

Il nuovo art. 4 l. 300/1970



di PAOLO PROVENZALI
(Ferrario Provenzali & Partners)

La l. 183/2014 ha conferito delega al Governo per la *"revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e temperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore"*.

Secondo la precedente formulazione dell'art. 4, co. 1 l. 300/1970 era *"vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori"*. Impianti e apparecchiature potevano essere installati con il solo fine di tutelare le *"esigenze organizzative e produttive"* o le esigenze di *"sicurezza del lavoro"*, e a patto che fosse raggiunto un accordo con i sindacati o fosse ottenuta un'apposita autorizzazione amministrativa.

L'art. 23, co. 1 del D.lgs. 151/2015 introduce la nuova norma. L'art. 4, co. 1 non contiene più il divieto generale di utilizzare impianti audiovisivi ed altri strumenti da cui derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, ma ne ammette l'utilizzo, purché siano rispettate precise condizioni. In sostanza è necessario che l'installazione sia preceduta da un accordo sindacale o da una autorizzazione amministrativa e che sia giustificata da specifiche esigenze aziendali. Sulla base della recente modifica legislativa, tali esigenze non sono più solo quelle *"organizzative e produttive"* e inerenti alla *"sicurezza del lavoro"*, ma anche quelle riguardanti la *"tutela del patrimonio aziendale"*, che deve essere inteso in senso ampio e quindi includere tanto i beni materiali quanto quelli immateriali, quali i marchi, i brevetti e il *know-how*. Il legislatore ha quindi inteso codificare i c.d. controlli difensivi di creazione giurisprudenziale, ammessi ove volti a sanzionare i comportamenti illegittimi del lavoratore, con il conseguente utilizzo in giudizio delle prove così acquisite.

Secondo il comma 2 del nuovo art. 4 le limitazioni previste nel comma 1 sono escluse con riferimento agli *"strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"* e agli *"strumenti di registrazione degli accessi e delle presenze"*. In tali ipotesi, dunque, il legislatore ha inteso ammet-

tere i controlli sull'attività del lavoratore a prescindere da accordi sindacali o autorizzazioni amministrative, e senza che debbano ricorrere particolari esigenze datoriali. Il comma 3, infine, detta alcune disposizioni conclusive: le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili *"a tutti i fini connessi al rapporto di lavoro"* ma 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 decreto legislativo 30 giugno 2003, n. 196"*.

Le problematiche annesse alla nuova normativa

a) La prima criticità riguarda l'individuazione di cosa costituisca strumento di lavoro. Il comma 2 dell'art. 4 esclude infatti la necessità di un accordo sindacale o dell'autorizzazione amministrativa nonché la ricorrenza di particolari esigenze aziendali, quando le informazioni vengono raccolte a mezzo degli *"strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa"*.

Sul tema, il Ministero del lavoro, con comunicato stampa del 18 giugno 2015, ne ha fornito un'interpretazione assai restrittiva, affermando che la nuova normativa non liberalizza la sorveglianza tecnologica, ma adegua la disciplina dell'art. 4 alle recenti innovazioni tecnologiche¹ e alle indicazioni che il Garante della *privacy* ha fornito negli ultimi anni, prime fra tutte le Linee guida del 2007 sull'utilizzo della posta elettronica e di internet. In particolare, il Ministero del lavoro sostiene che per tali strumenti debbano intendersi solo quelli che *"servono"* al lavoratore per adempiere alla sua prestazione, ad esempio il *pc*, il *tablet* e il cellulare. Nel momento in cui vengono modificati per controllarne l'attività (ad esempio con l'installazione di *software* di localizzazione o filtraggio), tornano ad essere necessari l'accordo o l'autorizzazione e la ricorrenza di particolari esigenze.

La lettura combinata dei commi 2 e 3 parrebbe invece ammettere che, nell'ipotesi del comma 2, il controllo sia direttamente autorizzato dalla natura intrinseca dello strumento. Inoltre, quando anche si volesse far fede all'interpretazione del Ministero del lavoro, possono individuarsi alcuni strumenti tramite cui il controllo datoriale sull'attività del proprio lavoratore dovrebbe considerarsi legittimo. Si pensi, ad esempio, allo *smartphone* conferito in uso al venditore a domicilio dotato di un'applicazione che il lavoratore consulta per i suoi

spostamenti: in tal caso non si può negare che l'applicazione con i relativi dati sia uno strumento che *"serve"* al lavoratore per rendere la sua prestazione. È invece discutibile l'utilizzo del *GPS*, talvolta installato nelle vetture aziendali, per poterne rilevare la posizione in caso di furto. In questo senso, può dirsi che lo strumento soddisfa specifiche esigenze aziendali senza costituire uno strumento di lavoro, ricadendo quindi nell'ambito di cui al co. 1. Sul punto, però, le indicazioni ministeriali ottenute sinora escludono la necessità di ogni tipo di autorizzazione, considerando il *GPS* e il veicolo un unico e inscindibile strumento di lavoro.

In base alla nuova normativa, la stessa eccezione di cui al co. 2 si applica anche agli *"strumenti di registrazione degli accessi e delle presenze"*. A tale riguardo, è possibile che il legislatore abbia voluto intendere per *"presenze"* l'entrata e l'uscita dal luogo di lavoro, mentre per *"accessi"* gli spostamenti all'interno di aree il cui ingresso è limitato ad alcuni soggetti. In questo modo, diverrebbe possibile non più solo individuare il momento di inizio e quello di fine lavoro, bensì anche il tempo in cui il lavoratore è presente e transita da un'area aziendale all'altra.

In questo contesto normativo, la corretta individuazione del significato da attribuire a tale disposizione è tanto più rilevante sol che si consideri che l'art. 23, co. 2 del D.lgs. 151/2015 ha modificato anche l'art. 171 del D.lgs. 196/2003 (c.d. Codice della *privacy*), il quale, oggi, richiama espressamente l'applicazione di sanzioni penali nell'ipotesi in cui sia violato l'art. 4, co. 1 e 2². È facile comprendere la delicatezza del ruolo che il giudice è chiamato a ricoprire: laddove escluda che la fattispecie non rientri nell'ambito di cui al comma 2, potranno applicarsi sanzioni penali.

1 Nello stesso senso sembrava disporre la l. 183/2014, la quale, come illustrato sopra, delegava il Governo alla *"revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica..."*.

2 L'art. 171 del D.lgs. 196/2003 dispone che *"La violazione delle disposizioni di cui (...) all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970"*. L'art. 38 dello Statuto dei lavoratori prevede la comminazione di una ammenda da Euro 154 a Euro 1.549 o l'arresto da 15 giorni fino ad un anno e, nei casi più gravi, l'applicazione congiunta di entrambe le sanzioni.

b) La seconda criticità della nuova disposizione investe il suo comma 3, secondo il quale i dati raccolti sia a mezzo degli strumenti ed impianti installati previo accordo o autorizzazione sia a mezzo degli strumenti del lavoratore sono utilizzabili "a tutti i fini connessi al rapporto di lavoro". Per la prima volta, la legge ammette espressamente che lo scopo del **controllo** può anche essere **disciplinare**, e quindi finalizzato a verificare il corretto adempimento della prestazione del dipendente. Tuttavia, la disposizione deve essere letta in modo coerente alle regole della disciplina generale in materia di protezione dei dati personali. Pertanto, essa non può significare una totale libertà di sorveglianza, ma piuttosto che il controllo è legittimo solo se strettamente necessario per la realizzazione di giustificati obiettivi datoriali che non possono essere soddisfatti in altro modo meno invasivo della sfera personale del lavoratore. A questo proposito, la raccomandazione del Consiglio d'Europa dell'1 aprile 2015, ancorché non abbia efficacia vincolante per gli Stati membri, contiene regole precise su come effettuare il trattamento dei dati personali e i controlli tecnologici. In particolare, la prima parte della raccomandazione (la quale si riferisce a "any processing of personal data for employment purposes") ribadisce che principale obiettivo in materia di protezione dei dati personali dei lavoratori è quello di diminuirne al minimo la circolazione e garantire la maggior trasparenza possibile nel loro utilizzo. Inoltre, ogni datore di lavoro deve tenere in considerazione le possibili implicazioni che il trattamento può avere per i diritti fondamentali e le libertà dei lavoratori. Pertanto, deve concludersi che le informazioni acquisite potranno essere usate per fini connessi al rapporto di lavoro, escludendone ogni uso eccessivo che non trovi giustificazione nell'esigenza di garantire la funzionalità del medesimo rapporto di lavoro.

Lo stesso comma 3, poi, fissa le due ulteriori condizioni che devono essere rispettate ai fini del legittimo utilizzo dei dati raccolti e, di nuovo, sia nell'ipotesi di cui al comma 1 che nell'ipotesi di cui al comma 2. In particolare è necessario che "al lavoratore sia data adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli" e che sia rispettato "quanto disposto dal decreto legislativo 30 giugno 2003, n. 196". In primo luogo, dunque, l'informazione resa al lavoratore deve essere 'adeguata', con ciò intendendosi che gli dovranno essere comunicati precisamente

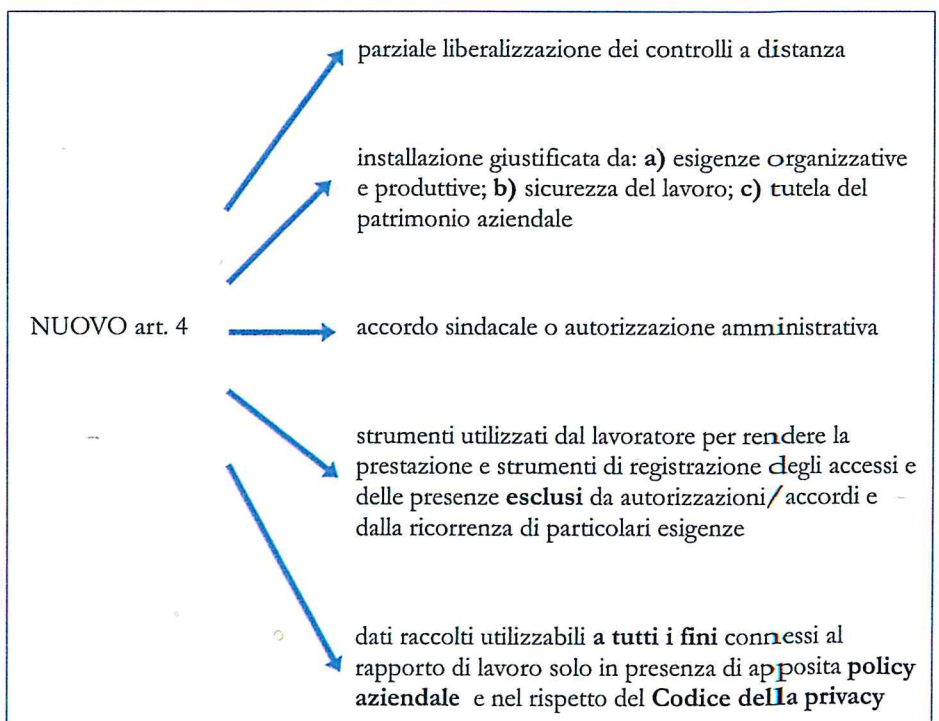
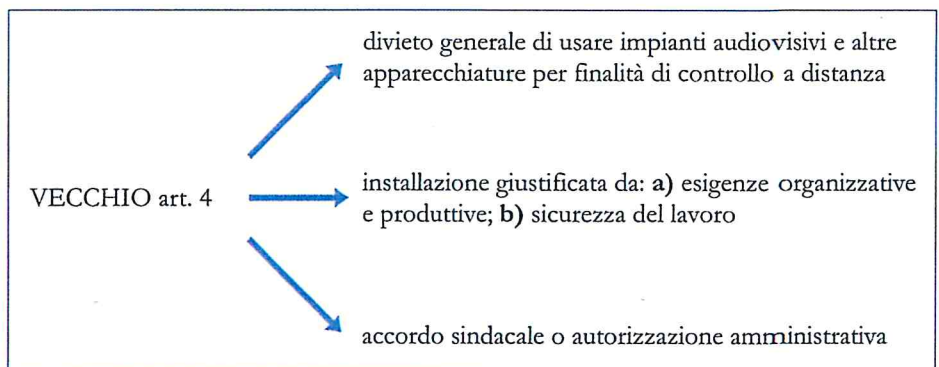
i termini e i limiti dei controlli cui può essere assoggettato. La previsione normativa si pone così in linea con la giurisprudenza secondo cui sono illegittimi i controlli effettuati ad insaputa del dipendente.

Occorre poi chiedersi se sia sufficiente rispettare il dettato dell'art. 13 del D.lgs. 196/2003 oppure se siano necessari accorgimenti ulteriori. Di certo, il datore di lavoro che intenda utilizzare i dati raccolti dovrà quantomeno osservare i principi di liceità, correttezza, necessità, determinatezza della finalità perseguita, pertinenza, completezza e non eccedenza. Ancor più in generale, occorre domandarsi se è necessario il rispetto sia delle disposizioni contenute nel D.lgs. 196/2003 sia dei provvedimenti del Garante. L'art. 154, comma 1, lett. c del Codice della *privacy*, secondo cui il Garante può prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, porta a ritenere che dovranno osservarsi entrambi. Lo stesso richiamo ministeriale, nel comuni-

cato stampa del 18 giugno 2015, alle Linee guida per l'uso della posta elettronica ed internet sul luogo di lavoro³ induce a muovere nella medesima direzione. In tal caso, tra i tanti, sarà necessario considerare: il Provvedimento del Garante del 12 novembre 2014 recante le *Linee guida in materia di riconoscimento biometrico e firma grafo metrica* (per l'utilizzo di strumenti che usano dati biometrici, come le impronte digitali al posto di semplici *badge*); l'Autorizzazione Generale n. 1/2014 sul trattamento dei dati sensibili dei lavoratori; il Provvedimento del Garante dell'8 aprile 2010 in materia di videosorveglianza; le *Linee guida in materia di trattamento dei dati dei lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati* (Deliberazione 53/2006) e *pubblici* (Deliberazione 23/2007).

Conclusioni

Se da un lato il divieto generale di cui al vecchio art. 4, co. 1 appare soppresso, allo stesso tempo, sol che si considerino i limiti



Cronaca Nazionale - Torino 7 aprile 2016

Innovazione e mercati internazionali nel settore ferroviario

posti dalla nuova disciplina, la liberalizzazione tecnologica operata dal D.lgs. 151/2015 non può certamente ritenersi integrale.

Quanto agli impianti e agli strumenti di cui al comma 1 dell'art. 4, la nuova disciplina ricalca la precedente, richiedendo accordi sindacali o autorizzazioni amministrative e specifiche esigenze che devono essere "esclusivamente" quelle indicate al nuovo comma 3. Diversi orientamenti si riscontrano già per quanto concerne l'individuazione di ciò che può costituire strumento di lavoro.

La norma è ben lungi dall'ammettere in modo incondizionato controlli sull'attività dei lavoratori. Certo è che, nel caso di unilaterale attivazione dei controlli datoriali che siano privi di un espresso accordo sindacale o di una autorizzazione amministrativa, sarà altamente probabile un contenzioso. Senza dubbio, per i datori di lavoro che intendano utilizzare le informazioni raccolte, è quanto mai necessario definire una **policy interna** che, per usare le parole del Garante, dovrà essere redatta "in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (...) e da sottoporre ad aggiornamento periodico"⁴.

3 Sul trattamento effettuato sulle e-mail dei dipendenti, si veda anche il recente Provvedimento del 30 luglio 2015 con cui il Garante ha ritenuto illegittimo il trattamento dei dati effettuato dalla società che non aveva immediatamente chiuso l'account di alcuni ex dipendenti e non aveva impostato un messaggio automatico sugli stessi che informasse i terzi della chiusura medesima, nonostante si fosse accorta di come gli ex dipendenti continuavano a gestire al di fuori dell'azienda affari che la stessa credeva chiusi da tempo. Ha infatti statuito che "il datore di lavoro, pur avendo la facoltà di verificare l'esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità e, in applicazione dei principi di liceità e correttezza dei trattamenti di dati personali, informare in modo chiaro e dettagliato circa le consentite modalità di utilizzo degli strumenti aziendali e l'eventuale effettuazione di controlli anche su base individuale"; inoltre "l'assenza di una esplicita policy di riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione".

Vedi "Linee guida del Garante per posta elettronica e internet" del 10 marzo 2007.



di GIORGIO BORELLO
(Socio CDAF)

Un mercato mondiale da 150 miliardi di euro anno.

Nell'ambito di EXPO Ferroviaria 2016 al Lingotto Fiere di Torino, si è svolto il Workshop "Innovazione e mercati Internazionali nel settore ferroviario" con obiettivo le tendenze della tecnologia ferroviaria nel breve e medio termine, derivanti dai bisogni della mobilità con ricadute sui mercati in termini di ristrutturazione del sistema industriale a livello globale. L'iniziativa è inserita nel Progetto Integrato di Filiera (PIF) Torino Piemonte Railway gestito dal Centro Estero per l'internazionalizzazione (Ceipiemonte).

Sono arrivate interessanti testimonianze da Ansaldo STS e da due attori industriali operanti in Turchia e Iran: Aselsan Group e MAPNA; questi ultimi hanno sottolineato le grandi opportunità che si aprono in questo settore per le nostre imprese nei rispettivi Paesi.

Relativamente all'innovazione del settore ferroviario, per sottolineare gli orientamenti di sviluppo e innovazione individuati dall'UE e dall'industria e le prospettive di sviluppo economico l'innovazione di questo settore è assistita dal finanziamento del Programma Pubblico Privato SHIFT2Rail che fa parte del programma generale HORIZON 2020.

Shift2Rail è la prima iniziativa ferroviaria tecnologica congiunta europea di ricerca mirata, innovazione e soluzioni di mercato accelerando l'integrazione di nuove e avanzate tecnologie in soluzioni innovative di prodotto ferroviario. Il programma pro-

muove la competitività dell'industria ferroviaria europea ed è in grado di soddisfare le mutevoli esigenze dei trasporti dell'Unione Europea.

Molti sono gli obiettivi presi in esame nel convegno, tra questi primeggia il raggiungimento di velocità sempre più elevate: già oggi il treno più veloce è cinese il CRH380A che viaggia a quasi 500 km ora ma anche noi in Italia con il Frecciarossa 1000 abbiamo raggiunto la velocità commerciale di quasi 400 Km ora che significa collegare Torino e Milano in circa 20 minuti (al netto dei rallentamenti).

Ma per avere veramente grandi velocità elevate occorrono nuove tecnologie quale ad esempio il Maglev, una modalità di trasporto innovativa anche se in continuo studio e perfezionamento da molti anni. Il Maglev è un treno a levitazione magnetica in servizio commerciale a Shanghai dove collega la città con l'aeroporto viaggiando a oltre 400 Km ora (ma può arrivare a 600 Km).

Altra modalità allo studio è il ripescaggio delle monorotaie che sembra avere un futuro interessante.

Altri obiettivi sono quelli di raddoppiare la capacità di trasporto di passeggeri e merci, ma molte innovazioni sono attese da altri settori quali i sistemi di controllo, automazioni, design, attrattività, smart materials, connettività Wireless, riduzione dei pesi e l'utilizzo della mecatronica.

Da quanto evidenziato al convegno è emersa una interessante possibilità di lavoro per le aziende piemontesi dei settori dei sistemi, elettrificazione, segnalamento, servizi di ingegneria, manutenzione, riparazioni, revamping e armamento ferroviario. Come detto, in primis su queste tematiche a breve, già oggi Turchia e Iran, ma a seguire Cina, India, Europa, Paesi del Golfo e area NAFTA (Usa, Canada e Messico).

