*Arturo Maresca**

I controlli tecnologici a distanza

SOMMARIO:

1. L'art. 4 L. n. 300/1970 alla luce del Regolamento UE 679/2016 e del D.Lgs. n. 101/2018.

Com'è noto l'art. 4 L. n. 300/1970 è destinato a regolare i limiti entro i quali il datore di lavoro può impiegare in azienda strumenti in grado di controllare a distanza l'attività lavorativa dei propri dipendenti ed ha subito un rilevante aggiornamento (ad opera dell'art. 23 D.Lgs. n. 151/2015 e dell'art. 5, comma 2, D.Lgs. n. 185/2016), tramite il quale, tra le altre modifiche, è stato inserito all'interno del suo ultimo comma un espresso rimando al Codice della *privacy*, laddove è prescritto che "*le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal d.lgs. 196/2003*".

Ne deriva un singolare circolo normativo in virtù del quale la disciplina di settore in materia di tutela della riservatezza rimette alla disciplina speciale lavoristica la regolamentazione del trattamento dei dati personali del lavoratore che sia realizzato in conseguenza dell'impiego di uno strumento

* Ordinario di Diritto del lavoro – Sapienza Università di Roma.

idoneo a realizzare un controllo a distanza dell'attività lavorativa. Regolamentazione che però, come prescrive la norma lavoristica, non è totalmente autonoma, essendo destinata ad integrarsi e coordinarsi con quella in materia di *privacy*, chiamando così l'interprete ad un'operazione ermeneutica non sempre semplice.

In questa sede appare dunque utile svolgere un sintetico esame dei contenuti della disposizione dello Statuto dei lavoratori per approfondire in che modo la stessa sia destinata ad interagire con le regole del Codice della *privacy*.

Procedendo con ordine, va subito rilevato che le ragioni della recente modifica dell'art. 4, L. n. 300/1970 sono state tradizionalmente individuate nella obsolescenza della disciplina statutaria causata dalle nuove tecnologie (Alvino, 2016; Tullini, 2017, 6) e forse, ancor più, dall'imponente evoluzione della normativa generale in materia di tutela della riservatezza (in particolare, il Codice e la sua implementazione da parte del Garante).

Volgendo lo sguardo all'art. 4 se ne può percepire, in grandi linee, l'evoluzione isolando almeno tre profili che evidenziano i tratti di continuità e discontinuità rispetto alla norma originaria contenuta nello Statuto dei lavoratori, quanto ad interessi tutelati e tecniche di regolamentazione.

Il primo concerne l'approccio al tema dei controlli a distanza tecnologici che conferma la volontà del legislatore di assoggettare questi controlli a limiti specifici finalizzati a tutelare la riservatezza del dipendente, escludendo la liberalizzazione di tali controlli.

Il secondo riguarda, nel segno della discontinuità, forme e strumenti di realizzazione della tutela del lavoratore che si caratterizzano per il declino dell'accordo sindacale come condizione generale e sufficiente di legittimità dei controlli a distanza. Infatti, il bene della riservatezza del lavoratore viene garantito dal legislatore in forme più coerenti alla dimensione individuale e personale di tale diritto, con attenzione per le modalità e la misura del controllo da correlare alle funzioni che esso legittimamente può assolvere. Ciò in coerenza con l'impostazione data alla regolazione del trattamento dal Regolamento UE 2016/679.

Il terzo profilo – che si pone in linea di sviluppo con quanto appena accennato – riguarda il raccordo, già più sopra anticipato, tra i controlli a distanza e l'utilizzabilità "*delle informazioni raccolte [...] a tutti i fini connessi al rapporto di lavoro*" (art. 4, comma 3). Un raccordo che chiarisce l'interazione funzionale dei poteri (in particolare, quelli di controllo e disciplinare) del datore di lavoro: da una parte il legittimo accertamento dell'infrazione e, dall'altra, la possibilità di sanzionarla.

Affianco a tali profili, va considerato che, pur in mancanza di una disposizione analoga a quella che si leggeva nel testo originario del comma 1 dell'art. 4, il nuovo testo continua a vietare al datore di lavoro di

avvalersi di strumenti tecnologici per controllare a distanza la prestazione del dipendente, in quanto tali controlli sono ammessi "*esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*" e, per converso, vietati in ogni altro e diverso caso.

2. La distinzione dei tre momenti della raccolta/acquisizione, della conservazione e dell'utilizzazione dei dati raccolti tramite strumenti di controllo a distanza.

Le considerazioni appena svolte consentono di mettere a fuoco alcune questioni che, specialmente nella fase applicativa della norma, hanno creato e potrebbero ancora creare incertezze e confusioni. Questioni di rilevante importanza per definire con chiarezza l'ambito della regolazione riservato alla disciplina in materia di *privacy* (Regolamento e Codice) rispetto a quello sul quale è destinato ad operare l'art. 4, L. n. 300/1970.

In questa logica, la prima questione, solo apparentemente banale, riguarda la distinzione tra esercizio del controllo a distanza ed utilizzo dei dati derivanti da tale controllo. Infatti, accade spesso che questi due aspetti vengano sovrapposti e percepiti come se fossero riconducibili ad un unico atto catalogabile come esercizio del potere di controllo. Ciò accade perché molto spesso l'avvenuto controllo, cioè l'acquisizione del dato, si manifesta in modo visibile soltanto quando si procede alla sua utilizzazione nei confronti del singolo lavoratore.

Per chiarire il punto occorre fare riferimento (almeno) a tre fasi cronologicamente e funzionalmente distinte: la prima riguarda l'acquisizione dei dati relativi all'attività lavorativa, come conseguenza automatica della tecnologia utilizzata dal dipendente per svolgere l'attività lavorativa; la seconda concerne la conservazione dei dati, cioè la loro memorizzazione; la terza – che è meramente eventuale – attiene all'utilizzazione dei dati per la gestione del rapporto di lavoro. La sequenza delle tre fasi connota e caratterizza la tipologia dei controlli tecnologici prevista dall'art. 4; controlli che, appunto, vengono definiti «a distanza» per segnare lo spazio di luogo o di tempo che intercorre tra il momento o il luogo in cui il dato inerente all'attività lavorativa viene a formarsi, quello della raccolta/acquisizione, quello della conservazione e, infine, quello dell'utilizzazione.

I limiti posti dall'art. 4 scandiscono bene (e, comunque, più nitidamente di quanto avveniva nella formulazione antecedente alle modifiche del 2015) le tutele del lavoratore con riferimento alle varie fasi, tenendo conto che il controllo a distanza si configura esaustivamente nel momento in cui il dato

viene acquisito (e memorizzato), anche prescindendo dalla sua utilizzazione che è solo eventuale.

Si potrebbe ulteriormente precisare che all'interno dell'art. 4 l'acquisizione del dato relativo all'attività lavorativa integra l'esercizio del potere di controllo secondo quanto stabilito dai commi 1 e 2; mentre il comma 3 detta le regole per l'utilizzazione del dato "*a tutti i fini connessi al rapporto di lavoro*" e ciò attiene non già al potere di controllo, bensì a quelli di gestione del rapporto di lavoro, in particolare (ma non solo) al potere disciplinare. Una distinzione che, peraltro, si riflette anche sul regime sanzionatorio previsto dall'art. 171 del Codice, che attribuisce rilievo penale alla violazione del solo comma 1 dell'art. 4 e non dei commi 2 e 3.

Alla stregua delle considerazioni accennate non appare quindi possibile sostenere, ad esempio, che i limiti al potere di controllo posti dall'art. 4 troverebbero applicazione e si attiverebbero non già nel momento in cui lo «strumento» acquisisce il dato attinente all'attività lavorativa, ma soltanto quando tale dato, seppure già residente nella memoria di un *server* aziendale, viene esaminato per valutarne la rilevanza ai fini disciplinari, cioè nel caso della sua utilizzazione. La conseguenza di una simile impostazione sarebbe infatti paradossale: l'accordo sindacale o l'autorizzazione amministrativa dovrebbero essere richiesti soltanto se il datore di lavoro fosse interessato ad utilizzare il dato, mentre è proprio l'acquisizione di esso che pone il tema della tutela della riservatezza a presidio della quale opera l'art. 4. D'altronde una simile interpretazione si rivelerebbe incompatibile anche con quanto prescritto dal GDPR ed in particolare con il principio di minimizzazione dei dati che impone che i dati siano acquisiti, a prescindere dalla loro successiva catalogazione, solo in quanto necessari alla realizzazione delle finalità legittime che hanno giustificato il trattamento.

3. La (ri)definizione e sistematizzazione dei c.d. controlli difensivi.

Prima di passare ad esaminare nel dettaglio i contenuti della nuova formulazione dell'art. 4 e a considerare il rapporto che intercorre tra le regole poste da tale disposizione e quelle dettate dal Codice e dal Regolamento, è opportuno affrontare immediatamente la questione riguardante la posizione che deve essere attribuita ai c.d. controlli difensivi rispetto al nuovo art. 4. È, infatti, necessario chiedersi se l'espressa inclusione della tutela del patrimonio aziendale, tra le esigenze che consentono l'installazione di strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori (ad opera dell'art. 23 D.Lgs. n. 151/2015), abbia prodotto il definitivo assorbimento dei controlli difensivi nell'area di applicazione della

disposizione statutaria, cosicché ora la realizzazione di tali controlli possa avvenire solo nel rispetto delle condizioni previste dal comma 1 (in tal senso: Alvino, 2016, 9; Balletti, 2018, 63; Lambertucci, 2015; Nuzzo, 2018, 51 e ss.). Ovvero, viceversa, se anche sotto il vigore della nuova formulazione, possa riconoscersi ai controlli difensivi uno statuto regolativo autonomo (cfr. in tal senso: Marazza, 2016; Maio, 2015, 1186; Maresca, 2016, 513; Proia, 2016, 547).

Per fornire una risposta a tale quesito si può inizialmente osservare che i c.d. controlli difensivi sono stati utilizzati dalla giurisprudenza per sostenere l'inapplicabilità dell'art. 4 (vecchio testo) e, quindi, la legittimità del controllo anche in assenza del preventivo accordo sindacale, atteso che oggetto del controllo sarebbe stata non già l'attività lavorativa, bensì l'illecito commesso in occasione della prestazione resa dal dipendente al datore di lavoro.

Questa tesi – mutuata da quella che ammette, *ex* art. 3 L. n. 300/1970, i controlli occulti tramite agenzie investigative finalizzati ad accertare condotte penalmente rilevanti dei dipendenti durante il servizio (cfr., tra le più recenti: Cass., 22 maggio 2017, n. 12810, in *Il Foro it., Rep. 2017, Lavoro (rapporto) n. 929*; Cass., 4 dicembre 2014, n. 25674, in *Il Foro it.,* 2015, I, 1671; Cass., 4 marzo 2014, n. 4984, in *Notiz. giur. lav.*, 2014, 486. Per la giurisprudenza di merito v., da ultimo, Trib. Padova 4 ottobre 2019, in *Riv, it. dir. lav*., 2020, II, 113) – sembra difficilmente armonizzabile con la regolamentazione dei controlli tecnologici contenuta nell'art. 4, proprio per le modalità di funzionamento di tali controlli.

Infatti, mentre l'incarico affidato ad un'agenzia investigativa può essere circoscritto alle sole indagini necessarie ad accertare la condotta illecita del singolo dipendente ed essere considerato legittimo proprio perché così delimitato, viceversa il controllo tecnologico derivante, ad esempio, dall'utilizzo di un sistema informatico registra l'insieme di tutti i dati relativi all'attività lavorativa svolta indistintamente dalla generalità dei dipendenti senza alcuna selettività, né soggettiva né oggettiva.

In questo caso, quindi, non si può configurare un controllo difensivo proprio perché il controllo non è focalizzato sull'attività illecita, ma indistintamente sulla prestazione lavorativa nel suo complesso resa da tutto il personale dipendente.

E non appare neppure possibile che tale qualificazione avvenga, per così dire a posteriori, cioè quando dall'analisi dei dati acquisiti riferita alla generalità dei lavoratori si riscontra una condotta illecita di un singolo dipendente.

Infatti, in questo caso il controllo a distanza è avvenuto quando sono stati acquisiti e memorizzati i dati relativi all'ordinaria attività lavorativa svolta dal personale dipendente ed a tale controllo trova sicura applicazione l'art. 4 la cui violazione rende illegittimo il controllo effettuato; senza alcuna pos-

sibilità che l'accertamento di comportamenti illeciti del dipendente in base ai dati complessivi già raccolti possa legittimare, con effetto retroattivo, il controllo ormai consumato.

Si può allora affermare, riprendendo le tre fasi più sopra evidenziate a cui fa riferimento la regolazione dettata dall'art. 4, che l'accertamento dell'illecito del lavoratore avviene nella fase di utilizzo dei dati a fini disciplinari, da distinguere da quella del controllo a distanza che si è consumata precedentemente con l'acquisizione dei dati.

Ciò non esclude in assoluto la possibilità di attivare un controllo realmente difensivo attraverso strumenti tecnologici al di fuori dell'ambito di applicabilità dell'art. 4, ma ciò può avvenire quando il sistema informatico (o una sua funzione) viene tarato in modo tale da accertare soltanto condotte illecite del dipendente e non già l'attività lavorativa nel suo complesso: ad esempio un *software* mirato a verificare l'autore di reati informatici.

Le considerazioni appena svolte consentono di ribadire che anche il nuovo art. 4 non si applica ai controlli difensivi – nel senso dei controlli aventi ad oggetto condotte illecite – che, conseguentemente, potranno essere attivati anche senza accordo sindacale o autorizzazione amministrativa.

Seguendo questa che sembra l'impostazione preferibile del problema, si può aggiungere che la previsione (art. 4, comma 1) dei controlli sul patrimonio aziendale dovrebbe consentire di ricondurre i controlli difensivi nel loro originario e corretto alveo.

Ciò potrebbe avvenire distinguendo tra: a) controlli a difesa del patrimonio aziendale costituito dai beni materiali ed immateriali di cui l'imprenditore ha la proprietà o il godimento e che riguardano la generalità dei dipendenti (o parte di essi) nello svolgimento della loro normale attività lavorativa che li pone a contatto con tale patrimonio. Questi controlli dovranno avvenire nel rispetto delle previsioni dell'art. 4, comma 1, ma anche del comma 3; b) controlli difensivi in senso stretto, mirati ad accertare selettivamente condotte illecite – anche di aggressione al patrimonio aziendale – di cui si presume, in base ad indizi concreti, siano autori singoli (o alcuni) dipendenti, anche se ciò avviene in occasione dello svolgimento della prestazione lavorativa. In questo caso si tratta di indagini che, salvo quelle condotte direttamente dalle autorità di polizia o dalla magistratura (il che esclude ovviamente l'applicazione dell'art. 4), possono essere attivate dal datore di lavoro avvalendosi di idonei strumenti tecnologici. Questi controlli si collocano al di fuori dell'ambito applicativo dell'art. 4, non avendo ad oggetto l'attività del lavoratore.

Peraltro tale impostazione appare perfettamente coerente con l'impostazione data alla tutela dei dati personali dal Regolamento, poiché anche in questo caso la registrazione dei dati e il loro successivo trattamento verrebbe svolto in conformità ai principi di liceità e correttezza in quanto

funzionali al contrasto e alla punizione di utilizzi illeciti degli strumenti tecnologici.

Il tema ha trovato soluzioni diverse presso la giurisprudenza di merito pronunciatasi su fattispecie ricadenti nell'ambito di applicazione dell'art. 4. Mentre secondo alcuni tribunali, conformemente all'opinione appena espressa, la categoria dei controlli difensivi volta ad accertare condotte illecite del dipendente non sarebbe stata assorbita dalla riforma all'interno della norma dello Statuto dei lavoratori (cfr.: Trib. Padova, 22 gennaio 2018, in *Dir. rel ind*., 2019, 302; Trib. La Spezia, 25 novembre 2016, in *Bollettino Adapt.it*, 2016), secondo un diverso orientamento, il riferimento espresso alla finalità di tutela del patrimonio aziendale ora contenuto all'interno dell'art. 4 comporta che anche il controllo avente la finalità di accertare la condotta illecita del dipendente debba necessariamente passare attraverso le garanzie predisposte da tale disposizione (cfr. Trib. Roma, 13 giugno 2018, in *Riv. giur. lav*., 2018 II, 562, nt. Verzaro).

Il primo orientamento sembra aver trovato una conferma nella soluzione enunciata dalla Camera Grande della Corte CEDU nella sentenza 17 ottobre 2019, *López Ribanda e altri c. Spagna*, relativa al caso della installazione da parte di un supermercato di telecamere, non visibili dal personale, in ragione del sospetto di sottrazioni formulato dal *manager* del *supermarket* sulla base delle significative perdite economiche registrate nel corso di molti mesi. In tale ipotesi, la Corte CEDU ha ritenuto compatibile con l'art. 8 della Convenzione la scelta di installare le telecamere occulte se realizzata contemperando i due interessi concorrenti al rispetto della vita privata dei lavoratori e della possibilità per il datore di lavoro di veder garantita la protezione della propria proprietà privata e di assicurare una agevole operatività della propria organizzazione aziendale, in particolare per mezzo dell'esercizio del potere disciplinare. La Corte ha infatti riscontrato come la misura fosse stata adottata nel rispetto del principio di proporzionalità, in quanto limitata rispetto ai luoghi (essendo le telecamere rivolte esclusivamente sulle postazioni di cassa) e ai tempi delle riprese (la durata dell'attività di video sorveglianza era infatti stata limitata al tempo necessario a riscontrare la fondatezza dei sospetti). Inoltre, la Corte ha rilevato che essendo le casse ubicate in un luogo pubblico, l'aspettativa di *privacy* dei lavoratori dovesse ritenersi necessariamente inferiore rispetto a quelli di altri luoghi privati (come ad es. i bagni o il guardaroba).

Su quest'ultimo punto si devono, però, ricordare anche le "*Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video*" dell'*European Data Protection Board* (EDPB) adottate il 29 gennaio 2020, in cui emerge un diverso orientamento in materia di ragionevole aspettativa di *privacy.* Infatti nel punto 37, si legge che "*nella maggior parte dei casi un dipendente sul luogo di lavoro non si aspetta di essere monitorato dal*

proprio datore di lavoro" e che "*le ragionevoli aspettative degli interessati sono quindi che non si attui alcuna videosorveglianza in tali zone*", volendo indicare che il legittimo interesse del datore di lavoro al controllo del proprio patrimonio, dovrebbe essere tutelato senza sacrificare le garanzie poste a tutela dei lavoratori.

4. Condizioni di legittimità dei controlli a distanza: l'accordo sindacale e l'autorizzazione amministrativa.

Prima di dedicarci ad esaminare in che modo la disciplina posta dall'art. 4 L. n. 300/1970 sia destinata ad interagire con quella dettata dal Codice e dal Regolamento, appare però utile brevemente ricordare che l'art. 4 distingue gli strumenti suscettibili di realizzare un controllo a distanza dell'attività lavorativa in due gruppi, a seconda che per la loro installazione sia imposto o meno il rispetto di un regime di autorizzazione.

Nel primo gruppo devono essere collocati gli strumenti, previsti dal primo comma dell'art. 4, la cui installazione sia avvenuta per far fronte ad esigenze organizzative e produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale.

In tali ipotesi l'installazione è condizionata dalla preventiva sottoscrizione di un accordo sindacale che, a differenza di quanto previsto dalla precedente formulazione, può essere stipulato con le RSA o la RSU presenti nell'unità produttiva ovvero con le «*associazioni sindacali comparativamente più rappresentative sul piano nazionale*» quando i controlli a distanza riguardano «*imprese con unità produttive ubicate in diverse province*».

Il legislatore si è così fatto carico del problema – ricorrente nella pratica – delle aziende plurilocalizzate che si avvalgono di sistemi di controllo a distanza identici da istallare nelle varie unità produttive. La trattativa con le associazioni sindacali esterne, anziché con la RSA/RSU, costituisce un'alternativa facoltativa e non già l'attribuzione di una competenza esclusiva riconosciuta a tali associazioni e sottratta alle rappresentanze sindacali costituite nell'azienda. Si tratta, quindi, di una legittimazione concorrente che implica l'eventualità di un raccordo tra le due strutture sindacali secondo prassi che caratterizzeranno le relazioni sindacali di ogni singola azienda o valutazioni effettuate di volta in volta.

In caso di mancato raggiungimento di un accordo sindacale, l'installazione dello strumento può essere autorizzata dall'Ispettorato territoriale del lavoro competente o dall'Ispettorato nazionale in caso di imprese che abbiano unità produttive ubicate in territori di competenza di ispettorati differenti.

È qui utile precisare che mentre i sindacati potranno del tutto legittimamente richiedere che i dati acquisiti dal datore di lavoro a seguito dei controlli a distanza non siano utilizzabili a fini disciplinari, tale posizione non potrà essere assunta dall'ispettorato del lavoro, nazionale o territoriale, essendo per essi impegnativa la previsione del comma 3 dell'art. 4 per la quale «*le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro*».

5. Le esenzioni riservate agli strumenti utilizzati per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze.

Il secondo gruppo di strumenti preso in considerazione dall'art. 4 è costituito da quelli per la cui utilizzazione il datore di lavoro è libero, non essendo necessario che lo stesso acquisisca la preventiva autorizzazione sindacale o amministrativa.

Rientrano in tale gruppo gli «*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*» e gli «*strumenti di registrazione degli accessi e delle presenze*».

Sottraendo tali strumenti alla necessità della preventiva autorizzazione, il legislatore muove dalla consapevolezza che tali strumenti assolvono alla funzione primaria di consentire al dipendente di rendere la prestazione e, quindi, adempiere agli impegni contrattuali che devono conformarsi all'organizzazione del lavoro come predisposta dall'imprenditore. Ha così ritenuto, in maniera condivisibile, di non poter imporre vincoli potenzialmente interdittivi all'impiego di tali strumenti, dovendo piuttosto occuparsi di tutelare il dipendente per quanto riguarda le «*informazioni raccolte*» dal datore di lavoro tramite di essi, anche perché tali informazioni sono «*utilizzabili a tutti i fini connessi al rapporto di lavoro*». A tale necessità provvede il comma 3 dell'art. 4.

Muovendo da queste premesse, si deve affrontare il nodo problematico relativo all'identificazione degli «*strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa*».

L'esame deve iniziare dalla relazione intercorrente tra gli «*strumenti*» del comma 1 e quelli del comma 2 dell'art. 4, per chiarire ciò che li differenzia: le loro caratteristiche morfologiche o piuttosto le finalità del loro impiego? La soluzione corretta appare quest'ultima, come suggerisce l'apertura del comma 2 quando avverte che «*la disposizione di cui al comma 1 non si applica* [...]»; precisazione necessaria, attesa l'insussistenza di una differenziazione ontologica tra tali «*strumenti*», per affermare l'inoperatività del comma 1 quando gli stessi «*strumenti*» siano utilizzati per le finalità del comma 2.

Quindi la distinzione tra comma 1 e 2 dell'art. 4 si coglie guardando alla funzione che gli «*strumenti*» assolvono nell'organizzazione predisposta dal datore di lavoro e non già alle loro caratteristiche oggettive (su questo tema v. anche le ricostruzioni di Alvino 2016, Del Punta 2016, Maio 2016, Marazza 2016, Salimbeni 2015).

Di qui alcune precisazioni.

La prima riguarda il termine «*strumenti*» che deve intendersi riferito alle due componenti di qualsiasi sistema informatico: l'*hardware* (dal *computer*, al *tablet*, allo *smartphone*, ecc.) che consente l'accesso ai vari tipi di *software* e di applicativi che animano il sistema ed il suo funzionamento; senza di essi le apparecchiature resterebbero inerti, anche quanto alla generazione di controlli a distanza. Quindi la riconducibilità degli «*strumenti*» nel comma 1 o 2 dell'art. 4 deve avvenire in relazione non solo all'*hardware*, ma anche e prevalentemente al *software*, quindi ai programmi a cui accede il dipendente.

Da quanto ora accennato discende anche che gli «strumenti» di cui al comma 2 non si possono identificare con gli strumenti di lavoro nel significato più tradizionale del termine, cioè di attrezzi o dotazioni individuali assegnati a ciascun dipendente per lo svolgimento del proprio lavoro. Anzi molto spesso tali strumenti si immedesimano con il/i sistema/i informatico/i di cui l'impresa si è dotata centralmente al quale si connettono i lavoratori utilizzando postazioni (periferiche) fisse o mobili per svolgere le attività di loro competenza.

L'art. 4 comma 2 non pone preclusioni per quanto riguarda gli strumenti informatici utilizzabili dai dipendenti e neppure limiti alla competenza ed alle valutazioni del datore di lavoro che, quindi, restano insindacabili anche in ragione della maggiore o minore incidenza di tali strumenti sulla riservatezza dei lavoratori. Infatti il comma 2 dell'art. 4 riguarda tutti gli «*strumenti*» accomunati dal fatto oggettivo dell'impiego da parte del prestatore a seguito delle decisioni imprenditoriali prese, come già detto, dal datore di lavoro.

Rientrano dunque in maniera pacifica tra gli strumenti di lavoro, ad esempio e per limitarsi agli strumenti oggi indispensabili, la posta elettronica e l'accesso alla rete *internet*. Con riferimento all'impiego di tali strumenti il Garante ha predisposto nel 2007 (provv. 13/2007) delle Linee guida che tuttora costituiscono il punto di riferimento per le imprese circa gli accorgimenti che devono essere adottati per realizzare l'impiego di tali dotazioni compatibilmente con la disciplina posta a protezione dei dati personali del lavoratore.

L'ambito di applicazione del comma 2 dell'art. 4 è contraddistinto anche dal fatto che gli «*strumenti*» devono servire al dipendente «*per rendere la prestazione lavorativa*». Una formulazione ampia all'interno della quale

non sembra possibile differenziare gli strumenti allorché siano utilizzati per organizzare oppure per eseguire la prestazione lavorativa, limitando a questi ultimi la previsione dell'art. 4, comma 2 e riconducendo gli altri al comma 1.

Si tratta, infatti, di una distinzione priva di riscontro testuale, in quanto l'art. 4, comma 2, prende in considerazione tutti gli strumenti che a vario titolo concorrono per consentire al lavoratore di «*rendere la prestazione lavorativa*» e ciò avviene ogni qualvolta lo stesso lavoratore si attiva per dare impulso al loro funzionamento, ma anche quando il dipendente se ne avvale (o vi accede) per acquisire dati utili per rendere tale prestazione.

Le precisazioni fin qui accennate consentono di affrontare una delle casistiche oggi più ricorrenti, quella dei sistemi di geolocalizzazione in uso al dipendente attivabili da un *tablet* o da uno *smartphone*; geolocalizzazione che appare opportuno prendere in considerazione anche per dare atto della pluralità di soluzioni prospettabili in relazione ai diversi usi di uno stesso strumento.

Il sistema di geolocalizzazione rientra tra gli strumenti previsti dal comma 2 dell'art. 4, quando è utilizzato, ad esempio, da un tecnico tenuto a rendere una prestazione lavorativa che comporta spostamenti da un luogo all'altro a seconda degli interventi da eseguire; interventi che la geolocalizzazione consente di realizzare con maggiore rapidità, segnalando al tecnico il luogo da raggiungere in quel momento più vicino.

In questo caso la geolocalizzazione permette al dipendente di rendere la prestazione lavorativa in tempi più rapidi (ed anche con minor disagio personale limitando gli spostamenti) e ciò costituisce il presupposto dell'applicabilità dell'art. 4, comma 2.

Ad una diversa conclusione si deve giungere quando la prestazione del lavoratore non è caratterizzata da alcuna mobilità territoriale, in questo caso il sistema di geolocalizzazione non è funzionale a rendere tale prestazione e, quindi, potrebbe rientrare nel comma 1 dell'art. 4 (con la conseguenza che sarebbe attivabile solo dopo l'accordo sindacale o l'autorizzazione dell'Ispettorato) sempre che sussista almeno una delle ragioni ivi previste: ad esempio la geolocalizzazione dell'auto condotta dal dipendente a tutela del bene aziendale (sul tema v. anche circ. INL 7 novembre 2016, n. 2 e provv. Garante 24 maggio 2017, n. 247).

Fin qui si è detto dei sistemi di geolocalizzazione che realizzano anche un controllo a distanza dell'attività del dipendente, ma potrebbe accadere che i dati acquisiti non siano accessibili al datore di lavoro il che esclude l'applicazione dell'art. 4; ad esempio quando il sistema è nella disponibilità della sola compagnia di assicurazione che, a fronte di questa dotazione (c.d. *black box)*, riduce il costo della polizza.

Il collegamento operato dal comma 2 dell'art. 4 tra utilizzo degli «*strumenti*» e «*prestazione lavorativa*» consente di affrontare anche la questione

relativa a quei controlli a distanza attivati dal datore di lavoro in adempimento di obblighi posti dalla legge o da una *authority* (Consob, Agcom, ecc.) a tutela degli interessi di terzi (ad esempio gli utenti di un servizio). Si tratta di casi, per limitarci solo a qualche riferimento, nei quali si deve procedere alla registrazione del colloquio telefonico nel corso del quale un dipendente raccoglie un ordine di borsa o conclude un contratto di fornitura di servizi con un utente.

In queste ipotesi la registrazione documenta non solo il contratto, ma anche l'operato del dipendente venendo così a configurare un controllo a distanza sull'attività lavorativa che sembra riconducibile nel comma 2 dell'art. 4, proprio perché la prestazione del lavoratore non potrebbe essere resa con una modalità diversa da quella che realizza il controllo a distanza dello stesso dipendente.

C'è poi da aggiungere che, in questo caso, la protezione dell'interesse dell'utente assume, secondo la valutazione espressa dall'ordinamento, carattere cogente e necessario, come tale inconciliabile con la previsione dell'art. 4, comma 1 che sottopone il controllo a distanza alla preventiva autorizzazione sindacale o dell'Ispettorato, non residuando in capo a questi soggetti alcun margine di valutazione in ordine all'attivazione del controllo ed essendo presidiata dal comma 3 (anche con il richiamo al Codice) la tutela dovuta al dipendente quanto alla sua esposizione al controllo.

Sulla scorta di questi spunti si può spostare l'attenzione su un profilo problematico relativo all'applicazione dell'art. 4, comma 2 quando si tratti di sistemi di sicurezza del lavoro il cui impiego è monitorato a distanza dal datore di lavoro con inevitabili implicazioni anche sul controllo dell'attività lavorativa.

In prima battuta tali sistemi sembrerebbero rientrare nella previsione del comma 1 dell'art. 4 che espressamente riguarda gli «*strumenti*» «*per la sicurezza del lavoro*». Ma se l'evoluzione tecnologica dovesse evidenziarne la particolare efficacia nel presidio della sicurezza del lavoratore – magari in alcuni contesti produttivi dove i rischi sono più elevati e tali da rendere necessario il potenziamento delle azioni di contrasto – si potrebbe ipotizzare che la sicurezza tecnologica così garantita al dipendente diventi una modalità della prestazione lavorativa obbligata *ex* art. 2087 c.c.

Si deve, inoltre, considerare che il comma 1 dell'art. 4 realizza – come in precedenza segnalato – un bilanciamento dei contrapposti interessi, del datore di lavoro al controllo e del dipendente alla riservatezza. Ma tale bilanciamento non può riguardare il caso in esame dove non si pone il tema della tutela degli interessi datoriali all'esercizio del potere di controllo sull'attività lavorativa, bensì quello dell'obbligo di favorire la sicurezza dei dipendenti nelle forme tecnologicamente più evolute.

In questa prospettiva si potrebbe, quindi, avviare una riflessione sul comma 1 dell'art. 4 per escluderne l'applicazione laddove il controllo a di-

stanza non sia finalizzato a realizzare un interesse del datore di lavoro quale creditore della prestazione lavorativa, quanto piuttosto quello del dipendente assoggettato sì ad un controllo a distanza, ma a tutela della sua sicurezza. Questo primo passaggio consentirebbe, poi, di ricondurre al comma 2 dell'art. 4 (e sempre nel rispetto delle tutele del comma 3) il caso in esame trattandosi di controlli derivanti dall'impiego di strumenti necessari per rendere la prestazione lavorativa, in quanto ne garantirebbero la sicurezza.

Un ultimo cenno sempre relativo all'ambito di applicazione del comma 2 dell'art. 4 riguarda la distinzione tra i controlli a distanza derivanti dall'impiego di *software* «*utilizzati dal lavoratore per rendere la prestazione lavorativa*» e l'implementazione di uno di questi *software* con funzioni aggiuntive, specificamente attivate per misurare il livello quali-quantitativo della produttività del lavoratore.

Nel caso in esame i controlli a distanza riconducibili all'art. 4, comma 2 sono quelli che derivano, secondo una non facile indagine tecnica più che giuridica, da un *software* dotato di varie funzioni sviluppate in modo integrato per lo svolgimento dell'attività lavorativa, ma che realizzano simultaneamente anche un controllo della produttività del singolo dipendente.

Se, invece, quest'ultimo controllo (sulla qualità/efficacia della prestazione) è realizzato da uno sviluppo applicativo originato dallo stesso *software* che, però, acquisisce una sua autonoma e specifica operatività rispetto alle funzioni di cui si avvale il dipendente per rendere la prestazione lavorativa, il controllo non sarà vietato dall'art. 4 se persegue «*esigenze organizzative e produttive*» del datore di lavoro, ma richiede il preventivo accordo sindacale o l'autorizzazione dell'Ispettorato essendo riconducibile al comma 1.

Appare più agevole l'identificazione degli «*strumenti di registrazione degli accessi e delle presenze*» a cui si riferisce l'art. 4, comma 2.

Con questa norma il legislatore intende, probabilmente, prendere posizione rispetto ad un orientamento della giurisprudenza – non univoco, ma accolto anche dalla Cassazione (Cass., 17 luglio 2007, n. 15892, in *Riv. giur. lav.*, 2008, II, 358, nt. Bellavista; Cass., 13 maggio 2016, n. 9904, in *Giur. it.*, 2016, I, nt. Marazza) – che affermava l'applicabilità dell'art. 4 (vecchio testo) al sistema informatizzato di rilevazione delle presenze all'inizio ed alla fine dell'orario di lavoro, in quanto idoneo a realizzare un controllo a distanza sui tempi della prestazione dovuta dal lavoratore, con la conseguenza che l'attivazione di tale sistema avrebbe dovuto essere preceduta dall'accordo sindacale o dall'autorizzazione amministrativa. Cosa che, peraltro, nella pratica avveniva molto raramente.

La norma vigente consente di ritenere superata tale questione equiparando i controlli delle presenze a quelli derivanti dagli strumenti di lavoro per i quali non occorre l'accordo sindacale o l'autorizzazione dell'Ispettorato del lavoro.

Semmai il problema interpretativo si può porre con riferimento al termine «*presenze*», perché il legislatore non precisa se si tratta soltanto di quelle che si registrano all'entrata ed in uscita e, quindi, lascia aperta la possibilità di un'interpretazione estensiva che consentirebbe l'utilizzo di strumenti in grado di monitorare a distanza la *presenza mobile* del dipendente anche all'interno dei luoghi di lavoro, vale a dire la mobilità e gli spostamenti effettuati dal lavoratore rispetto alla sua postazione.

Questa interpretazione – seppur letteralmente possibile – non appare però coerente con la *ratio* della norma che accomuna la registrazione degli accessi a quella delle presenze, evidenziando così che si tratta di due situazioni per le quali ricorre la medesima esigenza, cioè quella di acquisire un dato preciso relativo alla posizione del dipendente nel momento dell'accesso o di inizio o fine del lavoro; un dato che, attraverso il controllo, viene fissato nel tempo, tanto è vero che rispetto ad esso il legislatore ne prevede la «*registrazione*».

La rilevazione degli accessi può riguardare non soltanto l'ingresso in azienda (allorché si distingue dalla rilevazione dell'inizio dell'orario di servizio), ma anche il controllo di specifiche aree che, all'interno di uno stabilimento, sono riservate soltanto ad alcuni dipendenti, ad esempio per motivi di segretezza delle lavorazioni (oppure di sicurezza) che comportano l'esigenza di monitorare attraverso specifici varchi l'ingresso dei lavoratori.

Ci si potrebbe anche chiedere se il riferimento al controllo degli accessi di cui al comma 2 dell'art. 4, comprenda anche la connessione ai sistemi informatici aziendali.

L'estensione della regola prevista per gli accessi fisici anche a quelli informatici appare possibile sul piano interpretativo, anche se tale questione sembra assorbita e risolta alla stregua della prima parte del comma 2 nel cui ambito è più corretto ricondurre i collegamenti e le connessioni telematiche (ed i controlli a distanza che ne conseguono) effettuati dal dipendente per realizzare la prestazione lavorativa.

6. Controlli legittimi e utilizzabilità dei dati acquisiti per la gestione del rapporto di lavoro.

Nel comma 3 dell'art. 4 è racchiusa la tutela del dipendente destinata ad operare nella fase in cui, all'esito dei controlli a distanza legittimamente effettuati in conformità ai commi 1 e 2, il datore di lavoro si avvale dei dati acquisiti utilizzandoli «*per tutti i fini connessi al rapporto di lavoro*».

A ben vedere, quindi, la disposizione non riguarda l'esercizio del potere di controllo e le sue modalità, ma una fase successiva che si colloca a

valle del controllo, anzi quando esso si è esaurito, essendo le «*informazioni*» entrate nella disponibilità del datore di lavoro che potrà utilizzarle, a distanza di tempo o di luogo dal momento della loro acquisizione.

I limiti posti dal legislatore nel comma 3 operano, quindi, con riferimento non esclusivamente al potere di controllo, ma anche alla gestione del rapporto di lavoro ed ai poteri che caratterizzano tale gestione, tra i quali pure quello disciplinare. Ben potendo il datore di lavoro avvalersi delle «i*nformazioni*», ad esempio, per valutazioni relative sia alla remunerazione della prestazione lavorativa in rapporto ai risultati raggiunti sia alle competenze professionali del dipendente per il miglior impiego delle energie lavorative.

In altre parole la nuova norma opera un opportuno raccordo tra il potere di controllo tecnologico e gli altri poteri gestionali del datore di lavoro, venendo così a colmare una lacuna del vecchio art. 4 che, com'è noto, alimentava non poche incertezze applicative in ordine all'utilizzabilità dei dati derivanti dal controllo, potendosi ritenere che alla legittimità di tale controllo conseguisse ineluttabilmente la facoltà del datore di lavoro di avvalersene, ma anche, all'opposto che, il limite stabilito dal legislatore del 1970 ai controlli a distanza in funzione di «*esigenze organizzative e produttive*» o dettate «*dalla sicurezza del lavoro*» operasse pure con riferimento all'utilizzo dei dati acquisiti.

La questione si può ritenere oggi risolta con il comma 3 dell'art. 4 che incide in termini generali sulla posizione del datore di lavoro ogni qual volta decida di avvalersi dei dati raccolti. Decisione subordinata al rispetto delle due condizioni («[...] *a condizione* [...]»), indicate dal legislatore, dalle quali dipende la legittimità del controllo eseguito: a) che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli; b) che i controlli siano eseguiti nel rispetto della disciplina dettata dal D.Lgs. n. 196/2003.

Con riferimento alla seconda delle due condizioni appena indicate, ciò significa che l'analisi dei dati raccolti dallo strumento che sia stato legittimamente installato, secondo le regole sopra ricordate, deve avvenire nel rispetto dei principi generali in materia di trattamento dei dati enunciati dall'art. 5 del regolamento UE 679/2016 (cfr. Alvino 2016, Del Punta 2016, Lambertucci 2015).

Le considerazioni accennate sollecitano un duplice chiarimento per quanto concerne i soggetti destinatari della norma ed il momento in cui si configura l'utilizzabilità dei dati «*a tutti i fini connessi al rapporto di lavoro*».

Non c'è dubbio che il comma 3 dell'art. 4 riguarda il datore di lavoro, ma il suo raggio di azione appare più ampio perché in realtà coinvolge tutti i soggetti a vario titolo competenti in materia di controlli tecnologici a distanza secondo la previsione del comma 1, si tratta: dei sindacati (RSU,

RSA, ma anche dei sindacati comparativamente più rappresentativi a livello nazionale), dell'Ispettorato del lavoro (nazionale e territoriale) e dell'Autorità.

È, però, evidente che la norma non vincola i sindacati che ben potranno avanzare richieste per limitare i controlli o i loro effetti e tali richieste formeranno oggetto della trattativa con il datore di lavoro in funzione dell'eventuale accordo di cui al comma 1 (come già segnalato, ciò avverrà sicuramente con riferimento alla non utilizzabilità dei dati a fini disciplinari).

Diversamente si deve dire per l'Ispettorato e per il Garante per i quali la regola posta dal legislatore nel comma 3 dell'art. 4 risulta impegnativa e dovrà conformare il loro operato.

La seconda questione è più complessa e sottile, ma altrettanto rilevante.

Infatti si tratta di capire quando si configura (cioè dove inizia a porsi il tema dell'utilizzazione dei dati da parte del datore di lavoro che potrà avvenire soltanto nel momento in cui si saranno realizzate le condizioni imposte dal legislatore nel comma 3. Ciò significa, in altre parole, tracciare il confine tra l'esercizio del potere di controllo (commi 1 e 2 dell'art. 4) e ciò che si pone a valle di esso.

In questa prospettiva – e riprendendo questioni già accennate – appare possibile far coincidere l'utilizzazione dei dati con l'esame e la valutazione degli stessi da parte del datore di lavoro. Si tratta di un'operazione distinta e distinguibile: infatti essa è prodromica rispetto all'altra relativa ai provvedimenti che saranno adottati dal datore di lavoro, ma è successiva alla raccolta e memorizzazione dei dati.

Seguendo questo ragionamento si potrebbe dire che il datore di lavoro deve ottemperare alle condizioni poste dal comma 3 dell'art. 4 soltanto nel momento in cui decide di procedere all'esame dei dati legittimamente raccolti attraverso il sistema di controllo a distanza. Infatti soltanto dal collegamento tra tali dati ed il singolo lavoratore scaturisce per quest'ultimo la necessità di fruire delle garanzie apprestate dal legislatore.

Ne consegue che il datore di lavoro è tenuto ad ottemperare alle condizioni poste dal comma 3 dell'art. 4 allorché procede ad analizzare e valutare i dati raccolti che, pur essendo nella sua disponibilità, solo in questo caso verranno evidenziati nel loro collegamento con la prestazione del singolo lavoratore, identificandosi in ciò il primo atto di utilizzo dei dati.

Riprendendo quanto già detto, la raccolta dei dati (cioè l'esercizio del potere di controllo del datore di lavoro) dovrà avvenire nel rispetto del comma 1 dell'art. 4 (quindi previo accordo sindacale o autorizzazione dell'Ispettorato, salvi i casi riconducibili nel comma 2) a tutela della riservatezza della generalità dei lavoratori, mentre l'utilizzo dei dati postula l'«*adeguata informazione*» a protezione della posizione dei dipendenti che assume rilievo nel momento in cui il datore di lavoro decide di avvalersi di tali dati.

È necessario precisare che tale decisione non potrà riguardare *ad personam* un singolo dipendente, ma dovrà realizzarsi per tutti i dati acquisiti nei confronti dei lavoratori sottoposti al medesimo sistema di controllo a distanza, proprio perché in tal modo i dati vengono associati alla persona del prestatore di lavoro.

Sul piano applicativo le considerazioni svolte inducono ad ipotizzare la possibilità di un diverso approccio del datore di lavoro all'obbligo dell'«*adeguata informazione*» nei confronti del personale dipendente che in alcune occasioni (ad esempio per quanto attiene alla rilevazione delle presenze) sarà necessitata dall'utilizzazione routinaria di queste informazioni, mentre in altri casi avverrà se e quando il datore di lavoro intenderà avviare un esame dei dati raccolti, ma, beninteso, prima che tale esame venga esperito. Naturalmente l'ipotesi a cui si è accennato potrà porsi in concreto soltanto per quei dati che siano distinguibili e separabili, consentendo l'esame di alcuni di essi e non di altri.

7. L'informazione adeguata al lavoratore come condizione di trasparenza per l'utilizzabilità dei dati acquisiti dal datore di lavoro.

La ricostruzione del dato normativo fin qui accennata nei suoi tratti essenziali, porta a ritenere che l'informazione dovuta dal datore di lavoro *ex* art. 4, comma 3 realizza una tutela della persona del dipendente fondata sulla trasparenza. Ciò nella convinzione che l'obbligo di rendere edotto il lavoratore in ordine ai controlli a cui è sottoposto costituisce la modalità più efficace per proteggerlo non dal controllo, già avvenuto nel rispetto dei limiti previsti dal legislatore (commi 1 e 2 dell'art. 4), ma dall'utilizzo dei dati per le potenziali ripercussioni sulla posizione del prestatore nell'ambito del rapporto di lavoro (per quanto riguarda i profili disciplinari, ma non soltanto questi).

Ciò sta a significare che l'interesse del lavoratore in tal modo salvaguardato dal legislatore non è quello alla riservatezza il cui presidio è affidato, come più sopra messo in rilievo, ai principi generali sanciti dal Regolamento e dal Codice ed al bilanciamento con il potere datoriale di controllo realizzato dai commi 1 e 2 dell'art. 4, ma quello alla verificabilità del corretto procedimento di trattamento dei dati.

Infatti l'adeguata informazione imposta dal comma 3 dell'art. 4 implica la trasparente rappresentazione di tutto l'*iter* che va dalle modalità d'uso dello strumento di cui si avvale il dipendente alla raccolta dei dati relativi alla prestazione lavorativa. Ciò dovrebbe consentire al lavoratore di evidenziare errori o manipolazioni delle informazioni che il datore di lavoro inten-

de utilizzare, acquisendo elementi per difendersi di fronte a tali controlli, proprio perché esercitati con modalità palesi e non occulte.

Tale prospettiva dà quindi ragione della natura speciale dell'art. 4 rispetto all'ambito oggetto di regolazione da parte del Regolamento. Specialità che comunque permette di riscontrare la convergenza sul valore di fondo delle due discipline identificabile nell'obbligo di informazione funzionale alla piena realizzazione anche dei principi in materia di protezione dei dati personali.

A questo punto ci si deve chiedere quali siano le modalità dell'«*adeguata informazione*» da rendere al lavoratore.

Partendo dalla scontata considerazione che l'informativa, proprio perché è tale, non richiede alcuna accettazione del controllo da parte dei lavoratori che ne sono destinatari, le questioni che si pongono riguardano almeno due profili: il contenuto dell'informativa e le modalità con le quali la stessa deve essere portata a conoscenza del personale dipendente.

Quanto all'adeguatezza del suo contenuto i due riferimenti forniti dal legislatore – le «*modalità d'uso degli strumenti*» e l'«*effettuazione dei controlli*» – sembrano costituire un'endiadi utilizzata dal legislatore per chiarire le finalità stesse dell'informativa e, così, individuarne il contenuto necessario. I due riferimenti, quindi, devono essere considerati in modo concorrente e coordinato, nel senso che le modalità d'uso – delle quali occorre dare conto nell'informativa – sono quelle da cui consegue il controllo, cioè l'acquisizione dei dati relativi alla prestazione lavorativa del dipendente. Non si tratta, quindi, di redigere un manualetto di istruzioni per l'impiego dello strumento, ma di identificare le modalità del suo utilizzo che comportano l'acquisizione di dati relativi al lavoratore. In poche parole, spiegare come l'uso dello strumento si raccorda con il controllo che ne deriva.

La quantità delle informazioni da trasmettere al lavoratore non dovrà essere eccessiva, perché costituisce un dato di comune esperienza che la sovrabbondanza non favorisce la conoscibilità e la comprensione delle stesse informazioni che, anzi, richiedono un'esposizione completa, ma sintetica.

Proprio per questo appare preferibile un'informazione mirata e non generalizzata, nel senso che tale informazione dovrà riguardare gli strumenti utilizzati (o utilizzabili) dal lavoratore che così vengono ad essere identificati con riferimento ai controlli cui è sottoposto ciascun dipendente (o gruppi di lavoratori che utilizzano gli stessi strumenti). Invece un'informativa rivolta alla generalità dei dipendenti e che riguardi in modo indistinto tutti gli strumenti impiegati nell'azienda potrebbe risultare non coerente con la finalità perseguita dal legislatore di consentire la puntuale conoscenza da parte del lavoratore dei controlli ai quali è assoggettato.

Quanto appena detto consente di passare al secondo punto, cioè le modalità con le quali l'informativa deve essere portata a conoscenza dei lavo-

ratori con la consapevolezza della mancanza di un'indicazione espressa da parte del legislatore.

Per risolvere il quesito, e quindi comprendere le modalità della sua comunicazione (pubblicità), occorre partire dal contenuto dell'informazione. Se quest'ultimo non è generalizzabile per tutto il personale dipendente, in quanto gli strumenti impiegati dai lavoratori sono differenziati, i destinatari di essa saranno soltanto quei dipendenti che si avvalgono di determinati strumenti, ma non gli altri che impiegano strumenti diversi; l'estensione a questi ultimi dell'informativa dovuta ai primi potrebbe, addirittura, generare confusione.

Alla questione ora esaminata si aggiunge l'altra che riguarda la prova che il datore di lavoro dovrà fornire, in caso di contestazione in sede giudiziaria, in ordine all'adempimento degli obblighi di informazione di cui è gravato. In questo caso la ricevuta della comunicazione effettuata nei confronti di ciascun lavoratore costituisce la prova documentale più sicura, anche se la trasmissione è stata effettuata in via telematica (con una *e-mail* o mediante lettura sul sito aziendale debitamente documentata). Ciò, però, non esclude che la prova possa essere fornita anche con riferimento a modalità diverse di comunicazione, ad esempio, mediante affissione in luoghi accessibili ai lavoratori interessati.

Bibliografia: Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione tra le regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour & Law Issues*, 2016, vol. 2, I, 9; Balletti, *I poteri del datore di lavoro tra legge e contratto*, in *Dir. merc. lav.*, 2018, 63; Barbieri, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse),* in Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 183; Bellavista, *Il nuovo art. 4 dello statuto dei lavoratori*, in Zilio Grandi – Biasi (a cura di), *Commentario breve alla riforma "Jobs Act"*, Padova, 2016, 717; Califano, *Tecnologie di controllo del lavoro: limiti, procedure, garanzie*, in Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 165; Carinci M. T.*, Il controllo a distanza sull'adempimento della prestazione di lavoro*, in Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 50; Colapietro, *Tutela della dignità e riservatezza del lavoratore nell'uso delle tecnologie digitali per finalità di lavoro*, in *Giorn. dir. lav. rel. ind.*, 2017, 439; Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015)*, in *Riv. it. dir. lav.*, 2016, I, 81; Gragnoli, *Gli strumenti di controllo e i mezzi di produzione*, in *Var. temi dir. lav.*, 2016, 651; Ingrao, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Bari, 2018; Mainardi, *Il potere disciplinare e di controllo sulla prestazione*

del lavoratore agile, in Fiorillo – Perulli (a cura di)*, Il Jobs act del lavoro autonomo e del lavoro agile*, Torino, 2018, 213; Lambertucci*, Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli "a distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act),* in *WP C.S.D.L.E. "Massimo D'Antona".IT*, n. 155/2015; Maio*, La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. dir. lav.*, 2015, 1186; Marazza*, Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in *WP C.S.D.L.E. "Massimo D'Antona".IT*, n. 300/2016; Maresca*, Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *Riv. it. dir. lav.*, 2016, I, 513; Nuzzo, *La protezione del lavoratore dai controlli impersonali*, Napoli, 2018; Pinto, *I controlli "difensivi" del datore di lavoro sulle attività informatiche e telematiche del lavoratore,* in Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Torino, 2017, 139; Salimbeni, *La riforma dell'art. 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Riv. it. dir. lav.*, 2015, I, 589; Tebano*, La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *Riv. it. dir. lav.*, 2016, I, 356; Trojsi, *Controllo a distanza (su impianti e strumenti di lavoro) e protezione dei dati del lavoratore*, in *Var. temi dir. lav.*, 2016, 4, 684; Tullini*, La digitalizzazione del lavoro, la produzione intelligente e il controllo tecnologico nell'impresa,* in Tullini (a cura di), *Web e lavoro. Profili evolutivi e di tutela*, Torino, 2017, 6; 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.