LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 3 / 2020
(estratto)

Giuseppe Busia

Così vicini, così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente

Così vicini, così distanti: i controlli da remoto del datore di lavoro e la riservatezza del dipendente

Giuseppe Busia[1]

1. Lo Statuto dei lavoratori ... quando ancora non esisteva la privacy

Pochi contesti, quanto quello lavorativo, mostrano l'esigenza pressante di garantire la tutela della riservatezza e la protezione dei dati personali. Sul luogo di lavoro la conoscenza di informazioni riguardanti il lavoratore da parte del datore di lavoro accresce notevolmente l'influenza di quest'ultimo, finendo per accentuare lo squilibrio di potere che caratterizza fisiologicamente il rapporto fra le parti. Non è quindi un caso se, nel nostro Paese, le prime disposizioni in materia di tutela della riservatezza sono state introdotte proprio con riferimento all'ambito lavorativo, attraverso lo Statuto dei lavoratori del 1970: da questo punto di vista, si può arrivare a sostenere che la tutela dei dati personali del lavoratore ha in qualche modo preceduto quella del consumatore e quella del cittadino.

La ricostruzione storica della disciplina in materia di protezione dei dati personali nel nostro ordinamento evidenzia, dunque, il peso di una tardiva positivizzazione, avvenuta solo con la legge del 31 dicembre 1996, n. 675, in recepimento della direttiva 95/46/CE.

Sebbene l'esigenza di garantire la riservatezza della persona alla stregua di un diritto inviolabile *ex se*, indipendentemente dalla condizione personale e sociale dell'interessato, fosse fortemente avvertita nel corpo sociale – tanto da trovare ampio riconoscimento nel diritto pretorio e finanche nei noti pronunciamenti della Corte Costituzionale del 12 aprile 1973, n. 38 – l'introduzione di tale diritto si è posta, in un primo momento, in una posizione strettamente funzionale all'attuazione del mercato unico comunitario[2]: la prima legge organica in materia di protezione dei dati, infatti, venne

[1] Le osservazioni fatte e le opinioni espresse hanno carattere puramente personale e non impegnano in alcun modo il Garante per la protezione dei dati personali, presso cui l'avv. Giuseppe Busia, nel momento in cui si scrive, svolge le funzioni di Segretario generale.

2 Va infatti ricordato che la legge n. 675/1996, di recepimento della direttiva 95/46/CE, ha rappresentato un passo obbligato per il legislatore nazionale anche per il fatto che l'introduzione del diritto alla protezione dei dati personali nel nostro ordinamento era legato altresì alla piena applicazione dell'Accordo di Schengen, volto a creare uno spazio comune per la libera circolazione di lavoratori, beni, servizi e capitali, attraverso la progressiva soppressione dei controlli alle frontiere (mentre l'autorizzazione alla ratifica dell'Accordo di Schengen del 14 giugno 1985 era stata resa dall'Italia con la l. n. 338/1993). Senza il recepimento della direttiva citata, infatti, l'Italia non avrebbe potuto fare parte dell'area Schengen.

adottata in recepimento della sopra citata direttiva, il cui scopo era appunto quello di assicurare che, nel quadro dell'integrazione economica in atto, anche i dati personali potessero circolare liberamente, ma in forma corretta, all'interno dei confini dell'allora Comunità europea.

Non sempre si ha la piena percezione che questo vuoto di tutela era, invece, parzialmente anticipato dallo Statuto dei lavoratori che, fin dal 1970, aveva individuato una serie di garanzie proprio a tutela della giusta pretesa dell'individuo (*rectius* del lavoratore) a mantenere una propria sfera di intimità intangibile da ingerenze altrui (*rectius* del datore di lavoro) che non trovassero alcuna giustificazione nell'espletamento di un rapporto, quello lavorativo, bilanciato secondo parametri di reciproca correttezza tra i soggetti coinvolti. Solo in un ambito altrettanto delicato, quello sanitario, la tutela della riservatezza delle informazioni sulla persona era già presidiata a livello normativo.

Come detto sopra, lo Statuto dei lavoratori ha introdotto nell'ordinamento alcuni principi di diritto che avrebbero costituito, oltre venti anni dopo, i principali capisaldi della disciplina in materia di protezione dei dati personali anticipando, con straordinaria lungimiranza, molti dei criteri fondamentali che permeano le norme sulla riservatezza: si pensi alle cautele previste per tutelare la libertà di opinioni politiche, sindacali e di fede religiosa del lavoratore (artt. 1 e 8), il suo stato di salute (art. 5), il suo diritto di associazione e attività sindacale (art. 14), ovvero alla protezione contro atti diretti a fini di discriminazione politica, religiosa o razziale (art. 15). Cautele riguardanti quelli che decenni dopo, a partire dalla legge n. 675/1996, sarebbero stati qualificati come dati "sensibili" e assoggettati, proprio per il potenziale altamente discriminatorio insito nella loro natura, a un regime di protezione ancora più elevato rispetto ad altri dati, oltre ad essere ancora oggi annoverati nelle "categorie particolari di dati personali" ai sensi del Regolamento (UE) 2016/679 (di seguito anche "Regolamento") che, come noto, disciplina oggi la materia.

Vi è, poi, la disposizione statutaria che, forse ancora più di quelle citate, congloba nei suoi contenuti la formula primordiale e concreta di tutela del patrimonio informativo della persona, cioè dei dati che riguardano e identificano il lavoratore: ci si riferisce all'art. 4 che, nel regolamentare l'utilizzo datoriale degli strumenti di controllo, offre uno strumento normativo di garanzia a tutto tondo della riservatezza del lavoratore.

Se oggi si esaminano in parallelo lo Statuto dei lavoratori e il complesso normativo in materia di protezione dei dati personali (costituito dal Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e dal d.lgs. n. 196/2003, recentemente novellato dal d.lgs. n. 101/2018, recante il "Codice il materia di protezione dei dati personali", di seguito anche "Codice") appare evidente come si tratti di due centri gravitazionali che transitano uno nell'orbita dell'altro, in un rapporto quasi simbiotico e inscindibile senza, però, che il primo assorba totalmente il secondo o viceversa.

Si tratta di un'immagine forse suggestiva che però trova conferma, ed anzi viene esaltata, anche nel dettato normativo, dal fatto che, in entrambi, figura un espresso richiamo reciproco come non si registra per altre disposizioni le quali, parimenti, si intersecano con essi: se da un lato l'art. 4 dello Statuto invoca il rispetto del d.lgs. n. 196/2003; dall'altro lato, gli artt. 114 e 171 si riallacciano agli artt. 4 e 8 dello Statuto medesimo. Da parte sua, il Regolamento (UE) 2016/679 consente agli Stati membri – in aggiunta all'art. 9, par. 2, lett. *b*), sul trattamento delle categorie particolari di dati personali – l'adozione di norme più specifiche rispetto ai trattamenti che si svolgono nell'ambito dei rapporti di lavoro per assicurare la tutela dei diritti e delle libertà dei dipendenti, nel cui alveo vanno dunque ricomprese le norme statutarie (v. art. 88).

La *vexata quaestio* del controllo a distanza dei lavoratori posto in essere attraverso strumenti tecnologici (quali ad esempio la videosorveglianza o il monitoraggio degli accessi alla rete Internet o del sistema aziendale di posta elettronica) di cui all'art. 4 dello Statuto dei lavoratori, come riformulato dal d.lgs. n. 151/2015 e successivamente dal d.lgs. n. 185/2016 su delega del *Jobs Act* (legge n. 183/2014, che al suo art. 1, comma 7, lett. *f*), ha espressamente previsto la revisione della disciplina dei controlli a distanza), esige dunque l'esame dello stretto legame tra le due discipline: se lo Statuto prevede fondamentalmente le regole di natura procedurale, la normativa sulla protezione dei dati personali individua i limiti sostanziali sui quali si deve fondare la correttezza del trattamento.

2. I diritti datoriali e quelli del lavoratore: un bilanciamento difficile, ma necessario

Uno dei primi interrogativi per chi si accosta alla tematica dei controlli a distanza in ambito lavorativo è come si possa arrivare a conciliare due diritti apparentemente contrapposti, entrambi fondati sulla Carta fondamentale: nell'art. 2 Cost. quello alla riservatezza del lavoratore e nell'art. 41 Cost. quello alla libertà di iniziativa economica e di impresa del datore di lavoro, nel rispetto di libertà e dignità riconosciuto del lavoratore stesso [3]. Si tratta di un inquadramento estremamente esemplificativo che, per esigenze di sintesi, porta a trascurare la doverosa analisi non solo dell'art. 1 Cost., ai sensi del quale la Repubblica è fondata sul lavoro, ma anche la complessità interpretativa che pongono le altre due disposizioni citate. In questa sede, appare sufficiente un richiamo al fatto che entrambi i diritti in gioco hanno un solido fondamento costituzionale, proprio a dimostrazione della loro interrelazione quali elementi che, correttamente bilanciati, concorrono all'attuazione del sistema democratico sussistendo tra essi una antinomia solo apparente.

Nell'ambito del rapporto che li vincola reciprocamente, quindi occorre individuare gli elementi di convergenza sui quali, pur mantenendo una sostanziale distanza nei diversi diritti e interessi perseguiti, datore di lavoro e lavoratore si possano incontrare. Il punto di convergenza va allora individuato nella liceità e correttezza reciproca nel rapporto tra due soggetti con interessi potenzialmente differenti o contrapposti.

Al fine di dare concreta attuazione ai due predetti parametri, occorre porre a raffronto l'art. 4 dello Statuto dei lavoratori con i principi fondamentali della disciplina in materia di protezione dei dati personali (operazione inevitabile e costante nell'applicazione dell'art. 4, visto l'espresso rinvio contenuto, nel suo 3 comma, al d.lgs. n. 196/2003 vigente al momento della novella e che oggi deve naturalmente ricomprendere anche il Regolamento UE 2016/679) e desumere i criteri che legittimano il rapporto nel senso sopra citato.

Sotto il profilo della protezione dei dati personali, il rapporto dovrà essere improntato ai principi di liceità, limitazione della finalità e del periodo di conservazione, minimizzazione, esattezza, integrità e riservatezza dei dati personali dei lavoratori (art. 5, par. 1).

3 Va sgomberato il campo da qualsiasi interrogativo sul potere di coordinamento attribuito al datore di lavoro quale funzione essenziale per lo svolgimento di attività imprenditoriale che gli è attribuita dall'art. 2082 c.c. e, nel diritto del lavoro, assume i caratteri del potere direttivo di cui all'art. 41 Cost. e agli artt. 2094, 2104 c.c. in ambito privato, nonché dagli artt. 97-98 Cost. e artt. 1 e 2 d.lgs. n. 165/2001, in ambito pubblico.

Andrà altresì precisata la base giuridica che legittima il trattamento delle informazioni sul dipendente: poiché, per opinione quasi unanime, si esclude che il consenso[4], stante lo squilibrio di potere tra le due parti del rapporto lavorativo, possa costituire una base autonoma di liceità del trattamento e sopperiranno a tal fine gli altri presupposti di liceità dello stesso di cui all'art. 6, par. 1, del Regolamento. Potranno perciò rilevare le disposizioni normative (in particolare in ambito pubblico) oppure il "legittimo interesse" del datore di lavoro o ancora, ove applicabili, gli altri presupposti di liceità individuati dalla disposizione citata.

Ulteriore elemento fondamentale per assicurare la trasparenza, e quindi la correttezza, del trattamento, come peraltro sancito dal comma 3 dell'art. 4, è la previa informativa all'interessato. Informativa che dovrà preferibilmente avere un contenuto più ampio di quello previsto dall'art. 13 del Regolamento, dovendo contenere ragguagli anche sulle modalità d'uso degli strumenti e ai controlli che possono essere effettuati: dovrà dunque contenere l'indicazione della possibilità che sia controllata l'attività lavorativa le ragioni di cui al comma 1, mentre non si ritiene necessario specificare che lo strumento sarà utilizzato per contestare illeciti che, per l'appunto, non hanno alcuna connessione, neppure indiretta, con l'espletamento dei vincoli contrattuali da parte de lavoratore.

Infine, quali ulteriori requisiti di legittimità integrativi per i trattamenti di cui al 1 comma dell'art. 4, si segnala l'obbligo a carico del datore-titolare del trattamento dei dati del lavoratore di effettuare una valutazione di impatto *ex* art. 35 del Regolamento (quale estrinsecazione del principio di *privacy by design* di cui all'art. 25), come chiarito dal Garante per la protezione dei dati personali (di seguito "Garante")[5] e, nel caso emergano particolari rischi come risultato di tale analisi, si dovrà consultare il Garante (art. 36). Nel caso di imprese con 250 dipendenti o più il titolare-datore di lavoro è tenuto anche a predisporre un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30): si tratta di obblighi aggiuntivi a quello della previa informativa enunciato al comma 3 dell'art. 4, ricompresi nel rispetto della disciplina parimenti invocata dal comma 3[6].

3. La *vexata quaestio* dei controlli esperibili.

Uno degli aspetti più controversi della riforma riguarda i confini entro i quali il datore di lavoro si può muovere per effettuare controlli a distanza del lavoratore con strumenti elettronici, già vietati nel sistema vigente prima della riforma dello Statuto, operata a seguito del *Jobs Act*, mediante le due note categorie giurisprudenziali dei controlli preterintenzionali (legittimi solo in caso di previo esperimento della procedura concertativo-autorizzativa di cui al comma 1 dell'art. 4) e dei controlli

4 Non può esserlo anzitutto perché, come già rimarcava il Gruppo art. 29 nel *Parere 8/2001 sul trattamento di dati personali nell'ambito dei rapporti di lavoro* (WP48), del 13 settembre 2001, il trattamento rappresenta una "conseguenza necessaria ed inevitabile del rapporto di impiego. Il ricorso al consenso dovrebbe limitarsi a quei casi in cui il lavoratore sia effettivamente libero di scegliere e possa successivamente ritirare il proprio consenso senza alcun danno". Analoga considerazione è stata ribadita anche dal *Parere 2/2017 – Trattamento dei dati sul posto di lavoro* (WP 249) dell'8 giugno 2017, che ha specificato come il consenso non è valido in quanto non può essere considerato espressione di una volontà libera visto che un eventuale diniego del lavoratore "potrebbe causare allo stesso un pregiudizio reale o potenziale" non potendo per ciò solo quasi mai poter manifestare (prestare, rifiutare o revocare) liberamente la propria volontà proprio a causa dello squilibrio di potere tra l'uno e l'altro (in tal senso, anche Cass. pen., Sez. III, 17 dicembre 2019, n. 50919, Cass. Pen., Sez. III, 17 gennaio 2020, n. 1733).

5 V. provvedimento dell'11 ottobre 2018 (in www.gpdp.it, doc. *web* n. 9058979) ai sensi del quale occorre effettuare la valutazione di impatto per i "*trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dei dipendenti*".

6 Un approfondimento sul trattamento dei dati personali, tra disciplina previgente e Regolamento è rinvenibile in Garante per la protezione dei dati personali, *Relazione annuale 2018*, p. 118 e ss. (doc. *web* n. 9109211).

difensivi per la tutela del patrimonio aziendale (già ammessi dal diritto vivente e ora legittimati dal legislatore)[7].

Va preliminarmente considerato che i controlli datoriali, avendo ad oggetto i dati personali dei dipendenti, devono essere vagliati sotto il profilo della relativa liceità e della correttezza secondo le disposizioni in materia di protezione dei dati personali sopra citate, anche in virtù del rinvio a esse rinvenibile al comma 3 dell'art. 4.

Il punto di partenza per il rispetto della disciplina si può individuare nel principio di limitazione delle finalità (art. 5, par. 1, lett. *b*, del Regolamento) che, necessariamente astratto, deve essere di volta in volta identificato concretamente per determinare i confini del trattamento dei dati personali. Si tratta di un principio mobile che costituisce, però, la chiave di volta di qualunque trattamento di dati personali, sul quale si dovranno poi parametrare gli altri principi enunciati sempre all'art. 5 del Regolamento (liceità, minimizzazione, limitazione della conservazione, esattezza, integrità e riservatezza dei dati) per valutare la correttezza del controllo effettuato dal datore di lavoro: non a caso è citato anche nell'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

La finalità perseguita determina, infatti, i caratteri fondamentali del trattamento, graduando alla luce dei restanti parametri, l'estensione o meglio, i limiti, del controllo esercitabile dal datore di lavoro sul dipendente.

E' il datore di lavoro, in qualità di titolare, che è chiamato a effettuare tale ponderazione prima di iniziare il trattamento: alla luce dei presupposti di legittimità di cui all'art. 6 del Regolamento. In particolare, il datore di lavoro non si potrà sottrarre a un preliminare test comparativo, in base al principio di responsabilizzazione di cui all'art. 5, par. 2, del Regolamento, di bilanciamento tra i diritti in gioco, in modo che il trattamento non produca degli effetti pregiudizievoli ingiustificati sui diritti e le libertà del singolo, tenendo conto delle ragionevoli aspettative di riservatezza degli interessati[8] .

Sulla base di tale *iter* metodologico si potrà verificare la liceità dei controlli c.d. preterintenzionali di cui al comma 1 dell'art. 4[9], i quali – essendo comunque assoggettati a una

7 Sul tema la dottrina è vastissima; fra i tanti cfr. L. Cairo, *I controlli a distanza a quattro anni dal* Jobs Act, in *Il lavoro nella giurisprudenza*, 2019, 676; L. Angiello, *I controlli del datore di lavoro sui dipendenti: perduranti incertezze*, in *Lav. nella giur.*, 2019, 298; G. Cassano, *Prime pronunce sul nuovo art. 4 della l. n. 300/1970*, in *Dir. rel. Ind*, 2019, 303; S. Rossi, *Controlli a distanza - Tutela della riservatezza e limiti ai controlli difensivi,* in *Giur. it*., 2019, 387; F. Fusco, *La privacy del lavoratore tra riforma dell'art. 4 St. lav: e regolamento generale sulla protezione dei dati personali,* in *Diritti lavori mercati,* 2019, 295; A. Pizzoferrato, *Gli effetti del GDPR sulla disciplina nel trattamento aziendale dei dati del lavoratore*, in *ADL*, 2018, 1034; A. Federici, *I controlli investigativi tra libertà (d'impresa) e diritti (del lavoratore),* in *Riv. giur. lav. prev. soc.*, 2018, II, 22; S. Ciucciovino, *Le nuove questioni di regolazione del lavoro nell'Industria 4.0 e nella* gig economy: un problem framework *per la riflessione*, in *Dir. rel. Ind*., 2018, 1043; G. Bandelloni*, La rimozione del divieto di controllo a distanza: significato e conseguenze, in Riv. giur. lav. prev. soc., 2018, I, 85;* C. Favretto, *Controlli difensivi sul pc aziendale: l'area grigia della libertà e della dignità del lavoratore quale limite al potere datoriale*, in *ADL* 2017, 441; A. Sitzia, *Personalità (diritti della) - «i limiti del controllo della posta elettronica del lavoratore: una chiara presa di posizione della grande camera della Corte eur. dir. uomo»,* in *Nuova Giur. Civ*., 2017, 1652; D. Conte, Riflessioni sull'art. 4 dello statuto dei lavoratori alla luce della consistenza trifasica del controllo, in *Lav. prev. Oggi,* 2017, 1; M. Marciante*, Recenti sviluppi in tema di videosorveglianza nei luoghi di lavoro in ambito Cedu,* in *Giur. it*., 2018, 1157; G. Vidiri, *I controlli a distanza prima e dopo il* Jobs Act, in *Massimario di giurisprudenza del lavoro* 1/2-2017; P. Salazar – L. Failla, *Controlli difensivi: quali i limiti nel nuovo contesto dell'art. 4, L. n. 300/1970* , in *il lavoro nella giurisprudenza* 2017, 159; G. Consonni, *Il caso Barbulescu c. Romania e il potere di controllo a distanza dopo il Jobs act: normativa europea e italiana a confronto*, in *Diritto delle relazioni industriali,* 2016, 1171; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello statuto dei lavoratori*, in *RIDL* 2016, 513; A. Ricci, *Il controllo informatico a distanza sul lavoratore fra giurisprudenza e Jobs Act. La web-sorveglianza nella modernità liquida*, in *Studium Iuris* 3-4/2016, 306.

8 Cfr. in tal senso anche il Gruppo art. 29, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*, 9 aprile 2014, WP 217.

9 Con l'espressione controlli preterintenzionali ci si riferisce non solo ai trattamenti dai quali derivi "*anche la possibilità*" di una vigilanza da remoto sul lavoratore (comma 1), ma anche qualora l'informazione sia involontariamente acquisita tramite uno strumento legittimamente installato che può essere utilizzata a tutti i fini compreso quello disciplinare, secondo quanto previsto

procedura concertativa-autorizzativa, oltre ad essere finalizzati al perseguimento degli scopi tassativamente indicati al medesimo 1 comma - difficilmente potranno raggiungere una pervasività tale da renderli eccessivamente invasivi e, quindi, censurabili.

I medesimi criteri dovranno essere applicati per valutare la vigilanza datoriale introdotta al comma 3, che consente l'utilizzabilità dei dati raccolti ai sensi dei primi due commi dell'art. 4 "*per tutti i fini connessi al rapporto di lavoro*"[10].

Di fronte all'ambiguità del testo normativo, non si deve infatti cadere in interpretazioni poco garantiste per il lavoratore, aprendo la strada ad un ampliamento degli scopi legittimanti l'utilizzo da remoto di sistemi tecnici volti a monitorare l'attività del dipendente, notoriamente vietati nella formulazione originaria dell'art. 4, ma ammessi dalla giurisprudenza, dopo il superamento di orientamenti contrapposti, solo se funzionali alla tutela dell'integrità del patrimonio aziendali e per contrastare condotte fraudolente del dipendente, ma non per provare l'inadempimento contrattuale del lavoratore e la corretta esecuzione della prestazione lavorativa[11]. Se adesso il comma 1 consente a determinate condizioni il controllo "preterintenzionale" (*ex ante* e in astratto), il controllo a distanza per tutti i fini connessi al rapporto di lavoro, finanche per verificare le modalità di esecuzione della prestazione lavorativa, il medesimo trattamento sarà però legittimo solo nella misura in cui siano rispettate le stringenti condizioni esplicitate dal legislatore: non solo l'obbligo di fornire una preventiva informativa al lavoratore, ma anche il rispetto di tutti gli altri istituti previsti dalla disciplina in materia di protezione dei dati personali[12].

Questo è tanto più vero nell'epoca attuale, in cui gli sviluppi e le grandi potenzialità offerte dalla tecnologia richiedono di essere mitigate dal rigoroso rispetto della disciplina in materia di

dal comma 3. La dottrina distingue tra controlli *ex ante* ed *ex post*, riprendendo una linea già utilizzata precedentemente dalla giurisprudenza, in relazione alla vecchia formulazione della norma. In base a questa lettura l'esigenza di tutela del patrimonio aziendale inserita nel nuovo comma 1 dell'art. 4 della l. n. 300/1970, dovrebbe riferirsi esclusivamente a una necessità generica di protezione *ex ante* e astratta rispetto a una generalità non identificata di comportamenti illeciti, non essendo invece riscontrabile nel caso di controlli *ex post* o in concreto, la cui necessità sia giustificata da fatti contingenti e non prevedibili che generano esigenze di controllo puntuali. In altre parole, il nuovo comma 1, dell'art. 4 l. n. 300/1970, entri in gioco solo nell'ipotesi in cui l'installazione di uno strumento tecnologico sia giustificata da esigenze generiche di tutela del patrimonio, ritenendo invece che esorbitino dal campo di applicazione del suddetto articolo i controlli mirati.

10 Sui profili critici della riforma si rinvia a Audizione del Presidente A. Soro sugli schemi di decreti legislativi attuativi del c.d. Jobs Act *presso la Commissione Lavoro della Camera dei Deputati (9 luglio 2015) e la Commissione Lavoro del Senato (14 luglio 2015)* (doc. *web* n. 4119045), nonché intervento su *"L'Huffington Post", 8 settembre 2015, Caro senatore Ichino, facciamo chiarezza sui controlli a distanza nel* Jobs Act (doc. *web* n. 4235378*).*

11 In questa sede non si entra nel merito del sottile *discrimen* tra illecito extracontrattuale e illecito disciplinare, cioè quando la condotta del lavoratore è di tale particolare gravità tanto da configurare una palese violazione dei più elementari doveri di diligenza, lealtà e correttezza, diventando così illecita, a prescindere dal connesso profilo retributivo-disciplinare (illuminante in tal senso, Cass., Sez. lav., sent. 1° febbraio 2019, n. 3133).

12 Così il provvedimento del Garante del 26 marzo 2020 n. 65 (*in corso di pubblicazione*), con il quale è stata censurata l'assenza di informativa, in relazione a un controllo datoriale effettuato, in assenza di previa informativa, attraverso la consultazione della cronologia degli accessi ad Internet di una dipendente poi licenziata, che ha comportato anche l'accesso ai "dati esterni" tratti dal suo account di posta elettronica personale della reclamante nonché al contenuto delle comunicazioni attraverso la riproduzione dell'oggetto delle stesse, che ha, da un lato, consentito al datore di lavoro di effettuare un controllo sull'attività della dipendente (in vista della contestazione di comportamenti ritenuti non corretti sul piano dell'esecuzione della prestazione lavorativa) ed ha anche permesso di conoscere informazioni relative alla sua vita privata e, comunque, relative a fatti non rilevanti ai fini della sua attitudine professionale (dati sulla vita sessuale, sull'orientamento religioso, sulla salute dei figli, sulla situazione familiare ed altro), con violazione degli artt. 5, par. 1, lett. *a*), 13 e 88 del Regolamento, in relazione agli artt. 113 e 114 del Codice. Sulla stessa linea anche Corte di Cassazione (sent. 24 febbraio 2020 n. 4871) relativa al licenziamento disciplinare di un dipendente bancario che ha eseguito interrogazioni sui conti correnti dei clienti, non sostenute da ragioni di servizio, violandone la privacy.

protezione dei dati personali, in modo da impedire la realizzazione di una sorveglianza massiva e totale, continua e anelastica, sproporzionata e invasiva, del lavoratore[13].

Analoghe valutazioni vanno poi effettuate in relazione ai controlli difensivi realizzati in forma occulta, permettendo forme di vigilanza a distanza finalizzate ad accertare condotte del lavoratore illecite che non riguardino l'esatto adempimento della prestazione lavorativa, ma che assumono rilevanza sul diverso piano penale ed extracontrattuale.

Anche in tal caso spetta al datore di lavoro effettuare una valutazione prognostica per attivare, dopo aver tentato misure preventive meno limitative dei diritti dei lavoratori[14], un controllo necessitato da un pericolo attuale[15], derivante dal verificarsi di specifiche anomalie o accadimenti illeciti, che potrà essere anche di tipo retrospettivo[16], secondo una severa applicazione in concreto delle norme in materia di protezione dei dati personali: egli dovrà essere in grado di dimostrare che l'esercizio dei poteri datoriali, sia fondato sui presupposti di liceità di cui sopra, e che sia giustificata la limitazione della sfera di riservatezza del lavoratore, che non potrà comunque mai sconfinare nell'arbitrio e nell'irragionevolezza. Il controllo non potrà avvenire al di fuori dei consueti canoni di proporzionalità e selettività per il periodo strettamente necessario, così da assicurare che i controlli sul lavoro siano graduali nell'ampiezza e nella tipologia di intervento, rendendo marginali invece quelli maggiormente pervasivi, dovendosi censurare un controllo datoriale indiscriminato ed una illimitata attività di indagine anche al di fuori del contesto lavorativo.

Spetterà all'autorità adita dal lavoratore, che eventualmente lamenti un trattamento illecito dei suoi dati personali, effettuare una verifica *ex post*, sulla base delle modalità di accertamento utilizzate dalla parte datoriale, misurando il controllo difensivo sui richiamati criteri di correttezza, necessità, lealtà e proporzionalità.

Se il *Jobs Act* ha dunque fornito una copertura legislativa di rango primario alla materia dei controlli a distanza, i predetti approdi ermeneutici appaiono coerenti con i principi dettati anche dalla CEDU, offrendo una via interpretativa per contemperare posizioni inevitabilmente contrapposte[17].

13 Il Garante ha sempre sottolineato che la disciplina, infatti, pure a seguito del *Jobs Act*, non consente l'effettuazione di attività idonee a realizzare un controllo prolungato e indiscriminato sull'attività dei lavoratori (v. provv. del 16 novembre 2017, *web* n. 7355533, del 22 dicembre 2016, doc. *web* n. 5958296; ma v. anche *Linee guida per posta elettronica e internet*, del 1° marzo 2007, doc. *web* n. 1387522, spec. par. 4, con principi che possono ritenersi tutt'ora validi).

14 Ad esempio, il Garante ha affermato in più occasioni, che il datore di lavoro è tenuto all'individuazione preventiva della lista dei siti considerati correlati alla prestazione lavorativa, nonché dell'adozione di filtri per il blocco dell'accesso a determinati siti o del download di alcuni file. E non sono comunque consentite al datore di lavoro la lettura e la registrazione sistematica delle e-mail e delle pagine *web* visualizzate dal lavoratore (v. provvedimento del 22 dicembre 2016, doc. *web* n. 5958296).

15 In proposito si tenga presente che il trattamento di dati personali effettuato per finalità di tutela dei propri diritti deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (v. provvedimenti dell´8 marzo 2018, doc. *web* n. 8163433, e del 1° febbraio 2018 doc. *web* n. 8159221).

16 Vale a dire che i controlli difensivi possono essere finalizzati non solo ad accertare la perpetrazione di eventuali comportamenti illeciti del lavoratore (poi effettivamente riscontati), ma anche sulla verifica a posteriori della commissione di un illecito posto in essere dal dipendente avvalendosi del mezzo in dotazione, nelle settimane precedenti l'attuazione del controllo, sempreché sia giustificata sulla base di indizi gravi, precisi e concordanti cioè quando siano emersi – nel caso concreto - elementi di fatto tali da raccomandare l'avvio di un'indagine appunto retrospettiva dopo la consumazione della condotta addebitata al dipendente (v. Cass., Sez. lav., ord. del 28 maggio 2018, n. 13266).

17 La riprova di tale armonizzazione dei sistemi emerge dalla giurisprudenza CEDU: basti solo ricordare, molto succintamente, l'affermazione del principio di proporzionalità e trasparenza (*Bărbulescu c. Romania,* n. 614960/08 del 5 settembre 2017; *Garamukanwa v. The United Kingdom*, n. 70573/17 del 6 giugno 2019); la riconosciuta possibilità di effettuare controlli sul sospetto ragionevole e individualizzato o atti illeciti da parte di alcuni lavoratori (*López Ribalda e al. c. Spagna,* n. 1874/13 and 8567/13 del

4. La strumentazione in dotazione al lavoratore e la registrazione della presenza dei lavoratori: *quid iuris*?

L'art. 4, al comma 2, introduce una deroga al generale divieto di controllo a distanza, sottraendo ai limiti di cui al comma 1, gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e quelli di registrazione degli accessi e della presenza, utilizzati dal datore per controllare il rispetto dell'orario di lavoro.

L'eccezione alla regola del comma 1 può trovare applicazione nei casi in cui lo strumento sia essenziale per lo svolgimento della prestazione lavorativa; al contrario, se lo strumento viene impiegato per migliorarne l'efficienza, il connesso trattamento si rientra nell'alveo del comma 1 con conseguente necessità di attivare le previste procedure concertative-autorizzative.

E' sempre il datore di lavoro-titolare del trattamento dei dati a dover effettuare, secondo il principio di responsabilizzazione (art. 5, par. 2, del Regolamento) una verifica in concreto sulla tipologia di strumenti utilizzabili, sugli scopi perseguiti e sul rispetto delle norme: sebbene la norma in questione non si limiti a prevedere unicamente che lo strumento in dotazione al lavoratore sia utilizzato nello svolgimento dell'attività lavorativa, senza precisare alcun criterio di valutazione, al fine di godere l'esenzione dalle procedure di cui al comma 1 dell'art. 4.

Una sottile linea di confine, quella proposta dal legislatore, che è stata invece tracciata nettamente dal Garante con riferimento ai servizi *software* o applicativi, i quali per rientrare nell'esenzione di cui al comma 2 dovranno essere strettamente funzionali *a rendere* la prestazione lavorativa, anche sotto il profilo della sicurezza; viceversa, sono soggetti al comma 1 dell'art. 4 i dispositivi che rappresentano un elemento «aggiunto» agli strumenti di lavoro, senza avere alcuna utilità rispetto all'attività del lavoratore e senza che questi li possa utilizzare in via primaria ed essenziale per l´esecuzione dell'attività lavorativa[18].

Per quanto riguarda gli strumenti di registrazione degli accessi e delle presenza si ritiene di aderire a quell'orientamento dottrinario che interpreta staticamente la disposizione, ritenendo applicabile l'esenzione del comma 2 solo agli strumenti che individuano l'orario di ingresso e uscita, non anche quelli dinamici che individuano l'esatta ubicazione del lavoratore durante la giornata di lavoro[19], così dilatando a dismisura il potere di controllo del datore di lavoro fino a consentire una

17 ottobre 2019; *Libert c. Francia,* n. 588/13 del 22 febbraio 2018); l'interpretazione estensiva del concetto di vita privata fino a ricomprendervi anche la tutela della vita professionale nei luoghi aperti al pubblico (*Antović e Mirković c. Montenegro*, n.70838/13 del 28 novembre 2017). Il concetto di controllo preterintenzionale riecheggia nella Raccomandazione del Consiglio d'Europa C/Rec(2015)5 del 1 aprile 2015, sul trattamento dei dati personali in ambito lavorativo, ove si afferma che il monitoraggio dell'attività del dipendente non può essere lo scopo principale, bensì solo l'indiretta conseguenza di un'attività datoriale oltre a proteggere la produzione, la salute e la sicurezza dei lavoratori (punto 14).

18 Come chiarito dal Garante, qualora gli strumenti utilizzati dai lavoratori per rendere la propria attività lavorativa eccedano le funzionalità proprie di uno strumento di lavoro, rappresentando un strumento "aggiunto" ma rendono anche possibile raccogliere in maniera sistematica e continuativa informazioni di dettaglio riferibili alle modalità con cui i singoli lavoratori prestano l´attività lavorativa (ad es. informazioni relative alla produttività giornaliera del lavoratore), determinando la possibilità di un controllo a distanza dell'attività lavorativa da parte del datore di lavoro, devono essere soggetti alle procedure di garanzia richieste dal comma 1 dell'art. 4 (cfr. i provvedimenti del 7 marzo 2019, doc. *web* n. 9121890; dell' 8 marzo 2018, doc. *web* n. 8163433; del 18 aprile 2018, doc. *web* n. 9358266; del 16 novembre 2017, doc. *web* n. 7355533; del 13 luglio 2016, doc. *web* n. 5408460). Un orientamento interpretativo confermato anche dal Ministero del lavoro - Direzione generale per l'attività ispettiva (parere del 5 gennaio 2015 n. 37/0000011) e dall'Ispettorato nazionale del lavoro (v. circolari n. 2 del 7 novembre 2016 e n. 5 del 19 febbraio 2018).

19 In tale senso, si veda il provvedimento del Garante che si è espresso negativamente in ordine alla richiesta di una società di dotare i propri dipendenti addetti alla pulizia delle strade di dispositivi indossabili dotati anche di un *gps*, con i quali effettuare la lettura delle etichette elettroniche collocate sui cestini getta rifiuti e segnalare l'eventuale spostamento di quelli non ancorati al

sorta di Panopticon datoriale[20]. In ogni caso, le esigenze organizzative e di sicurezza produttive non possono derogare comportare dei trattamenti esorbitanti da tali finalità: ad esempio, il Garante si è espresso in senso critico, nell'esercizio dei suoi poteri consultivi, sulle misure di contrasto di cui all'art. 2 del disegno di legge recante interventi per la concretezza dell'azione delle pubbliche amministrazioni, approvato dal Parlamento e divenuto legge n. 56/2019 (in base al quale, ai fini della verifica dell'osservanza dell'orario di lavoro in ambito pubblico, è consentita l'introduzione di sistemi di identificazione biometrica e di videosorveglianza) ritenendo esorbitante dallo scopo perseguito l'utilizzo sistematico e generalizzato di strumenti così invasivi, in assenza di specifici fattori di rischio o di particolari presupposti, per violazione dei principi i liceità, di proporzionalità e di "minimizzazione dei dati" di cui all'art. 5 del Regolamento[21]

5. Lavoro agile e piattaforme digitali: il rischio di un "periscopio datoriale" nella vita degli altri.

La tematica dei controlli a distanza e il correlato bilanciamento tra il potere datoriale di controllo e la tutela della riservatezza del lavoratore presenta una problematicità ancora più evidente nei casi in cui viene consentito al dipendente di eseguire la prestazione lavorativa al di fuori della sede di lavoro[22]: si pensi al telelavoro (nel cui ambito il lavoro è interamente svolto all'esterno dei locali aziendali) e al lavoro agile (che prevede invece la possibilità di svolgere la prestazione lavorativa

suolo, proprio perché si sarebbe così monitorato lo spostamento del lavoratore (doc. *web* n. 9094427). Al contrario, nel caso di una importante società telefonica che ha giustificato la necessità di installare n sistema di localizzazione degli *smartphone* dati in dotazione ai propri tecnici dipendenti per motivi di sicurezza, dovendo recarsi in zone remote o disagiate per interventi di manutenzione, soprattutto in caso di emergenze e/o calamità naturali, il Garante ha acconsentito al trattamento previa adozione di una serie di accorgimenti volti a mitigare l'invasività del controllo a distanza, a tutela degli interessati (doc. *web* n. 3505371). Altrettanto interessante è il provvedimento riguardante il trattamento dei dati personali prefigurato da una società specializzata in contratti di somministrazione, connesso all´installazione di una specifica applicazione - contenente una funzionalità di localizzazione geografica - sul dispositivo *smartphone* dei dipendenti, preordinata all´effettuazione della timbratura del cartellino e la rilevazione delle presenze, con il quale il Garante ha imposto alla società stessa di cancellare il dato relativo alla posizione del lavoratore, avendo verificato preventivamente l´associazione tra le coordinate geografiche della sede di lavoro e la posizione del lavoratore, conservando, eventualmente, il solo dato relativo alla predetta sede di lavoro, alla data e all´orario cui si riferisce la timbratura (doc. *web* n. 5497522).

20 Sui limiti di utilizzabilità dei badge, v. Corte di Cassazione, Sez. Lav., sent. 14 luglio 2017, n. 17531.

21 Il richiamo al legislatore è stato molto severo: v. V. parere al Governo dell'11 ottobre 2018 (doc. web n. 9051774) nonché audizione del Presidente del Garante presso le Commissioni riunite I (Affari Costituzionali) e XI (Lavoro) della Camera dei Deputati (6 febbraio 2019) (doc. *web* n. 9080870). I medesimi principi sono stati ribaditi nel parere sullo schema di d.P.C.M. concernente la disciplina di attuazione della disposizione di cui all'articolo 2 della legge 19 giugno 2019, n. 562019 (doc. *web* n. 9147290).

22 Anche su tale punto la dottrina è nutrita: cfr. D. Garofalo, *La prima disciplina del lavoro su piattaforma digitale*, in *Lavoro giur*., 2020, 5; S. Bini, *Lo* smart working *al tempo del coronavirus. Brevi osservazioni, in stato di emergenza*, in *Giustizia civile Emergenza Covid Speciale*, 2020, 67; C. Di Carluccio, *Emergenza epidemiologica e lavoro agile*, in *RIDL*, 2020, 3; C. Macchione, *Il lavoro agile ai tempi del coronavirus*, in *Giustizia civile.com;* A. Ingrao, *Il potere di controllo a distanza sull'ozio telematico e il limite del diritto alla privacy del lavoratore,* in *RIDL,* 2019, 416; G. Gosetti, *La digitalizzazione del lavoro. Questioni aperte e domande di ricerca sulla transizione*, in *Economia e società regionale*, 2019, 91; M. Lai, *Prime tutele per i lavoratori delle piattaforme digitali*, in *Dir. Prat. Lav*., 2019, 2741; F. Capponi, *Lavoro tramite piattaforma digitale: prima lettura del d.l. n. 101/2019 convertito in l. n. 128/2019*, in *Dir. Rel. Ind.,* 2019, 1231; F. Mattiuzzo, Blockchain e smart contact: *nuove prospettive per il rapporto di lavoro*, in *Il lav. nella giur*., 2019, 236; M. Lai, *Prime tutele per i lavoratori delle piattaforme digitali*, in *Dir. Prat. Lav*., 2019, 2741; E. Raimondi, *Potere di controllo, tutela della riservatezza e «lavoro agile»,* in *Riv. giur. lav. prev. soc.,* 2019, I, 69; V. Maio, *Il diritto del lavoro e le nuove sfide della rivoluzione robotica,* in *Argomenti Dir. Lav.,* 2018, 6, 1414; E. Barraco*, Il controllo sullo smart worker,* in *Dir. Prat. Lav.,* 2018, 623; AA.VV., *Il lavoro nelle piattaforme digitali: nuove opportunità, nuove forme di sfruttamento, nuovi bisogni di tutela, Atti del Convegno «Il lavoro nelle piattaforme digitali: nuove opportunità, nuove forme di sfruttamento, nuovi bisogni di tutela» svoltosi a Roma il 20 ottobre 2017, Quaderno 2/2017 della Riv. Giur. Lav. Prev. Soc.*

in parte al di fuori dei locali, modalità fortemente incentivata a seguito dell'emergenza epidemiologica da Covid-19)[23].

La smaterializzazione della postazione di lavoro e l'assenza di vincoli di continuità della prestazione, in gran parte flessibile e demandata all'autonomia organizzativa del dipendente che risponde per obiettivi, genera l'esigenza di attivare forme di controllo da remoto del dipendente digitale, anche al fine di poter esercitare quegli indispensabili poteri direttivi e di coordinamento della prestazione del lavoratore in modo da trarne l'utilità attesa: evidentemente la tutela del lavoratore non può comprimere, fino ad annullare del tutto, le legittime esigenze produttive e di sicurezza della parte datoriale.

Per quanto riguarda il lavoro agile, l'art. 21 della legge n. 81/2017 sottopone, con una forma un po' pleonastica, al rispetto dell'art. 4 della legge n. 300/1970 l'esercizio del potere di controllo del datore di lavoro sulla "*prestazione resa dal lavoratore all'esterno dei locali aziendali*".

Sebbene la lettera della norma sembri limitare l'oggetto del controllo datoriale, di fatto esso può sconfinare anche sull'attività resa, in quanto, essendo state demandate al lavoratore le scelte organizzative, queste potrebbero essere anche oggetto di verifica parte del datore di lavoro. Non solo: anche l'ordinaria attività lavorativa in sé può comportare l'uso di applicazioni informatiche – ad esempio le piattaforme più frequentemente utilizzate per riunioni virtuali – che permettono al datore di entrare in casa del dipendente. Ne deriva il rischio di intrusioni nella sfera addirittura domestica o comunque strettamente privata del lavoratore, come non accade per la prestazione fornita nei locali di lavoro.

L'art. 4 della legge n. 300/1970, specie il suo comma 1, in tale ambito viene ridimensionato, poiché incide sul potere di controllo datoriale con una diversa intensità rispetto al tradizionale rapporto di lavoro: in quest'ultimo, l'intento del legislatore è solo quello di delineare, ma non limitare o vietare, il controllo sull'attività del lavoratore o, meglio, sull'esatto adempimento: per ottenere tale risultato occorre, però, un cambiamento di prospettiva. La vera sfida deve essere quella di valorizzare l'autonomia e difendere la dignità dei lavoratori spostando il controllo -in tutti i casi in cui è possibile- dagli orari ai risultati, dalla verifica puntuale delle azioni agli obiettivi.

Analogamente, il lavoro tramite piattaforme anche digitali (come disciplinato dal d.l. n. 101/2019, convertito in legge, con modificazioni, dall'art. 1, comma 1, legge n. 128/2019, che ha ampliato e integrato alcune previsioni già contenute nel d.lgs. n. 81/2015) cioè attraverso "*i programmi e le procedure informatiche delle imprese che, indipendentemente dal luogo di stabilimento, organizzano le attività di consegna di beni, fissandone il prezzo e determinando le modalità di esecuzione della prestazione*", richiede inevitabilmente l'esposizione del lavoratore a forme di controllo da remoto; ciò, sebbene la novella

23 E' soprattutto in ambito pubblico, un settore nel quale non si rinveniva una diffusa applicazione di tali forme innovative di esecuzione della prestazione lavorativa, che si è data una forte spinta al ricorso a forme di lavoro agile, arrivando a qualificarlo come modalità ordinaria di svolgimento della prestazione lavorativa nelle pubbliche amministrazioni di cui all'articolo 1, comma 2, del d.lgs. n. 165/2001, fino alla cessazione dello stato di emergenza epidemiologica da COVID-2019, ovvero fino ad una data antecedente stabilita con d.P.C.M. su proposta del Ministro per la pubblica amministrazione (v. d.l. n. 18 del 17 marzo 2020, convertito con legge del 24 aprile 2020 n. 27, recante "*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*"). Da ultimo, il testo del d.d.l. di conversione in legge del d.l. 19 maggio 2020, n. 34, recante misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19 (c.d. decreto "rilancio"), attualmente all'esame delle Camere, prevede la proroga fino al 31 dicembre 2020 del lavoro agile per il 50% dei dipendenti che svolgono attività eseguibili da remoto (artt. 90 e 263). La commissione Bilancio della Camera ha poi proposto l'introduzione del "Piano organizzativo del lavoro agile" (POLA), con il quale dal 1° gennaio 2021 la percentuale dovrebbe salire ad almeno il 60%. ***[NB: Occorrerà aggiornare la nota sulla base della conclusione dell'iter di conversione del decreto legge]***

legislativa, nell'estendere le tutele proprie del lavoro subordinato abbia, tra le altre cautele, introdotto l'espresso obbligo di trattare i dati personali dei lavoratori in conformità al Regolamento e al d.lgs. n. 196/2003 (art. 47-*sexies* del d.lgs. n. 81/2015).

Fermo restando che il monitoraggio deve comunque avvenire nel rispetto della disciplina in materia di protezione dei dai personali, e che nell'ambito di tali rapporti viene rimarcato – non a caso, proprio per la loro peculiarità – l'obbligo del datore di lavoro di garantire il rispetto della sua personalità e della sua libertà morale (v. art. 115 del Codice), il panorama normativo, *de jure condito*, appare povero di indicazioni concrete in tal senso[24].

Tuttavia, non per questo il potere direttivo del datore può trasformarsi in un "periscopio" virtuale che si insinua nella vita domestica del lavoratore, né quest'ultimo può ritenersi esente da ragionevoli forme di coordinamento e verifica. La ricerca di un difficile punto di equilibrio tra potere datoriale e diritto alla riservatezza, senza che nessuno dei due esondi nell'arbitrio e nell'abuso del diritto, potrà essere soddisfatta seguendo due vie parallele.

Da una parte, bisogna garantire che le nuove tecnologie rappresentino un fattore di progresso (e non di regressione) sociale, valorizzando anziché comprimendo le libertà affermate sul terreno lavoristico: diventa allora indispensabile garantirne la sostenibilità sotto il profilo democratico e la conformità ad alcuni irrinunciabili principi che confluiscono tutti nel diritto alla protezione di dati personali riguardanti i lavoratori. Occorre pensare a un nuovo Statuto dei lavoratori, che, anche alla luce di un diritto emergenziale che ha imposto il diffuso ricorso alle forme di lavoro da remoto, cd. lavoro agile, generalmente necessitato e improvvisato sul campo, sappia coniare nuovi diritti nuovi doveri di lavoratori e datori di lavoro, a fronte dell'ormai irrinunciabile utilizzo delle nuove tecnologie nel mondo lavorativo: un esempio per tutti, assicurare *anche un diritto alla disconnessione, inteso come possibilità di distaccarsi dalle sollecitazioni inerenti la sfera lavorativa e preservare i necessari spazi di vita privata, individuando quindi limiti in assenza dei quali finiscono per essere messe in discussione molte delle conquiste di tutela del lavoratore e della sua dignità, che costituiscono elementi essenziali del diritto del lavoro*"[25]..

Sotto un diverso profilo, occorre fare anche ricorso a strumenti duttili, in grado di superare la rigidità del dato normativo e rispondere alle incalzanti sfide derivanti dal progresso tecnologico: ci si riferisce alle regole deontologiche in ambito lavorativo (cfr. artt. 2-*quater* e 111 del Codice), che dovendo peraltro essere adottate nell'osservanza del principio di rappresentatività e sottoposte a consultazione pubblica, consentono anche di superare eventuali critiche su un paventato deficit di democraticità nel momento in cui si sottraggono al procedimento legislativo vero e proprio.

6. Il quadro sanzionatorio e il dilemma dell'inutilizzabilità dei dati raccolti in violazione della disciplina sulla riservatezza: per un approccio *privacy-oriented* in sede giudiziaria.

Infine, un breve cenno merita il sistema sanzionatorio, declinato sempre nell'ottica della protezione dei dati personali, vale a dire qualora si registri una violazione dell'art. 4 dello Statuto

24 Sebbene i controlli difensivi, per consolidata giurisprudenza, siano ritenuti consentiti tanto più quando il lavoro deve essere eseguito al di fuori dei locali aziendali, ossia in luoghi in cui è più facile la lesione dell'interesse all'esatta esecuzione della prestazione lavorativa e dell'immagine dell'impresa, all'insaputa dell'imprenditore (v. Cass., sez. lav., sent. 12 ottobre 2015, n. 20440).

25 Si veda A. Soro, *Audizione del Presidente del Garante per la protezione dei dati personali sull'affare assegnato atto n. 453 relativo al tema Ricadute occupazionali dell'epidemia da Covid-19, azioni idonee a fronteggiare le situazioni di crisi e necessità di garantire la sicurezza sanitaria nei luoghi di lavoro*, presso la Commissione 11a (Lavoro pubblico e privato, previdenza sociale) del Senato della Repubblica, 13 maggio 2020 (doc. *web* n. 9341993).

quale conseguenza diretta e immediata del mancato rispetto delle norme che presidiano la riservatezza del lavoratore.

La maggior parte delle disposizioni citate in materia di protezione dei dati personali è assoggettata, in caso di inosservanza, alle sanzioni amministrative pecuniarie di cui all'art. 83, par. 4 e 5, del Regolamento, anche in virtù del rinvio effettuato ad esso dall'art 166, commi 1 e 2, del Codice (con eventuale sanzione accessoria della pubblicazione del provvedimento sanzionatorio e con iscrizione del caso nel registro delle violazioni di cui all'art. 57, par. 1, lett. *u*, del Regolamento). Il datore di lavoro, inoltre, potrà essere destinatario di misure correttive, come previsto dall'art. 58, par. 2, del Regolamento, e può essere chiamato al risarcimento del danno patito dal suo dipendente, secondo quanto previsto dall'art. 82 del Regolamento medesimo.

A rigore l'art. 4, comma 3, dello Statuto, nel condizionare l'utilizzabilità delle informazioni raccolte ai sensi dei commi precedenti al rispetto delle disposizioni in materia di protezione dei dati personali contiene un chiaro limite probatorio nell'ipotesi in cui la raccolta dei dati del lavoratore sia fondata su controlli inammissibili.

La lettera della norma non dovrebbe lasciare spazio ad alcun dubbio, stante l'espresso rinvio al rispetto della disciplina in materia di protezione dei dati personali: ai sensi dell'art. 2-*decies* del Codice, infatti, i dati trattati in sua violazione sono inutilizzabili[26]. Si tratta di un principio generale che viene apparentemente derogato dalla circostanza che tale ultima disposizione fa salvo, a sua volta, quanto previsto dall'art. 160-*bis* del Codice, il quale dispone che la validità, l'efficacia e l'utilizzabilità di dati trattati in difformità dalle norme sulla riservatezza è disciplinato secondo il codice di rito.

In ambito civilistico, a differenza di quello penale che all'art. 191 c.p.p. censura con l'inutilizzabilità la prova acquisita in violazione dei divieti di legge[27], non si rinviene alcuna norma che sancisca l'inutilizzabilità delle prove legittimamente acquisite. Una questione non banale, visto che il giudice deve fondare le sue decisioni sulle prove proposte dalle parti (art. 115 c.p.c.) il che porterebbe a interrogarsi se possa ricorrere anche a quelle raccolte in violazione della riservatezza del lavoratore.

Uno scenario ancora più critico si apre sull'apparato sanzionatorio penale: originariamente, il Codice, da un lato, aveva abrogato l'inciso dell'art. 38 dello Statuto che sanzionava penalmente l'art. 4, dall'altro lato, aveva disposto all'art. 171 del Codice medesimo che la violazione dell'art. 4 dello Statuto fosse punita con le sanzioni dell'art. 38 dello Statuto.

L'art. 23, comma 2, d.lgs. 151/2015, ha cercato di riordinare il sistema attraverso una novella all'art. 171 del Codice, ma limitando la sanzione penale per la violazione solo dei primi due commi del nuovo art. 4 dello Statuto. A ben vedere il richiamo al comma 2, norma permissiva e quindi non suscettibile di violazione, si è rivelato superfluo, tanto che è stato eliminato dall'art. 15, comma 1,

26 Cfr., *ex multis*, A. Ingrao, *Lavoro (rapporto) - I controlli difensivi tra passato e presente: di privacy del lavoratore e inutilizzabilità dei dati*, in *Nuova Giur. Civ.*, 2019, 4, 649; A. Cordero, *Utilizzabilità in giudizio di prove in contrasto con la privacy del lavoratore*, in *Giur. it.*, 2019, 1557; G. Bandelloni, *Le nuove regole del controllo a distanza sulla prestazione lavorativa* (nota a sentenza Trib. Savona 01/03/2018), in *Riv. giur. lav. prev. Soc.*, 2018, 574; C. Carta, *L'inutilizzabilità dei dati raccolti in violazione dell'art. 4 St. lavoratori* (Nota a Tribunale Prato, 14.11.2017), in *Riv. giur. lav. prev. Soc.*, 2018, 416; M. Verzaro, *Controlli tecnologici e utilizzabilità dei dati acquisi*ti (Nota a Trib. Roma 22.3.2018, Trib. Roma 13.6.2018 ord.), in *Riv. giur. Lav.*, 2018, 562.

27 Va osservato, però, che in tale ambito emergono pronunciamenti di segno contrario nell'ipotesi in cui la raccolta dei dati in violazione dell'art. 4 sia qualificabile come prova atipica disciplinata dall'art. 189 c.p.p. e come tali utilizzabili in quanto le previste garanzie statutarie riguardano soltanto i rapporti di diritto privato tra datore di lavoro e lavoratori, ma non possono avere rilievo nell'attività di accertamento e repressione di fatti costituenti reato (così Cass. pen., Sez. II, 19 giugno 2019, n. 35143; Cass. pen., Sez. V, 18 aprile 2019, n. 17155).

lett. *f)*, del d.lgs. n. 101/2018, sicché il presidio penale avverso controlli a distanza illeciti permane unicamente in riferimento al comma 1[28].

Nessun reato si configura per la violazione del comma 3, per cui il trattamento di dati del lavoratore effettuato ai sensi dei commi 1 e 2 senza la prevista informativa o in violazione delle norme sulla riservatezza rimane confinato nell'area del penalmente lecito. Anche in questo caso, tuttavia, la legge penale può rientrare in considerazione con riferimento alle possibili violazioni della disciplina sui dati personali - come detto, esplicitamente richiamata come limite e quindi parametro di liceità dei trattamenti - la quale è a sua volta presidiata da sanzioni non solo amministrative, ma anche penali.

Sarà compito del giudice adito effettuare una valutazione *privacy-oriented* sulle risultanze dell'attività datoriale.

Ad esempio, specie nei casi in cui abbia ad oggetto dati di cui agli artt. 9 e 10 del Regolamento, il trattamento potrà anche qualificarsi come illecito ai sensi dell'art. 167 del Codice. E ancora, specie in ambito civilistico, lasciando all'autorità giudiziaria il compito di valutare lo scenario probatorio; diversamente si sarebbe corso il rischio anche di una interferenza ingiustificata da parte del Garante per la protezione dei dati personali nell'attività giudiziaria (peraltro chiaramente scongiurata anche ai sensi dell'art. 23, par. 1, lett. *f*, del Regolamento e dell'art. 2-*duodecies* del Codice, che prevedono limitazioni alla disciplina in relazione ai trattamenti effettuati per ragioni di giustizia), essendo l'autorità che solitamente viene interpellata per verificare la liceità del trattamento.

Sarà il giudice a dover garantire quell'equo bilanciamento tra diritti anche nella fase patologica del rapporto tra lavoratore e datore di lavoro.

* * *

Da un quadro così complesso quale quello sopra delineato, si rileva come, specialmente in ambito lavorativo, il baricentro del sistema risieda nella protezione dei dati: è una disciplina che deve necessariamente affiancare le norme dello Statuto ed anzi, come si è ipotizzato precedentemente, rappresentare anche la base per l'approvazione di un nuovo o rinnovato Statuto dei lavoratori.

E' indubbio che le risorse e le facilitazioni offerte dalla tecnologia e dall'informatica non devono comprimere la dignità del lavoratore, che proprio su di esse deve basare la propria qualificazione professionale. Peraltro, il nostro Paese non si può sottrarre alla modernizzazione digitale che rappresenta un fattore ineludibile di competitività a livello mondiale.

La vera sfida sarà quella di conciliare uomo e macchina, lavoro e vita privata, diritti e doveri del dipendente con diritti e doveri del datore di lavoro. L'obiettivo non potrà che essere quello di garantire il diritto alla protezione dei dati personali, in un panorama lavorativo profondamente modificato dalla diffusione delle tecnologie digitali nonché sempre più fondato sull'utilizzo dei dati personali: la disciplina sull'uso dei dati finisce quindi per diventare uno degli elementi più sensibili e delicati per garantire un corretto bilanciamento fra i poteri ed i doveri reciproci delle parti.

28 *A latere* di tale problematica, sia consentito rilevare che secondo la giurisprudenza di legittimità la fattispecie criminale in esame si configura alla stregua di un reato di pericolo, essendo diretto a salvaguardare le possibili lesioni della riservatezza dei lavoratori, con la conseguenza che per la sua integrazione è sufficiente la mera predisposizione di apparecchiature idonee a controllare a distanza l'attività dei lavoratori, in quanto per la punibilità non è richiesta la messa in funzione o il concreto utilizzo delle attrezzature e la sola installazione dell'impianto (v. Sez. III, 26 ottobre 2016, n. 45198; Sez. III, 2 novembre 2013, n. 4331; Sez. III, 15 dicembre 2006, n. 8042).