlli sulle attività telematiche dei lavoratori e l'art. 4 Stat lav.: tra lavoro subordinato, *smart working* e lavoro tramite piattaforme digitali.

In questo scritto saranno presi in considerazione i principali problemi giuridici sollevati dalla sorveglianza digitale nel contesto sopra descritto.

L'area di interesse è quella delle «attività telematiche dei lavoratori»: locuzione qui intesa in chiave meramente stipulativa, che può essere utilizzata per riassumere le diverse situazioni in cui lo svolgimento di operazioni digitali che generano dati, informazioni e ogni altro elemento di interesse, anche se riguardante la vita privata del lavoratore, possa interferire con la dimensione dello scambio contrattuale e con le aspettative di riservatezza della persona che lavora.

La casistica più ricorrente riguarda il controllo delle *email* e degli accessi a *internet*, spesso associati alle pratiche di *cyberloafing* o *cyberslacking*[18]. Ma vi rientrano anche il monitoraggio via GPS o tramite tecnologie a ultrasuoni, così come le verifiche biometriche o per mezzo di *software* per il riconoscimento facciale[19].

L'analisi di queste fattispecie sarà condotta alla luce dell'art. 4 della l. n. 300/1970[20], che fornisce la cornice regolativa generale entro cui

nell'economia digitale, in C. ALESSI, M. BARBERA, L. GUAGLIANONE, *Impresa, lavoro e non lavoro nell'economia digitale*, Bari, 2019, 151 ss.

[18] Cioè l'uso del *web* per acquisti, intrattenimento, *social networking* e scambio di messaggi a contenuto privato durante l'orario di lavoro. Cfr. DEL PUNTA, *Social Media and Workers' Rights: What Is at Stake?*, in *Int. Journ. of Comparative Lab. Law and Ind. Rel*., 2019, 79 ss.

[19] G. ZICCARDI, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *Lab. & Law Issues*, 2016, 48 ss.

[20] La bibliografia sulla novella della disciplina statutaria, operata dall'art. 23 del d.lgs. 14 settembre 2015, n. 151, e successivamente dall'art. 5, comma 2, d.lgs. 24 settembre 2016, n. 185, è molto vasta. Cfr., limitatamente alle opere monografiche più recenti, A. SARTORI, *Il controllo tecnologico sui lavoratori. La nuova disciplina italiana tra vincoli sovranazionali e modelli comparati*, Torino, 2020; A. INGRAO, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci, Bari, 2018; V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, Editoriale scientifica, Napoli, 2018. Si v. altresì, 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*, cit., 329 ss.; A. MARESCA, *I controlli tecnologici a distanza*, in *Lav. prev. oggi*, 2021, 1 ss.; A. INGRAO, *Il potere di controllo a distanza sull'attività lavorativa e la nuova disciplina della privacy nella sfida delle nuove* tecnologie, in G. LUDOVICO, F.F. ORTEGA, T.C. NAHAS (a cura di), *Nuove tecnologie e diritto del lavoro*, Milano, 2021, 111; A. TROJSI, *Potere informatico del datore di lavoro e controllo sui lavoratori, cinquant'anni dopo*, in *Dirittifondamentali.it*, 2020, 1411 ss.; M.T. CARINCI, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in P. TULLINI (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 45 ss.; P. LAMBERTUCCI, I *poteri del datore di lavoro nello Statuto dei lavoratori dopo l'attuazione del c.d. Jobs Act del 2015: primi spunti di riflessione*, in *Arg. dir. lav*., 2016, I, 514 ss.; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015),* in

ricomporre l'equilibrio tra l'interesse del datore di lavoro al buon funzionamento dell'organizzazione imprenditoriale e i diritti della personalità del lavoratore.

La disciplina dello Statuto, in particolare, sarà utilizzata come chiave di lettura unitaria per trattare le questioni che accomunano i rapporti di lavoro *standard* a quelli di nuova generazione, come lo *smart working* e il lavoro tramite piattaforme digitali.

A questo proposito basti ricordare che il raggio operativo dell'art. 4 si estende al di là dell'idealtipo per cui è stato pensato, cioè il lavoro dipendente prestato all'interno della fabbrica novecentesca[21].

Nella specie, per quanto riguarda il «lavoro agile» il dettato statutario trova integrale applicazione grazie all'art. 21 della l. n. 81/2017: è vero infatti che tale disposizione rimette all'accordo fra le parti «la disciplina dell'esercizio del potere di controllo sull'attività resa dal lavoratore all'esterno dei locali aziendali», ma ciò deve avvenire «nel rispetto di quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300». Dal che si desume che l'autonomia individuale non è abilitata a disporre delle garanzie ivi previste, se non per irrobustirle a vantaggio del lavoratore[22].

Inoltre, l'art. 12.3 del Protocollo sul lavoro agile per il settore privato, sottoscritto in data 7 dicembre 2021, ribadisce la piena operatività del Regolamento 2016/679/EU (da ora anche GDPR), al cui interno è codificato il principio per cui il consenso dell'interessato non può costituire una legittima base del trattamento dei dati personali nelle situazioni in cui sussista uno squilibrio di potere contrattuale fra le parti[23]. Il che è quanto

---

Riv. it. dir. lav., 2016, I, 77; A. BELLAVISTA, *Il nuovo art. 4 dello Statuto dei lavoratori,* in G. ZILIO GRANDI, M. BIASI (a cura di), *Commentario breve alla riforma "Jobs Act"*, Milano, 2016, 717; C. ZOLI, *Il controllo a distanza dell'attivita dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970,* in *Var. Temi Dir. Lav.,* 2016, 635 ss.; M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *ADL,* 2016, I, 483; I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Lab. & Law issues*, 2016, 1 ss.; V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *ADL* 2015, 1186 ss.

[21] Da ultimo S. SCIARRA, *Diritti e poteri nei luoghi di lavoro. Una lettura dello Statuto dei lavoratori nel tempo della pandemia*, in *Moneta e Credito*, 2021, 11 ss.

[22] A. BELLAVISTA, *Il potere di controllo sul lavoratore e la tutela della riservatezza*, in G. ZILIO GRANDI, M. BIASI (a cura di), *Commentario breve allo statuto del lavoro autonomo e del lavoro agile*, Milano, 2018, 621 ss.; S. MAINARDI, *Il potere disciplinare e di controllo sulla prestazione del lavoratore agile*, in L. FIORILLO, A. PERULLI (a cura di), *Jobs act del lavoro autonomo e del lavoro agile*, Torino, 2018, 223 ss. Dubitativamente A. PESSI, *I controlli dell'imprenditore nel lavoro agile e nel lavoro tramite piattaforma*, in C. PISANI, G. PROIA, A. TOPO (a cura di), *Privacy e lavoro*, cit., 530.

[23] Cfr. il *Considerando* n. 43 e l'art. 4, par. 1, n. 11 del GDPR, su cui cfr. da ultimo *European Data Protection Board*, *Linee guida sul consenso,* n. 5/2020*,* dove si ribadisce il principio per cui, nella maggior parte dei casi, il consenso del lavoratore non può considerarsi «libero,

accade nel contesto occupazionale, dove il consenso del prestatore di lavoro gioca un ruolo marginale, *a fortiori* per ciò che riguarda l'attivazione dei sistemi di monitoraggio a distanza[24].

Quanto sopra indica che le sfide poste dalla crescente diffusione del lavoro da remoto non riguardano tanto le regole applicabili ai controlli tecnologici, quanto la difficoltà di delimitare l'estensione del potere da cui tali controlli promanano, tenuto conto della commistione tra tempi di lavoro e tempi di riposo cui dà vita la *homebody economy*[25]. Non per caso il tema su cui più si discute riguarda l'effettività del cosiddetto diritto alla disconnessione, nella consapevolezza che le risposte sinora fornite dal legislatore nazionale[26] e dal citato Protocollo[27] non appaiono esaustive.

Sicché, in attesa che si compia l'iniziativa europea finalizzata ad introdurre «norme e condizioni minime» per garantire che tale diritto possa essere esercitato efficacemente[28], il principale baluardo contro il rischio che il lavoratore a distanza sia considerato «*always on*» – e dunque sempre

specifico, informato e inequivocabile». Per un'applicazione in concreto v. l'ordinanza ingiunzione del Garante per la protezione dei dati personali, 28 ottobre 2021, 384.

[24] In generale, sull'inderogabilità della disciplina dei controlli a distanza e sull'indisponibilità delle relative garanzie da parte dell'autonomia individuale, va richiamato il consolidato orientamento della magistratura penale secondo cui l'inosservanza dell'*iter* procedimentale prescritto dall'art. 4 Stat. Lav. – cui consegue la sanzione penale *ex* artt. 171, d.lgs. n. 196/2003 e 38 St. lav. – non può essere in alcun modo sanata attraverso la stipulazione di un accordo scritto fra il datore di lavoro e tutti i dipendenti, dovendosi presumere che la dichiarazione di questi ultimi non sia genuina, alla luce dello squilibrio di potere contrattuale fra le parti del rapporto. Cfr. Cass. pen., sez. III, 17 gennaio 2020, n. 1733, in *Guida al lav*., 2020, n. 6, 50, con nota di M. DELLE CAVE, *Installazione di telecamere, il consenso dei dipendenti non basta per evitare il reato*; Cass. pen., sez. III, 17 dicembre 2019, n. 50919, in *Lav. giur*., 2020, p. 1, con nota di G. TAIANI, *Violazione dell'art. 4 St. lav. e consenso del lavoratore*.

[25] V. BAVARO, *Questioni in diritto su lavoro digitale, tempo e libertà*, in *Riv. Giur. Lav.*, 2018, I, 38.

[26] Va qui ricordato che l'art. 2 del d.l. 13 marzo 2021, n. 30, conv. dalla l. 6 maggio 2021 n. 61, ha riconosciuto il diritto del lavoratore agile «alla disconnessione dalle strumentazioni tecnologiche e dalle piattaforme informatiche, nel rispetto degli eventuali accordi sottoscritti dalle parti e fatti salvi eventuali periodi di reperibilità concordati». Ma si tratta di una previsione collocata nel contesto della legislazione emergenziale, che sconta il limite della transitorietà. Cfr. P. BOZZAO, *Lavoro subordinato, tempi e luoghi digitali*, in *Federalismi.it*, cit., 116. Critica rispetto alla disposizione anche R. ZUCARO, *Il diritto alla disconnessione. Nuove modalità di tutela della qualità del tempo di vita nella prospettiva giuslavoristica*, in *Lav. Dir. Europa*, 2022, 1 ss.

[27] Anche in questo caso le previsioni appaiono piuttosto generiche, specialmente per ciò che riguarda la variante del lavoro agile per «obbiettivi», dove un intervento più deciso sarebbe stato necessario, tenuto conto che in questo caso il rischio di commistione tra tempi produttivi e tempi liberi è certamente maggiore di quello che si prospetta nella variante «a tempo».

[28] Cfr. la Risoluzione del parlamento Europeo del 21 gennaio 2021, recante *Raccomandazioni alla Commissione sul diritto alla disconnessione*, 2019/2181/INL, su cui E. FIATA, *L'iniziativa europea sul diritto alla disconnessione*, in *Lav. Dir. Europa*, 2021, 1 ss.

monitorabile – rimane la contrattazione collettiva. E qui gli attori sindacali hanno già dato prova di saper allestire valide soluzioni[29].

Più complessa è l'individuazione dei limiti alla sorveglianza algoritmica nel lavoro tramite piattaforme digitali, dove l'applicazione dell'art. 4 Stat. Lav. deve fronteggiare lo stress *test* sulla qualificazione del rapporto, che costituisce problema comune nel panorama internazionale[30].

In ambito domestico la disciplina delle collaborazioni etero-organizzate *ex* art. 2 del d.lgs. n. 81/2015 è esplicitamente applicabile anche ai lavoratori delle piattaforme, e costituisce lo strumento principale per l'esportazione delle tutele dello Statuto nella zona grigia tra autonomia e subordinazione.

Non a caso, la giurisprudenza sinora pronunciatasi sulla saga dei ciclofattorini ha chiarito che l'esercizio dei poteri di direzione e controllo attraverso il *management* algoritmico va considerato un equivalente funzionale dell'uso delle prerogative unilaterali da parte di un datore di lavoro umano, quale che sia la natura della relazione contrattuale controversa[31]. A tale indirizzo ha fatto eco anche il Garante per la protezione dei dati personali, che ha ulteriormente allargato il raggio operativo dell'art. 4 Stat. Lav., sottolineando come le garanzie ivi previste rientrino fra i livelli minimi di tutela che l'ordinamento riconosce anche ai *rider* autonomi *ex* art. 47-*quater*, d.lgs. n. 81/2015[32].

A monte di questi interventi, peraltro, non va trascurato che l'uso del trattamento algoritmico è sottoposto al limite generale di cui all'art. 22 del GDPR, che sancisce il divieto delle decisioni basate unicamente su trattamenti automatizzati, anche ai fini della profilazione, quando da ciò

[29] Cfr. i casi citati da A. LEVI, *tempo di lavoro, digitalizzazione e diritto alla disconnessione, tra vecchie esigenze di tutela e nuove modalità' di protezione*, in corso di pubblicazione in *Studi in onore di A. Garilli*.

[30] Il tema è centrale nella proposta di Direttiva della Commissione UE sul miglioramento delle condizioni di lavoro nelle piattaforme, COM (2021) 762, su cui M. BARBIERI, *Prime osservazioni sulla proposta di direttiva per il miglioramento delle condizioni di lavoro nel lavoro con piattaforma*, in *Lab. & Law. Issues*, 2021, 3 ss.; S. GIUBBONI, *La proposta di direttiva della Commissione europea sul lavoro tramite piattaforma digitale*, in *www.eticaeconomia.it*, Menabò, 16 gennaio 2022.

[31] F. CARINCI, *Il percorso giurisprudenziale sui rider. Da Tribunale Torino 7 maggio 2018 a Tribunale Palermo 24 novembre 2020, ADL*, 2021, 1 ss. Cfr., da ultimo, Trib. Torino, 18 novembre 2021, in *Labor,* 2022, 213, con nota di A. GARILLI, C. DE MARCO, *La qualificazione del lavoro dei rider: ancora una volta il giudice accerta la subordinazione e individua nella piattaforma interponente il reale datore di lavoro*. Ancora più recente, Trib. Milano, 20 aprile 2022, n. 1018, *inedita*.

[32] Cfr. Garante per la protezione dei dati personali, ord. ingiunzione 10 giugno 2021, n. 234.

derivino conseguenze giuridiche sull'interessato o altri effetti che incidano in modo significativo sulla sua persona[33].

Ciò comporta che qualsiasi decisione basata su algoritmi digitali, per essere lecita, deve incorporare almeno in parte il contributo umano, in modo tale che il lavoratore possa comprenderne il significato ed eventualmente contestarla, secondo una logica che oppone il controllo democratico al determinismo tecnologico[34].

Si tratta di una importante limitazione al potere del titolare del trattamento, la cui funzione, già oggetto di interventi da parte del Garante *privacy*[35], ha cominciato ad essere valorizzata anche dalla giurisprudenza nazionale, che si è dimostrata particolarmente attenta all'esigenza di garantire pratiche di monitoraggio etico e trasparente, a tutela dei diritti fondamentali della persona[36].

3. Le attività telematiche tra strumenti di lavoro e strumenti di controllo.

È opinione condivisa che la riscrittura in chiave evolutiva dell'art. 4 Stat. Lav. abbia apportato elementi di maggiore flessibilità al sistema dei controlli a distanza, pur senza intaccare il divieto di sorveglianza anelastica e fine a sé stessa dell'attività dei lavoratori[37].

Segnatamente, l'attuale disciplina continua a basarsi sul modello generale della procedimentalizzazione del potere datoriale, il cui esercizio è sottoposto al doppio vincolo della co-determinazione (tramite accordo sindacale o autorizzazione amministrativa)[38] e della ricorrenza di specifici presupposti giustificativi per «l'installazione di impianti audiovisivi o di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» (art. 4, comma 1)[39].

---

[33] Sul rischio che tali strumenti spingano gli svantaggiati sempre più in basso nella piramide sociale, cfr. G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Il Mulino*, 2019, 199 ss.

[34] Cfr. Gruppo di lavoro art. 29, *Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione*, 3 ottobre 2017, in *https://ec.europa.eu/*.

[35] V. Autorità garante per il trattamento dei dati personali, 11 ottobre 2018, n. 467, che prescrive l'obbligo di sottoporre a valutazione di impatto *ex* art. 35, comma 4, del Regolamento (UE) n. 2016/679, i trattamenti automatizzati.

[36] Da ultimo cfr. Cass. 25 maggio 2021 n. 14381, in *Riv. giur. lav.*, 2021, II, 441 ss., con nota di C. DE MARCO, *Algoritmi reputazionali e consenso validamente prestato*.

[37] M. RICCI, *I controlli a distanza dei lavoratori tra istanze di revisione e flessibilità "nel lavoro"*, in *ADL*, 2016, I, 740 ss.; C. ZOLI, Il *controllo a distanza dell'attività dei lavoratori e la nuova struttura dell'art. 4, legge n. 300/1970*, in *Var. Temi Dir. Lav.*, 2016, 635 ss.

[38] Su cui v. E. VILLA, *Accordo sindacale e procedura amministrativa nei controlli a distanza dei lavoratori*, in *Var. temi. Dir. Lav.*, 2016, 707 ss.

[39] La nozione di attività dei lavoratori, come è noto, non coincide con quella di attività lavorativa, avendo portata più ampia, cioè comprensiva sia delle condotte solutorie sia di

Il controllo diretto e subdolo rimane dunque vietato, mentre continua ad essere ammesso quello preterintenzionale, quale conseguenza indiretta del ricorso di «esigenze organizzative, produttive e di sicurezza del lavoro», cui la novella ha aggiunto anche la «tutela del patrimonio aziendale».

Soltanto per «gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa» e per quelli di «registrazione degli accessi e delle presenze» non è richiesto alcun filtro autorizzativo, delineandosi in tal modo un'area residuale in cui il controllo incidentale è libero, o per meglio dire giustificato *in re ipsa*, promanando da apparecchiature tecnologiche direttamente integrate nel processo produttivo (art. 4, comma 2).

La distinzione tra «strumenti di controllo» e «strumenti di lavoro» assume un peso determinante ai fini dell'individuazione dei limiti al monitoraggio a distanza, ma quando il *focus* è centrato sulle attività telematiche si incontra uno specifico elemento di complicazione.

Ed infatti, poiché l'infrastruttura della società dell'informazione è essenzialmente costituita dall'apporto di mezzi telematici, accade sempre più spesso che il lavoratore sia allo stesso tempo soggetto attivo, che si avvale di una connessione informatica per intervenire sul processo produttivo, e soggetto passivo, che può subirne la forza intrusiva.

Sui criteri che permettono di distinguere gli strumenti di lavoro da quelli di controllo il panorama interpretativo è assai vario.

La posizione più liberista suggerisce di qualificare come strumento di lavoro qualsiasi dispositivo tecnologico che assolva una funzione in senso lato prestazionale: vi rientrerebbero cioè anche le risorse ausiliarie, che vengono fornite al personale per migliorare la produttività o l'efficienza[40].

In un contesto in cui la realtà materiale e quella digitale si autoalimentano, una simile opzione non è condivisibile: essa porterebbe alla rapida neutralizzazione dello spazio applicativo dell'art. 4, comma 1, alterando il rapporto regola-eccezione con il comma 2.

Ancor meno convincente è la tesi per cui lo strumento di lavoro sarebbe quello identificato come tale dal datore di lavoro nell'esercizio del potere direttivo[41]: se così fosse, il creditore della prestazione potrebbe

---

quelle non direttamente strumentali all'adempimento, come le cosiddette licenze comportamentali o le pause. V. in tal senso Cass. 3 luglio 2001, n. 8998, in *Notiz. Giur. Lav.*, 2002, 34.

[40] Così PISANI, *Gli strumenti utilizzati per rendere la prestazione lavorativa e quelli di registrazione degli accessi e delle presenze*, cit., 446; G. PROIA, *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione*), cit. 329. In giurisprudenza la tesi è accolta da Trib. La Spezia, ord., 25 novembre 2016, in *Notiz. Giur. Lav.*, 2017, 16, che ha considerato strumento di lavoro *ex* art. 4, comma 2, la tessera *Viacard* utilizzata dal lavoratore per effettuare pagamenti ai caselli autostradali.

[41] In tal senso A. MARESCA, *I controlli tecnologici a distanza*, cit., 10 ss. In termini simili anche E. GRAGNOLI, *Gli strumenti di controllo e i mezzi di produzione*, in *Var. Temi Dir. Lav.*, 2016,

disapplicare a proprio piacimento le garanzie poste a tutela del contraente debole, disponendo di una normativa che si è già ricordato essere inderogabile *in peius*.

In mezzo si colloca l'opinione, senz'altro più persuasiva, secondo cui non esiste una definizione ontologica dello strumento di lavoro, dovendosi procedere volta per volta mediante un approccio ermeneutico a geometria variabile[42]: gli *hardware* e i *software* diffusi negli ambienti di lavoro hanno carattere polifunzionale e si prestano ad usi promiscui, per cui l'individuazione di ciò che è funzionale all'adempimento varia a seconda del tipo di mansione e dell'organizzazione aziendale[43].

I *social network*, ad esempio, possono essere considerati strumenti di lavoro per coloro che svolgono mansioni di *social media manager* o curano il *web marketing* per conto di imprese o personaggi famosi. Allo stesso modo, le *chat online* potrebbero esserlo per quanti vengano adibiti ai servizi di *customer care* allestiti direttamente sul *web* dalle grandi multinazionali[44].

Più difficile giungere alla medesima conclusione quando le *community virtuali* siano utilizzate per favorire la condivisione o l'interscambio di informazioni in ambito aziendale, anche se un recente pronunciamento della Corte di Cassazione sembra aprire prospettive in tal senso[45].

Questo non significa che la classificazione debba fondarsi su basi essenzialmente casistiche, restando affidata al libero apprezzamento dell'interprete.

Nella *law in action* – che in questa materia è frutto dell'integrazione sinergica tra il formante giurisprudenziale, le pronunce del Garante per la protezione dei dati personali e le prescrizioni delle altre autorità amministrative (Ispettorato e Ministero del lavoro) – si è infatti suggerito il fondamentale criterio-guida per cui gli «strumenti di lavoro» sono

651; A. INGRAO, *Il potere di controllo a distanza sull'attività lavorativa e la nuova disciplina della* privacy, cit., 124.

[42] Così M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, cit., 488.

[43] In questo senso Trib. Torino 19 settembre 2018, n. 1664, in *Riv. it. dir. lav.*, 2019, II, 9 con nota di C. CRISCUOLO, *Potere di controllo e computer aziendale.*

[44] E. ROCCHINI, *Social network e controlli a distanza. Alla ricerca di un difficile equilibrio*, in *Mass. Giur. Lav.*, 2019, 143 ss.; M. FORLIVESI, *Il controllo della vita del lavoratore attraverso i social network*, in P. TULLINI (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, 2017, 37.

[45] Cass. 22 settembre 2021, n. 25731, in *Dejure*, che in un *obiter dictum* ha qualificato la chat aziendale via *whatsapp* come strumento funzionale alla prestazione lavorativa. V. però Trib. Milano 24 ottobre 2017, in *Dir. rel. ind.*, 2019, II, 303, con nota di G. CASSANO, *Prime pronunce sul nuovo art. 4 l. n. 300/1970*, che ha considerato *whatsapp* strumento di controllo *ex* art., 4, comma 1, per assenza della sua strumentalità rispetto all'adempimento della prestazione lavorativa.

esclusivamente quelli indispensabili per l'esatto adempimento della prestazione lavorativa[46].

Nel regime residuale di cui all'art. 4, comma 2, rientrano pertanto i soli dispositivi tecnologici senza i quali il lavoratore non potrebbe utilmente assolvere gli obblighi contrattuali[47].

Tendenzialmente si possono considerare strumenti di lavoro il *pc* aziendale, il sistema operativo, l'antivirus, il *browser internet* e il *client* di posta elettronica aziendale[48]: ancorché si tratti di *hardware* e *software* che consentono di incamerare dati informatici, essi rientrano nell'area di esenzione dalla procedura co-determinativa prevista dall'art. 4, comma 1, ferme restando le garanzie sancite dal comma 3 per il trattamento e l'utilizzabilità delle informazioni raccolte, di cui si dirà *infra*[49].

In casi più circoscritti, anche i dispositivi per la raccolta e il trattamento di dati biometrici possono essere considerati indispensabili ai fini dell'adempimento: l'Ispettorato Nazionale del Lavoro, ad esempio, ha ritenuto sottratta ai vincoli autorizzativi l'installazione di sistemi di riconoscimento biometrico per l'avviamento delle macchine di lavoro, laddove tale scelta risponda all'esigenza di impedire l'accesso di soggetti non autorizzati ad aree in cui sia necessario assicurare elevati e specifici livelli di sicurezza, e sempre che sia rispettato il criterio dell'*extrema ratio*

[46] Cfr. la Relazione del Garante per la protezione dei dati personali, 28 giugno 2016, *Relazione annuale per l'anno 2015*; Ispettorato nazionale del lavoro, circolare 7 novembre 2016, n. 2 e circolare 26 luglio 2017, n. 4; Ministero del Lavoro, nota 18 giugno 2015.

[47] Per questa tesi cfr. A. BELLAVISTA, *Il nuovo art. 4 dello Statuto dei lavoratori,* cit., 717; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza*, cit., 77; M.T. CARINCI, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, cit., 45 ss.

[48] Qualifica l'*email* aziendale come strumento di lavoro Trib. Roma, 24 marzo 2017, in *Dir. rel. ind.*, 2018, 265, con nota di E. GRAMANO, *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi*. La *email* privata del dipendente non può ovviamente costituire strumento di lavoro. Sul punto va altresì precisato che i messaggi trasmessi tramite applicazioni di messaggistica e coperti da password o filtri *privacy* sono inutilizzabili: contenuto dei dati esteriori delle comunicazioni e *file* allegati sono coperti dalle garanzie costituzionali in tema di segretezza della corrispondenza personale, sicché il datore non potrebbe sottoporli ad attività di controllo, quand'anche l'invio avvenga dal luogo di lavoro. Cfr. Cass. 10 settembre 2018, n. 21965, in *Riv. giur. lav.*, 2018, II, 477, con nota di S. BINI, *Offese reali in contesti virtuali: social network e limiti al diritto di critica*. V. anche I. PICCININI, M. ISCERI, *Questioni attuali sul potere di vigilanza e controllo del datore*, in *Lav. dir. Europa*, 4/2021, 1 ss.; C. CRISCUOLO, *Il controllo sugli account di posta elettronica e di messaging aziendale*, in *Riv. It. Dir. Lav*., 2016, 284 ss.

[49] Per i principi cui si deve allineare il datore di lavoro nel trattamento dei dati personali mediante posta elettronica, v. Garante per la protezione dei dati personali, 22 dicembre 2016, n. 547; Garante per la protezione dei dati personali, 1 febbraio 2018, n. 53, nonché le linee guida emanate con delibera 1 marzo 2007, n. 13. V. sul punto C. CARTA, I *limiti al potere di controllo sui lavoratori nell'uso di internet e dei servizi di comunicazione elettronica: per un diritto alla moderazione*, in *Labor*, 2018, 467 ss.

nel trattamento dei dati relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona[50].

Si giunge invece a conclusioni diverse quando sugli strumenti di lavoro vengano installate componenti aggiuntive che operano in funzione di tracciamento dell'attività posta in essere dal lavoratore: tali sono i *proxy server* per il monitoraggio della navigazione *internet*[51] o della posta elettronica aziendale[52], ma anche le applicazioni che rilevano se i dipendenti sono connessi alla rete aziendale e lavorano[53], o ancora quelle che registrano le sequenze di tasti e i movimenti del *mouse*, o che riflettono lo schermo dei dipendenti per proiettarlo direttamente sulla scrivania del datore di lavoro[54].

Il criterio interpretativo finora seguito va utilizzato anche per le tecnologie di geolocalizzazione satellitare, che in linea di massima non costituiscono strumenti per rendere la prestazione lavorativa[55], nemmeno

[50] Cfr. Ispettorato Nazionale del Lavoro, circolare 19 febbraio 2018, n. 5, che richiama il Provvedimento generale prescrittivo in tema di biometria emanato dal Garante per la protezione dei dati personali del 12 novembre 2014. Sul punto va altresì osservato che l'utilizzo della verifica biometrica non è ammesso ai fini del controllo generalizzato dell'accesso ai luoghi di lavoro e della rilevazione delle presenze in servizio. Cfr. Garante per la protezione dei dati personali, ordinanze ingiunzioni 14 gennaio 2021, n. 16; 22 maggio 2018, n. 331 e 1 marzo 2018, n. 124. Si v. altresì il Parere 19 settembre 2019, n. 167, che ha censurato per gli stessi motivi lo schema di regolamento di attuazione dell'art. 2, l. 19 giugno 2019, n. 56 (cd. «Legge Concretezza»).

[51] Garante per la protezione dei dati personali, 13 maggio 2021, n. 190; Garante per la protezione dei dati personali, 5 febbraio 2015, n. 65. Nel precedente quadro normativo, l'obbligo di seguire la procedura codeterminativa per il monitoraggio dei dati di traffico *internet* era stato affermato da Cass. 19 settembre 2016, n. 18302, in *Dejure*, e da Cass.1 ottobre 2012, n. 16622, in *Lav. Giur.*, 2013, 383, con nota di E. BARRACO, A. SITZIA, *Un* de profundis *per i "controlli difensivi" del datore di lavoro?*. V. anche Cass. 23 febbraio 2010, n. 4375, in *Riv. giur. Lav.*, 2010, II, 462, con nota di A. BELLAVISTA, *La Cassazione e i controlli a distanza sui lavoratori*.

[52] Garante per la protezione dei dati personali, 13 luglio 2016, n. 303, che ha censurato l'utilizzo, da parte di un'università italiana, di un *software* che permetteva il monitoraggio massivo delle attività telematiche (internet e posta elettronica) poste in essere dai dipendenti.

[53] Garante per la protezione dei dati personali, 8 marzo 2018, n. 13, che ha considerato strumento di controllo e non di lavoro il *software* «Arcadia», impiegato dai lavoratori addetti ad *un call center* per la gestione del servizio clienti di una grande società di telecomunicazioni. Diverso il caso dei *dialer* che permettono il mero smistamento delle telefonate dal centralino, qualificati come strumento di lavoro da Trib. Pescara, 25 ottobre 2017, *Dejure*.

[54] Prima della riforma dell'art. 4 Stat. Lav., Cass. 9 febbraio 2016, n. 2531, in *Mass. Giur. Lav.*, 2016, 299, aveva ritenuto necessaria l'autorizzazione sindacale o amministrativa per l'uso di un *software* attraverso cui Poste Italiane poteva monitorare in tempo reale le operazioni compiute dagli addetti allo sportello, attraverso il *mirroring* dello schermo.

[55] V. Ispettorato Nazionale del Lavoro, circolare 7 novembre 2016, cit., secondo cui il GPS può essere considerato strumento di lavoro, esentato dalle regole dell'art. 4, comma 1, Stat. Lav., soltanto in casi eccezionali, quando ad esempio l'installazione sia richiesta da specifiche normative di carattere legislativo o regolamentare (es. uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00, ecc.). In senso analogo, Garante per la protezione

se integrati nelle applicazioni delle piattaforme digitali o negli *smart weareable*[56]*:* anche in questi casi si tratta di dispositivi che normalmente «eccedono le necessità immediate della prestazione»[57], venendo installati per soddisfare l'interesse datoriale all'incremento delle *performance* lavorative, con finalità di controllo aggiuntivo sul *quantum* della prestazione.

Nei casi sopra esaminati, pertanto, sebbene lo strumento di lavoro e quello di controllo possano risultare compenetrati in un'unica risorsa digitale multifunzione, occorrerà rispettare i vincoli procedurali e finalistici dell'art. 4, comma 1, pena l'inutilizzabilità dei dati raccolti e l'illiceità dell'attività di monitoraggio, tuttora assistita dalla sanzione penale *ex* art. 38 Stat. Lav.

4. L'obbligo di adeguata informazione e i principi conformativi dell'ordinamento *privacy*.

A prescindere dalla qualificazione che si attribuisca allo strumento informatico – «di lavoro» o «di controllo» – l'utilizzabilità dei dati raccolti «per tutti i fini connessi al rapporto di lavoro», quindi anche disciplinari[58], è subordinata ai vincoli posti dal nuovo art. 4, comma 3 dello Statuto.

Ivi è previsto che il lavoratore debba essere adeguatamente informato sulle «modalità d'uso degli strumenti e di effettuazione dei controlli», e che il trattamento dei dati avvenga «nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196»[59].

La previsione ha decretato in modo esplicito l'integrazione fra l'ordinamento giuslavoristico e l'ordinamento *privacy*[60], riconoscendo nella disciplina sulla protezione dei dati personali l'elemento di chiusura del sistema: l'operatività di tale normativa è piena e generalizzata, ma la sua centralità si manifesta soprattutto nell'area del controllo libero *ex* art. 4,

---

dei dati personali, 16 marzo 2017, n. 138. Prima della riforma dell'art. 4, l'obbligo di assoggettare l'installazione del GPS alla procedura codeterminativa era stato affermato da Cass. 5 ottobre 2016, n. 19922, in *Mass. Giur. Lav.,* 2017, 48 ss., con nota di G. VIDIRI, *I controlli a distanza prima e dopo il Jobs Act*.

[56] *Contra*, R. DI MEO, *Tecnologie e poteri datoriali: commento a margine del c.d. braccialetto Amazon*, in *Labour & Law Issues*, 2018, 1 ss.; A. INGRAO, *Il braccialetto elettronico tra privacy e sicurezza del lavoratore*, in *Dir. Rel. Ind.*, 2019, I, 895 ss.

[57] A. INGRAO, *Il controllo a distanza sulla prestazione del ciclo fattorini tra Scoober App e GPS*, in *Labour & Law Issues*, 2021, 168.

[58] In tal senso, espressamente, Cass. 9 novembre 2021, n. 32760, in *Guida al lav.*, 2021, 32, con nota di G. DE FAZIO, *Il datore può controllare il computer aziendale del dipendente anche per fini disciplinari.*

[59] Oggi da leggere alla luce del d.lgs. 10 agosto 2018, n. 101, di adeguamento al GDPR.

[60] La qual cosa si poteva già desumere nel precedente quadro normativo, cfr. A. BELLAVISTA, *I poteri dell'imprenditore e la privacy del lavoratore*, in *Dir. lav.*, 2003, 169 ss.

comma 2, dove le regole poste a tutela della riservatezza definiscono i confini della legittima acquisizione dei dati riguardanti l'attività lavorativa e ne condizionano l'utilizzabilità anche in sede processuale. Il che costituisce, *de facto*, il principale (se non l'unico) presidio a difesa del lavoratore che si avvalga di strumenti telematici direttamente funzionali all'adempimento[61].

Sebbene si riscontri una diffusa tendenza a distinguere l'attività di controllo (art. 4, commi 1 e 2) dal regime di utilizzabilità dei dati raccolti (art. 4, comma 3)[62], è preferibile ritenere che il nesso «controlli-*privacy*» si sviluppi all'interno di una relazione circolare: le regole per il monitoraggio tecnologico e quelle per il trattamento dei dati personali si tengono e si condizionano a vicenda, perché il controllo a distanza costituisce esso stesso una forma di «trattamento automatizzato» di dati personali dei lavoratori[63].

Da ciò alcuni corollari di rilievo per il tema che si sta trattando.

Innanzitutto va precisato che il monitoraggio sulle attività telematiche dei lavoratori deve essere sempre preceduto dall'adeguata informazione sulle modalità d'uso degli strumenti e di effettuazione dei controlli. Non è infatti condivisibile la tesi per cui l'informativa potrebbe essere resa anche in un momento successivo alla raccolta dei dati, afferendo al momento, solo eventuale, in cui insorga l'interesse aziendale all'utilizzo dei dati raccolti[64].

Se così fosse, l'obbligo di informare il lavoratore della possibilità di essere sottoposto a controllo sarebbe *inutiliter dato*, risolvendosi in un avviso «a cose fatte», con intuibili ripercussioni laddove le informazioni raccolte all'insaputa dell'interessato rilevino sul piano disciplinare.

Al contrario, le metodologie di acquisizione, conservazione e utilizzazione dei dati personali devono essere prevedibili, cioè in grado di garantire la ragionevole aspettativa alla *privacy* dell'interessato. E ciò in

[61] Nel regime generale di cui all'art. 4, comma 1, invece, la disciplina della *privacy* costituisce un secondo filtro, che si aggiunge all'obbligo di rispettare le condizioni autorizzatorie per l'installazione degli strumenti di controllo a distanza, dalla cui inosservanza la giurisprudenza faceva già discendere l'inutilizzabilità delle informazioni raccolte. Cfr., da ultimo, Trib. Roma, 13 giugno 2018, in *Riv. Giur. Lav*., 2018, II, 62, con nota di M. VERZARO, *Controlli tecnologici e utilizzabilità dei dati acquisiti.*

[62] I. ALVINO, *I nuovi limiti al controllo «a distanza» dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, cit. 15 ss.; G. PROIA, *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione)*, cit., 335; A. MARESCA, *I controlli tecnologici a distanza*, cit., 3 ss.

[63] A. INGRAO, *Il potere di controllo a distanza*, cit., 119.

[64] A. MARESCA, *I controlli tecnologici a distanza*, cit., 16. G. PROIA, *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione)*, cit., 338.

linea con la filosofia del GDPR, che si ispira al modello prevenzionistico della normativa in tema di salute e sicurezza sui luoghi di lavoro.

L'informazione *ex* art. 4, comma 3, va dunque fornita in un momento necessariamente antecedente all'inizio della raccolta dei dati, in modo che la funzione investigativa delle tecnologie di monitoraggio sia contenuta a vantaggio di quella deterrente/pedagogica. In tal senso si sono recentemente espressi sia la Corte di Cassazione[65], sia il Garante per la protezione dei dati personali[66], in conformità all'orientamento già espresso dalla Corte Edu nel celebre caso *Bărbulescu*[67].

Va poi considerato che l'obbligo di adeguata informazione sui controlli è inscindibilmente legato all'informativa sul trattamento dei dati personali *ex* artt. 13 e 14 del GDPR (già art. 13 del codice della *privacy*).

Sebbene si tratti di due adempimenti diversi[68], nulla vieta che le «modalità d'uso degli strumenti e di effettuazione dei controlli» e le «finalità e le modalità del trattamento cui sono destinati i dati» vengano esplicitate in un unico documento, da redigere nel rispetto dei principi conformativi di «trasparenza», «correttezza», «pertinenza», «minimizzazione» e «responsabilizzazione» (art. 5 GDPR e 11 d.lgs. n. 196/2003)[69].

Il contenuto dell'informativa deve dunque risultare, nella sua interezza, chiaro e formulato con linguaggio semplice (art. 12 GDPR), specificare le finalità e i mezzi utilizzati per il trattamento dei dati e indicare chi vi ha accesso e in quali circostanze, dando corpo al principio di *accountability* che grava sul responsabile del trattamento (art. 24 GDPR).

Tutto ciò, se da una parte induce a ritenere che il documento debba essere personalizzato in base alla tipologia di strumento informatico con

[65] Cass. 22 settembre 2021, n. 25731, in *Dejure*, che ha ritenuto inutilizzabili per finalità disciplinari le informazioni tratte da una *chat* aziendale, destinata alle comunicazioni di servizio dei dipendenti, in assenza di adeguata informazione preventiva fornita ai lavoratori circa la possibilità di controllo.

[66] Cfr. Ordinanza ingiunzione 15 aprile 2021, n. 137 e Ordinanza ingiunzione 13 maggio 2021, n. 197, con cui è stato censurato l'operato di alcune imprese che avevano monitorato l'attività telematica dei propri dipendenti senza aver fornito, in anticipo, informazioni chiare e mirate su fini e mezzi del tracciamento a distanza. Sul punto v. A. SITZIA, *Lavoro, controlli e privacy: un nouveau parcours per il test di bilanciamento nell'elaborazione della Sezione Lavoro (e del Garante Privacy)*, in *Mass. Giur. Lav.,* 2021, 957 ss.

[67] C. Edu, Grande Chambre, 5 settembre 2017, *Bărbulescu v. Romania*, che ha ravvisato la violazione dell'art. 8 della CEDU in relazione all'assenza di una chiara informazione preventiva sull'attività di monitoraggio svolta da un'impresa sulle conversazioni informatiche intrattenute da un dipendente con la fidanzata durante l'orario di lavoro.

[68] G. PROIA, *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza fare confusione)*, cit., 344.

[69] Cass., 10 novembre 2017, n. 26682, con nota di A. LEVI, *Il controllo difensivo a distanza e l'inoperatività dell'art. 4 dello Statuto*, in *Lav. giur.*, 2018, 5.

cui possa entrare in contatto il lavoratore[70], dall'altra consente di affermare che i dati raccolti non potranno essere trattati e utilizzati in sede disciplinare, laddove il datore di lavoro non abbia indicato tale possibilità tra gli scopi del monitoraggio[71].

5. Attività telematiche e controlli difensivi.

La disciplina dell'art. 4 Stat. Lav. entra in sofferenza quando è chiamata a confrontarsi con la sua nemesi, rappresentata dalla categoria dei «controlli difensivi».

Come è noto, con tale espressione viene identificata una tipologia di controlli occulti storicamente sottratta al campo di applicazione dell'art. 4 dello Statuto, in quanto rispondente allo scopo di accertare comportamenti illeciti del lavoratore, diversi dai meri inadempimenti[72].

L'inapplicabilità delle garanzie statutarie viene generalmente motivata facendo perno sull'esigenza di proteggere il patrimonio aziendale da attacchi improvvisi e imprevedibili ad opera di dipendenti infedeli[73]: in questa prospettiva i controlli difensivi vengono considerati una forma di legittima difesa del datore di lavoro, da collocare all'esterno del dettato statutario per via della difficoltà di conciliare i tempi del confronto sindacale o amministrativo con l'interesse alla protezione immediata del diritto di proprietà[74].

---

[70] Trib. Vicenza 28 ottobre 2019, in *Dejure*; Trib. Torino 19 settembre 2018, n. 1664, in *Il Giuslavorista*, con nota di S. APA, *Disciplina dei controllo sui lavoratori e adeguatezza dell'informativa*, secondo cui «l'informativa non deve ridursi ad un adempimento formale rivolto alla generalità dei lavoratori, ma deve essere esaustiva e adeguata e tale non può essere considerata l'indicazione di istruzioni relative all'uso dello strumento tecnologico, non accompagnate dalla specifica individuazione delle modalità di utilizzo che comportano l'acquisizione dei dati».

[71] Cass. 22 settembre 2021, n. 25731, cit., secondo cui l'obbligo di adeguata informazione non può considerarsi assolto mediante l'elaborazione di un regolamento aziendale che preveda la mera possibilità da parte del datore di lavoro di accedere alla *chat* aziendale in caso di interventi di manutenzione, senza nulla specificare circa le modalità e le finalità di esecuzione dei controlli. V. anche, per un caso in cui l'informativa è stata considerata adeguata, Trib. Savona, 1 marzo 2018, in *Riv. giur. lav.*, 2018, II, 574 ss., con nota di G. BANDELLONI, *Le nuove regole del controllo a distanza sulla prestazione lavorativa.*

[72] Con massima ricorrente la S.C. afferma che tale tipo di controlli non può essere utilizzato per contestare al lavoratore mere violazioni dell'obbligo di diligenza, essendo la categoria deputata a tutelare beni estranei al rapporto di lavoro. Per un riepilogo v. la rassegna a cura di G. CASSANO, *I controlli ex art. 4, L. n. 300/1970*, in *Lav. giur.*, 2020, 778 ss.

[73] La nozione di patrimonio aziendale è stata intesa in senso ampio, comprensivo cioè delle componenti materiali e immateriali, ma anche dell'immagine dell'impresa e della sua reputazione commerciale.

[74] Da ultimo V. MAIO, *I controlli difensivi a tutela del patrimonio aziendale*, in C. PISANI, G. PROIA, A. TOPO (a cura di), *Privacy e lavoro*, cit., 412 ss.

Da qui la loro legittimazione in forma clandestina, *a fortiori* quando il datore li attivi *ex post*, ovvero in seguito all'insorgere di elementi indiziari a carico del lavoratore[75].

Sebbene la giurisprudenza vi abbia dato ampio credito, anche in sede penale[76], l'indirizzo è sempre stato molto controverso, esponendosi a numerose obiezioni che non è qui possibile ripercorrere.

Merita però di essere segnalata l'aporia di fondo della teoria dei controlli difensivi, vale a dire l'artificiosità della distinzione tra la sorveglianza finalizzata alla tutela dei beni aziendali (ammessa al di fuori dei vincoli dell'art. 4 Stat. Lav.) e quella focalizzata sull'esecuzione della prestazione (vietata in via generale dalla medesima disposizione).

La dottrina più accorta ha sottolineato come sia assai difficile che un illecito extracontrattuale non integri allo stesso tempo una negligenza nell'adempimento: gli illeciti sul lavoro sono tendenzialmente plurioffensivi, sicché ammettere il controllo occulto per proteggere beni estranei al contratto significa autorizzare anche il controllo latente sull'attività dei lavoratori, aggirando il divieto posto dal dettato statutario[77].

Quanto detto trova una conferma lampante nella casistica in tema di controlli sulle attività telematiche dei lavoratori.

La Corte di Cassazione ha ad esempio escluso dall'ambito di applicazione del previgente art. 4 dello Statuto: 1) l'estrazione della cronologia dei siti *web* visitati da una lavoratrice durante l'orario di servizio, dalla quale era emerso l'accesso prolungato a numerosi siti *internet* estranei all'ambito lavorativo[78]; 2) il controllo effettuato sui dati del GPS installato sulla vettura aziendale affidata ad un operaio di un'impresa di servizi ambientali, che si era più volte allontanato dall'area di sua

[75] *Ex multis*, Cass. 23 febbraio 2012, n. 2722, in *Riv. giur. lav.*, 2012, II, 740, con nota di G. GOLISANO, *Controllo della posta elettronica e accertamento ex post degli abusi del dipendente*; Cass. 28 maggio 2018, n. 13266, in *Foro it*., 2018, I , 2357.

[76] Da ultimo Cass. pen., Sez. III, 27 gennaio 2021, n. 3255, in *Dejure,* secondo cui non integra il reato contravvenzionale previsto dagli artt. 4 e 38 dello Statuto dei lavoratori l'installazione di impianti audiovisivi diretti a tutelare il patrimonio aziendale da comportamenti illeciti dei dipendenti, anche in caso di assenza dell'accordo con le rappresentanze sindacali e dell'autorizzazione dell'Ispettorato del lavoro, con conseguente utilizzabilità dei dati acquisiti come mezzo di prova nel processo a carico del lavoratore.

[77] P. LAMBERTUCCI, I *poteri del datore di lavoro nello Statuto dei lavoratori dopo l'attuazione del c.d. Jobs Act del 2015: primi spunti di riflessione*, cit., 514 ss.; P. TULLINI, *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, in *Riv. it. dir. lav.*, 2011, II, 89 ss.; A. BELLAVISTA, *La Cassazione e i controlli a distanza sui lavoratori*, cit., 462.

[78] Cass. 1 febbraio 2019, n. 3133, in *Riv. it. dir. lav*., 2019, II, 414, con nota di A. INGRAO, *Il potere di controllo a distanza sull'ozio telematico e il limite del diritto alla privacy del lavoratore*.

competenza per intrattenersi al bar oltre il limite delle pause dal lavoro[79]; 3) la creazione di un falso profilo femminile su *Facebook*, utilizzato dal datore di lavoro come agente provocatore nei confronti di un lavoratore sospettato di aver navigato sui *social* mentre era in servizio, mettendo a rischio il regolare funzionamento della sicurezza degli impianti aziendali[80].

Si tratta di vicende che dimostrano in modo paradigmatico come i controlli finalizzati ad accertare condotte illecite siano tendenzialmente anche controlli diretti sull'attività dei lavoratori, a conferma che molto spesso il danno arrecato alla proprietà d'impresa costituisce il naturale prodotto del non lavorare per dedicarsi ad altro.

Il che è la migliore testimonianza della caducità della teoria dei controlli difensivi.

Con l'inserimento della «tutela del patrimonio aziendale» fra le causali che consentono il controllo a distanza *ex* art. 4, comma 1, la questione avrebbe dovuto considerarsi risolta nel senso dell'assorbimento dei controlli difensivi nella disciplina statutaria[81]. Ciò, per inciso, avrebbe reso del tutto irrilevante la distinzione tra illeciti contrattuali ed *extra* lavorativi.

Su tale conclusione, tuttavia, permangono forti divergenze tra gli interpreti. Anzi, le prime decisioni della Corte di Cassazione sul nuovo testo dell'art. 4 Stat. Lav. sembrano minimizzare l'impatto della riforma, prodigandosi nel tentativo di ritagliare una zona franca in cui i controlli difensivi possano continuare ad esprimere la loro inalterata vitalità[82].

---

[79] Cass. 12 ottobre 2015, n. 20440, in *Riv. it. dir. lav.*, 2016, II, 249, con nota di M. AVOGARO, *Abbandono ingiustificato del lavoro, gps e investigatori privati tra controlli difensivi e Jobs Act.*

[80] Cass. 27 maggio 2015, n. 10955, in *ADL*, 2015, II, 1303, con nota di F. OLIVELLI, *Lo "stratagemma" di facebook come controllo difensivo occulto: provocazione o tutela del patrimonio aziendale?,* e in *Riv. it. dir. lav.*, 2015, II, 984, con nota di M. FALSONE, *L'infelice giurisprudenza in materia di controlli occulti e le prospettive del suo superamento.*

[81] R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro* cit., 82; C. ZOLI, Il *controllo a distanza dell'attività dei lavoratori*, cit., 641; A. BELLAVISTA, *Il nuovo art. 4 dello Statuto dei lavoratori,* cit., 722.

[82] Si tratta di Cass. 12 novembre 2021, n. 34092, in *Guida al lav.* 2021, f. 49, 41, con nota di A STANCHI, *Sorveglianza digitale. Osservazioni al risorgere dei controlli difensivi sugli illeciti del lavoratore*, relativa al licenziamento di un *manager* aziendale accusato di aver diffuso via email informazioni finanziarie riservate, la cui colpevolezza era stata accertata in seguito ad un *alert* del sistema informatico, che aveva indotto il datore ad avviare un controllo sui file di *log* contenuti nel suo pc. Identica l'impostazione seguita da Cass. 22 settembre 2021, n. 25732, in *Riv. Giur. Lav.*, 2022, II, 11 ss., con nota di G. BANDELLONI, *Controllo a distanza: la giurisprudenza di legittimità fa il punto sulle nozioni di adeguata informativa e di controllo difensivo*, in cui si discuteva della legittimità del controllo informatico operato sul pc aziendale in uso ad una lavoratrice, poi licenziata per aver navigato su internet per scopi privati, scaricando un allegato contenente un *virus* che aveva contaminato la rete aziendale. Su tale pronuncia v. anche i commenti di E. GRAMANO, *Controlli difensivi, condotte illecite e inadempimento del prestatore di lavoro: un cerchio che non si chiude* in *Dir. rel. ind.*, 2022, II, 272; C. COLAPIETRO, A. GIUBILEI, *Controlli difensivi e tutela dei dati dellavoratore: il nuovo*

Ancora una volta gli interventi della giurisprudenza scaturiscono da vicende in cui la sorveglianza occulta era stata attivata per sanzionare dipendenti sospettati di aver compiuto attività telematiche illecite sul posto di lavoro.

Secondo la Cassazione i controlli difensivi attivabili previo accordo sindacale o autorizzazione amministrativa sono esclusivamente quelli «in senso lato», «vale a dire quelli 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».

Questi ultimi vanno distinti dai controlli difensivi «in senso stretto», cioè quelli disposti al fine accertare, anche tramite apparecchiature tecnologiche, condotte illecite del singolo, di cui il datore sospetta in base a concreti indizi: questi ultimi continuano ad essere leciti in deroga alle garanzie statutarie, in quanto non aventi ad oggetto la normale attività dei lavoratori[83].

Per supportare siffatta ricostruzione la S.C. richiama diffusamente la giurisprudenza della Corte EDU relativa ai casi *López Ribalda* e *Bărbulescu*, dove il controllo difensivo mirato è stato ammesso previo superamento di un articolato *test* di bilanciamento tra interesse aziendale e dignità dei lavoratori, elaborato allo scopo di individuare i margini di compatibilità della sorveglianza occulta rispetto al diritto alla riservatezza protetto dall'art. 8 della Convenzione Europea dei Diritti dell'Uomo.

Quest'ultimo aspetto, al quale i primi commentatori delle citate pronunce hanno attribuito particolare risalto[84], non sembra in realtà costituire una novità così dirompente: al di là delle riserve che può suscitare l'utilizzo della giurisprudenza EDU in chiave ablativa delle garanzie previste dall'art. 4 Stat. Lav.[85], va osservato che l'obbligo di limitare l'indagine a distanza allo stretto indispensabile figura da tempo tra le condizioni poste dalla Cassazione per legittimare la sorveglianza tecnologica occulta. Sul piano applicativo, infatti, il «decalogo di cautele»[86]

punto della Cassazione, in *Labour & Law Issues*, 2021, 189 ss.; D. CONTE, *Primi arresti della Cassazione sul nuovo art. 4 dello Statuto dei Lavoratori: è cambiato tutto…anzi quasi nulla?*, in *Lav. Prev. Oggi*, 2021, 771 ss.

[83] In dottrina questa lettura è proposta da A. MARESCA, *I controlli tecnologici a distanza*, cit., 6.

[84] La soluzione della S.C. viene presentata come frutto di un'interpretazione «convenzionalmente orientata» da A. SITZIA, *Lavoro, controlli e privacy: un* nouveau parcours *per il test di bilanciamento nell'elaborazione della Sezione Lavoro (e del Garante Privacy)*, cit., 968 ss.

[85] V. al riguardo il contributo di A. BELLAVISTA in *q. Volume*

[86] C. Edu, Grande Chambre, 5 settembre 2017, *Bărbulescu*, cit., punti 121 e 122, su cui F. BUFFA, Il *controllo datoriale delle comunicazioni elettroniche del lavoratore dopo la sentenza Barbulescu 2 della Cedu*, in *Questione giustizia*, 18 ottobre 2017.

discendenti dall'art. 8 della Convenzione EDU riproduce in larga parte i principi postulati dalla disciplina sul trattamento dei dati personali di fonte UE, la cui osservanza era già stata ritenuta indispensabile nei numerosi pronunciamenti intervenuti sul testo previgente dell'art. 4 Stat. Lav.[87].

Un più netto segnale di discontinuità rispetto al passato va invece colto nell'ulteriore passaggio argomentativo con cui la S.C. chiarisce che i controlli difensivi «in senso stretto» sono leciti solo se attivati «*ex post*».

Anche in questo caso non si è in presenza di una condizione nuova, trattandosi di un requisito che la stessa Corte aveva già utilizzato in alcune occasioni precedenti. Questa volta però viene specificato che il sospetto sull'operato del lavoratore non consente di avviare indagini «di carattere retrospettivo»[88], consistenti cioè nella lettura e analisi di informazioni già raccolte e conservate preventivamente. Diversamente il datore di lavoro «potrebbe acquisire per lungo tempo ed ininterrottamente ogni tipologia di dato, provvedendo alla relativa conservazione, e, poi, invocare la natura mirata (*ex post*) del controllo incentrato sull'esame ed analisi di quei dati»[89].

La precisazione è apprezzabile, perché intende superare il classico problema logico per cui l'accertamento *a-posteriori* finisce per giustificare il controllo tecnologico già avvenuto, autorizzando lo scorrimento a ritroso di informazioni incamerate all'insaputa del lavoratore.

Le nuove decisioni della S.C. puntualizzano dunque che la natura e*x post* del controllo sussiste «solo ove, a seguito del fondato sospetto del datore circa la commissione di illeciti ad opera del lavoratore, il datore stesso provveda, da quel momento, alla raccolta delle informazioni».

Si deve cioè trattare di una verifica prospettica, che viene disposta per confermare la fondatezza degli indizi di colpevolezza attraverso l'acquisizione di dati informatici nuovi e non preesistenti[90].

Siffatta impostazione presenta importanti ricadute sull'onere della prova a carico del datore di lavoro, che dovrà dimostrare di avere attivato

[87] V. ad esempio Cass. 1 agosto 2013, n. 18443, in *Nuova Giur. Civ. Comm.*, 2014, 103, con nota di A. SITZIA, *I «controlli tecnologici» del datore di lavoro tra necessità e proporzionalità. Chiare indicazioni lavoristiche dalla prima sezione civile,* e Cass. 3 novembre 2016, n. 22313, in *ADL*, 2017, II, 441, con nota di C. FAVRETTO *Controlli difensivi sul pc aziendale: l'area grigia della libertà e della dignità del lavoratore quale limite al potere datoriale*, in cui vengono richiamati i principi di proporzionalità, selettività e durata del controllo per il periodo strettamente necessario, affinché la reazione datoriale non sia eccedente rispetto all'offesa subìta.

[88] Cfr. *supra* nt. 77.

[89] Così Cass. 12 novembre 2021, n. 34092, cit.

[90] V. ancora Cass. 12 novembre 2021, n. 34092, cit., secondo cui «nel classico esempio dei dati di traffico contenuti nel browser del pc in uso al dipendente, potrà parlarsi di controllo *ex post* solo in relazione a quelli raccolti dopo l'insorgenza del sospetto di avvenuta commissione di illeciti ad opera del dipendente, non in relazione a quelli già registrati».

il controllo come conseguenza di un indizio maturato *aliunde*, vale a dire con modalità diverse dal monitoraggio tecnologico: solo per fare un esempio, appare chiaro che il sospetto sull'utilizzo di *internet* per finalità extralavorative non potrà essere dimostrato sulla base del controllo effettuato sul pc aziendale, perché altrimenti la giustificazione dell'indagine a distanza avrebbe carattere circolare e il tracciamento delle attività informatiche poste in essere dal lavoratore non sarebbe più *ex post* ma a ritroso.

Sotto questo profilo il campo di operatività della sorveglianza occulta viene opportunamente ridimensionato, riflettendo una maggiore attenzione per i diritti della personalità di chi lavora.

Resta tuttavia da chiedersi se abbia senso l'insistenza con cui la giurisprudenza rivitalizza ciclicamente la categoria dei controlli difensivi estranei al perimetro dello Statuto.

Se è chiara l'esigenza di giustizia sostanziale che ne costituisce il fondamento – non potendosi negare la responsabilità del lavoratore dinnanzi all'evidenza di un illecito – rimane nondimeno oscura la scelta di perseguire tale finalità attraverso soluzioni ermeneutiche che non trovano corrispondenza nel diritto positivo.

Al netto dei correttivi proposti, la dicotomia «controlli difensivi in senso ampio/controlli difensivi in senso stretto» appare forzata e in qualche modo ipocrita, perché sovrappone il punto di vista dell'interprete a quello del legislatore, svalutando l'ampliamento dei presupposti giustificativi del controllo a distanza operato dalla riforma del 2015.

In atto la materia dei controlli è assoggettata alla disciplina auto-conclusa dell'art. 4 Stat. Lav., che assicura protezione anche all'interesse difensivo del patrimonio aziendale latamente inteso, bilanciandolo con una serie di garanzie poste a tutela della riservatezza del lavoratore.

È vero che la riforma ha allargato le possibilità di utilizzo degli elementi raccolti tramite gli strumenti di controllo, consentendo di indirizzarli anche alla verifica dell'esatto adempimento o della commissione di un illecito[91]. Ma la contropartita di tale estensione è costituita dall'irrinunciabile diritto del lavoratore di essere adeguatamente informato circa la possibilità di essere sottoposto a controllo, circa le modalità con cui questo viene effettuato, e circa gli scopi per cui le informazioni verranno raccolte e potranno essere utilizzate: diritto che obbliga il datore di lavoro a predisporre un'apposita *policy* aziendale in difetto della quale nessun controllo potrà considerarsi legittimo, a prescindere dal fatto che venga

[91] In tal senso anche l'*obiter dictum* contenuto in Cass. 9 novembre 2021, n.32760, in *Dejure*, secondo cui «dopo il cd. *Jobs Act*, gli elementi raccolti tramite tali strumenti (*ex* art. 4, commi 1 e 2, *ndr*) possono essere utilizzati anche per verificare la diligenza del dipendente nello svolgimento del proprio lavoro, con tutti i risvolti disciplinari e di altra natura connessi».

realizzato tramite apparecchiature di monitoraggio *tout court* ovvero tramite strumenti per rendere la prestazione lavorativa o per registrare le presenze[92].

Non occorrono macchinosi distinguo tra controlli generalizzati e controlli mirati, né è necessario investire la magistratura del delicato compito di operare il bilanciamento mobile tra i diversi valori in gioco: l'art. 4 dello Statuto fornisce un elenco tipico e tassativo delle finalità che giustificano il controllo, per cui se il datore di lavoro vuole difendersi ricorrendo alla tecnologia può farlo, ma deve seguire modalità che riflettono il punto di equilibrio tra interessi contrapposti predeterminato *ex ante* dal legislatore.

6. Osservazioni conclusive.

Se è vero che il progresso tecnologico ha intensificato le opportunità di sorveglianza dei dipendenti, modificando le culture aziendali e rendendo le pratiche di monitoraggio uno strumento per ottenere vantaggi competitivi, non va dimenticato che la costruzione di un ecosistema digitale equo e sostenibile risponde all'interesse di entrambe le parti del rapporto di lavoro[93].

La necessità che le imprese definiscano politiche chiare, che governino il modo in cui viene effettuato il monitoraggio e che ne prevengano l'uso improprio e l'abuso, è questione che non riguarda soltanto i valori della dignità e della riservatezza della persona che lavora.

La letteratura aziendalistica segnala che le forme di sorveglianza intensiva riducono l'autonomia operativa e la fiducia nel *management* aziendale, rivelandosi controproducenti per la stessa funzionalità delle imprese[94]: poiché il monitoraggio può «meta comunicare» i sistemi di valori organizzativi ai dipendenti, la sua estremizzazione può essere vissuta come

[92] Non si condivide pertanto l'opinione di A. SITZIA, *Lavoro, controlli e privacy*, cit., 972, secondo cui il diritto alla trasparenza è recessivo di fronte all'esigenza di reprimere un atto illecito, fermo restando il bilanciamento tra le modalità del controllo occulto e l'esigenza di non comprimere del tutto la dignità del lavoratore.

[93] V. da ultimo l'Accordo Quadro delle Parti Sociali Europee sulla Digitalizzazione, stipulato il 22 giugno 2020, dove si sottolinea che «è nell'interesse dei datori di lavoro e dei lavoratori adattare l'organizzazione del lavoro, ove necessario, alla continua trasformazione del lavoro derivante dall'utilizzo di dispositivi di lavoro digitali».

[94] M. ABRAHAM, C. NIESSEN, C. SCHNABEL, K. LOREK, V. GRIMM, K. MÖSLEIN, M. WREDE, *Electronic monitoring at work: The role of attitudes, functions, and perceived control for the acceptance of tracking technologies*, in *Hum. Resour. Manag. J.*, 2019, 657 ss.

una messa in discussione delle loro competenze e del loro impegno organizzativo, disincentivandone il rendimento e la produttività[95].

Per evitare questo effetto collaterale, si suggerisce di promuovere il coinvolgimento dei dipendenti nella progettazione dei sistemi di monitoraggio, anche attraverso la mediazione delle rappresentanze collettive, valutando l'impatto delle strategie di *co-design* come componente di primaria rilevanza per la realizzazione di un ambiente di lavoro *privacy friendly*.

D'altra parte, l'attuale formulazione dell'art. 4 Stat. Lav. non esclude che la protezione sindacale rientri in gioco anche nelle ipotesi in cui la codeterminazione non costituisce un requisito di legittimità per l'esercizio del potere di controllo: laddove i rapporti di forza lo consentano, nulla vieta che le parti sociali contribuiscano a definire, soprattutto in sede di contrattazione aziendale, quali siano gli strumenti funzionali all'esercizio delle mansioni *ex* art. 4, comma 2, stabilizzando il segmento più complesso della vigilanza sulle attività informatiche e telematiche.

In questa prospettiva il contropotere collettivo potrebbe operare come fondamentale valvola di adattamento del diritto alle conquiste della tecnica, assicurando che le opportunità da essa offerte non conducano ad accettare il controllo capillare, sul lavoro e nella vita, come parte integrante di una società sempre più de-umanizzata.

[95] K. BALL, *Electronic Monitoring and Surveillance in the Workplace. Literature review and policy recommendations*, Publications Office of the European Union, Luxembourg, 2021, 11 ss.