LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con le norme di oggi.

LORENZO CAIRO
Studio Legale Gattai, Minoli, Agostinelli & Partners

vol. 2, no. 2, 2015

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con le norme di oggi.

LORENZO CAIRO
Studio legale Gattai, Minoli, Agostinelli & Partners
lcairo@gattai.it

ABSTRACT

Last September, the legislation concerning remote monitoring of employees underwent a reform (Legislative Decree No. 151/2015 which amended Article 4 of Law No. 300/1970, article 4). The article aims at analyzing the practical effects of such reform.

To this end, the article focuses on three case-law precedents, decided under the previous legislation, and hypothesizes how they could be solved in light of the new regulation.

The main issues examined are the following:

- Limits to the gathering of evidence: according to the reform, evidence gathered through devices which allow for remote monitoring of employees can be used, as long as such devices have been lawfully installed in compliance with the requirements set out by Article 4 (prior agreement with works council or authorization from the local body of the Labour Ministry). The article addresses the consequences in the event that the devices in question have been unlawfully installed. In particular, it discusses whether the employer is prevented from producing evidence so gathered in Court.
- Under the new regulation, devices used by employees in the performance of their work activities is not subject to any prior agreement or authorization. However, the definition of what constitutes a "device used in the performance of work activities" is not entirely clear. Thus, identifying what kind of devices can or cannot be installed without any prior formality remains uncertain. As such, the article focuses on the issue of whether a personal

computer can be considered a device falling within the scope of Article 4. It also further examines whether hardware and software should be considered separate "devices" and whether they can be separately considered in order to assess whether the formal requirements of Article 4 should apply.

Monitoring of employees suspected of having committed unlawful acts affecting the employer's assets (so-called *defensive controls*): the reform has now included such types of controls as falling within the scope of Article 4. Prior to the reform and according to consistent case-law precedents, the same types of controls were not considered subject to any prior requirement. The article analyses the potential implications of this new provision on the jurisprudence relating to defensive controls.

Keywords: employer's monitoring powers; employee's dignity; employee's privacy; defensive controls.

Il controllo a distanza dei lavoratori: precedenti nella giurisprudenza di ieri decisi con le norme di oggi.

SOMMARIO: 1. Cass., sez. lavoro, 23 febbraio 2010, n. 4375. – 2. Garante Privacy, provvedimento 2 aprile 2008. – 3. Cass., V sez. penale, 1 giugno 2010, n. 20722.

Come cambia in concreto la disciplina dei controlli a distanza? Per rispondere a questa domanda prendiamo tre casi, due risolti dalla Corte di Cassazione, uno dal Garante per la Protezione dei Dati Personali quando era in vigore il testo dell'art. 4 Stat. Lav. precedente alla riforma del 2015 (D. Lgs. 14 settembre 2015, n. 151) e proviamo a vedere come gli stessi casi potrebbero essere risolti alla luce del nuovo testo.

I casi che esamineremo sono:

1) **Cass., sez. lavoro, 23 febbraio 2010, n. 4375**, relativa a un controllo fatto mediante un software installato sul computer in dotazione a una dipendente. Il controllo era relativo agli accessi a Internet effettuati da una lavoratrice su siti non attinenti all'attività lavorativa.

2) **Garante Privacy, provvedimento 2 aprile 2008, doc. web. 1519695**, relativo a un controllo sulla posta elettronica di alcuni dirigenti effettuato direttamente sul personal computer aziendale assegnato agli stessi dirigenti. Il controllo era stato effettuato nell'ambito di un'investigazione interna per l'accertamento di eventuali condotte illecite.

3) **Cass., V sez. penale, 1 giugno 2010, n. 20722**, relativa a un controllo effettuato mediante installazione di videocamera nascosta, orientata su un dipendente sul quale si erano appuntati sospetti di appropriazione indebita.

1. Cass., sez. lavoro, 23 febbraio 2010, n. 4375.

(a) Il caso risolto dalla sentenza

Una lavoratrice veniva licenziata a seguito di procedimento disciplinare, in cui le era stato contestato un reiterato utilizzo di Internet per fini privati, non conforme al regolamento aziendale. Gli accessi contestati erano stati rilevati dal software SuperScout, che consentiva la registrazione automatica di tutti i siti visitati dai dipendenti. Tale strumento era stato installato senza previo accordo sindacale, né autorizzazione della competente direzione territoriale del lavoro. La lavoratrice proponeva ricorso ex art. 700 c.p.c. all'esito del quale veniva reintegrata ai sensi dell'art. 18 Stat. Lav., testo precedente alla riforma del 2012. Il

Giudice riteneva, in particolare, illegittimo il licenziamento perché le prove della condotta illecita erano state raccolte in violazione dell'art. 4, secondo comma, Stat. Lav. In assenza di prove (lecitamente acquisite) della condotta illecita, il licenziamento veniva quindi ritenuto illegittimo.

Una volta reintegrata, la lavoratrice veniva licenziata nuovamente all'esito di una seconda contestazione. Tale contestazione aveva ad oggetto altri indebiti accessi a siti Internet non attinenti all'attività lavorativa oltre ai fatti già contestati nella precedente procedura disciplinare. Nell'ambito del secondo procedimento disciplinare, i dati relativi alle connessioni erano stati ricavati mediante accesso diretto al personal computer della lavoratrice.

Con sentenza del 31 marzo 2004, il Tribunale di Milano (1) dichiarava l'illegittimità di entrambi i licenziamenti: il primo, in quanto le prove dei fatti che fondavano la contestazione erano stati reperite in violazione dell'art. 4, secondo comma, Stat. Lav.; il secondo, per la tardività della contestazione. Veniva quindi disposta la reintegrazione della lavoratrice con sentenza successivamente confermata in appello (2).

Il datore di lavoro ricorreva quindi in Cassazione.

La Suprema Corte rigettava il ricorso confermando la decisione della Corte d'Appello di Milano, secondo cui «*i programmi informatici che consentono il monitoraggio della posta elettronica e degli accessi ad Internet sono strumenti di controllo allorquando consentono al datore di lavoro di controllare a distanza e in via continuativa l'attività lavorativa. In tal caso, la loro installazione è soggetta alla disciplina di cui all'art. 4 l. n. 300/70. La violazione di tale disciplina rende inutilizzabili i dati acquisiti per eventuali sanzioni disciplinari*». La Corte di Cassazione riteneva inoltre infondate le censure mosse dal datore di lavoro relativamente all'inapplicabilità dell'art. 4 Stat. Lav. per la natura difensiva del controllo in questione, confermando il principio (già espresso dalla stessa Corte di Cassazione con la sentenza 17 luglio 2007, n. 15892 (3)) secondo cui «*l'insopprimibile esigenza di evitare condotte illecite non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore, per cui tale esigenza non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti. In tale ipotesi si tratta, infatti, comunque di un controllo c.d. "preterintenzionale" che rientra nella previsione del divieto "flessibile" di cui all'art. 4 citato, comma 2*».

(1) In *OGL*, 2004, 108, con nota di L. Cairo.

(2) Corte d'Appello Milano, 30 settembre 2005 in *D&L*, 2006, 899, con nota di S. Chiusolo.

(3) In *RIDL*, 2008, 714, con nota di M.L. Valluri.

(b) Possibile risoluzione del caso alla luce del nuovo testo

Nel caso in esame gli strumenti utilizzati per raccogliere le prove della condotta illecita sono due: il software SuperScout, utilizzato nel primo procedimento disciplinare, e il personal computer, utilizzato nel secondo procedimento.

(*i*) Sullo strumento utilizzato nel primo procedimento disciplinare: il software Superscout

Il primo procedimento disciplinare si fondava su informazioni reperite dal datore di lavoro per mezzo del software SuperScout. Da una descrizione reperibile sul sito www.software.it, queste sono le caratteristiche del SuperScout:

- Tiene traccia di tutti i siti visitati in Internet, nonché dei messaggi di posta elettronica.
- Può visualizzare l'accesso Internet per tutta la rete, per un segmento, per un dipartimento o per la singola *workstation*.
- Attiva il controllo e la gestione dell'accesso Internet: le regole possono consentire il filtro e il blocco della navigazione e il controllo sulla connessione abilitata e impedita agli utenti, workstation e gruppi, intervalli di orari e date, liste URL, gruppi URL, domini, indirizzi IP, protocolli e *Control List*.

Si tratta, in definitiva, di un software la cui funzione è proprio quella di monitorare continuativamente gli accessi a Internet con lo scopo di mantenere la sicurezza del sistema informatico. Tale funzionalità primaria non esclude – anzi implica – la possibilità di effettuare un controllo continuo sull'uso che il lavoratore fa di Internet per tutto il tempo in cui è al lavoro. Nessun dubbio quindi che il SuperScout ricada nel campo di applicazione dell'art. 4, primo comma, Stat. Lav. nuovo testo. Esso fa riferimento a "*strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori*" utilizzati per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Il nuovo primo comma della norma (così come il secondo comma del vecchio testo) prevede che questi strumenti possano essere installati e successivamente utilizzati previo accordo sindacale o, in mancanza, previa autorizzazione da parte della Direzione Provinciale del Lavoro competente.

La norma individua strumenti la cui destinazione d'uso sia "altra" rispetto al controllo dell'attività dei lavoratori, ma che possano consentire un simile controllo come effetto, per così dire, collaterale. Il SuperScout nasce come strumento per la sicurezza informatica, ma può consentire il controllo a distanza dell'attività dei lavoratori: si tratta di uno strumento che ha le caratteristiche e le

finalità d'uso individuate dal primo comma dell'art. 4 e, quindi, dovrebbe essere soggetto alle formalità preliminari all'installazione previste dalla norma.

A questo punto, è necessario chiedersi se questo software rientri nell'eccezione del secondo comma dell'art. 4 Stat. Lav., secondo cui gli strumenti utilizzati dal lavoratore per rendere la prestazione non sono soggetti ad accordo sindacale o autorizzazione amministrativa. La risposta, nel caso di specie, è no: il SuperScout non viene utilizzato per svolgere la prestazione. Si tratta di un software che può essere installato su ciascun computer (o sul server aziendale che distribuisce la connessione a Internet agli altri computer) che però non serve al funzionamento del computer, né è essenziale per svolgere attività utili al lavoro (come le applicazioni *word*, *excel*, ecc.). Non è quindi applicabile l'eccezione del secondo comma del nuovo testo.

Né la finalità di tutela del patrimonio aziendale del controllo operato tramite il SuperScout potrebbe determinare la disapplicazione del primo comma dell'art. 4. Tali finalità sono comprese nel nuovo testo del primo comma dell'art. 4 tra quelle che legittimano l'uso di strumenti di controllo a condizione che l'installazione sia preceduta da un accordo sindacale o da un'autorizzazione amministrativa.

Sotto questo profilo, il legislatore sembra avere cristallizzato nel nuovo testo dell'art. 4, l'orientamento della giurisprudenza precedente alla riforma (per la verità minoritario), al quale la sentenza in esame aveva aderito, secondo il quale *«l'insopprimibile esigenza di evitare condotte illecite non può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore, per cui tale esigenza non consente di espungere dalla fattispecie astratta i casi dei c.d. controlli difensivi ossia di quei controlli diretti ad accertare comportamenti illeciti. In tale ipotesi si tratta, infatti, comunque di un controllo c.d. "preterintenzionale" che rientra nella previsione del divieto "flessibile" di cui all'art. 4 citato, comma 2».*

Dunque, sia in punto di qualificazione dello strumento, sia sotto il profilo delle finalità per le quali esso è stato utilizzato, se dovessimo decidere oggi il caso in esame sulla base della nuova normativa potremmo verosimilmente arrivare, sul SuperScout, a una prima (identica) conclusione: l'installazione del SuperScout doveva essere preceduta da un accordo sindacale o da un'autorizzazione amministrativa e dalla consegna di un'informativa ai lavoratori ai sensi dell'art. 13 D. lgs. 196/2003 (di seguito anche *Codice Privacy*).

Raggiunta questa prima conclusione è ora necessario capire quali siano le conseguenze.

La sentenza in esame, confermando la decisione della Corte d'Appello, affermava piuttosto chiaramente che «non può essere attribuito alcun valore

probatorio ai dati acquisiti in violazione dell'art. 4 Stat. Lav., che sono dunque non utilizzabili in causa» (cfr. Corte d'Appello Milano, 30 settembre 2005 cit, che richiama come precedente conforme Cass. 17 giugno 2000, n. 8250). Dal che discendeva l'infondatezza del fatto contestato e quindi l'illegittimità del licenziamento, con le conseguenze previste dalla legge all'epoca vigente (cioè la reintegrazione secondo l'art. 18 Stat. Lav. pre-riforma Fornero).

A una prima lettura del nuovo testo della norma, sembrerebbe scontata una conferma anche di questa seconda conclusione. Il nuovo testo dell'art. 4 peraltro, a differenza del vecchio, prevede la possibilità di utilizzare i dati raccolti nel rispetto dell'art. 4 e della disciplina rilevante in materia di trattamento dei dati personali "per tutti i fini connessi al rapporto di lavoro" (cfr. terzo comma del nuovo art. 4). Il che equivale ad affermare l'impossibilità di utilizzare i dati raccolti se la normativa in questione viene violata.

Su quest'ultimo punto è però opportuna una riflessione di natura processuale per comprendere la reale portata del nuovo terzo comma della norma.

Il nuovo terzo comma dell'art. 4 ricalca (in positivo) la previsione dell'art. 11, secondo comma del Codice Privacy che recita: «I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati». Rispetto a quest'ultima previsione, il nuovo terzo comma dell'art. 4 nulla aggiunge. L'art. 4 è infatti richiamato dall'art. 114 del Codice Privacy del quale, quindi, fa parte. Ne deriva che l'art. 4 costituisce "disciplina rilevante in materia di trattamento dei dati personali" la cui violazione, già prima della riforma del 2015, ben poteva essere sanzionata con l'inutilizzabilità dei dati ai sensi dell'art. 11, secondo comma del Codice Privacy.

Al di là di questa precisazione è opportuno chiedersi se sia veramente fondata (ieri come oggi) la trasposizione in termini processuali del divieto di utilizzabilità dei dati sancito dalle due norme sopra richiamate. In particolare, l'inutilizzabilità del dato acquisito in violazione della norma ai a sensi dell'art. 4, terzo comma Stat. Lav. e dall'art 11, secondo comma del Codice Privacy si traduce in inammissibilità della prova in giudizio?

La questione è di particolare rilievo dal 2012. L'art. 18 Stat. Lav. come modificato dalla riforma Fornero prevede infatti diverse tutele a seconda che il vizio del licenziamento disciplinare colpisca la sostanza (in particolare, la sussistenza del fatto) oppure la forma (il fatto sussiste ma il procedimento è viziato). Lo stesso vale per i casi in cui si applichi la tutela prevista dal Jobs Act (art. 3, D. Lgs. 23/2015) che prevede la reintegrazione nei licenziamenti disciplinari, in caso di insussistenza del fatto materiale.

È dunque oggi interessante chiedersi se il divieto di utilizzabilità del dato incida sulla capacità di provare in giudizio la sussistenza del fatto materiale, poiché su questo punto si spiega la tutela più forte prevista dalla legge.

In passato, parte della dottrina già aveva sostenuto che le prove acquisite illecitamente fossero utilizzabili nel processo civile. Esse conserverebbero il loro valore probatorio principalmente perché il codice di procedura civile non prevede una disposizione analoga all'art. 191 c.p.p. secondo il quale "Le prove acquisite in violazione dei divieti stabiliti dalla legge non possono essere utilizzate" (4).

Oltre a questo argomento si potrebbe sostenere che il divieto di utilizzazione dei dati stabilito dall'art. 4, terzo comma, Stat. Lav. e dall'art. 11, secondo comma del Codice Privacy limita il datore di lavoro / titolare del trattamento, non il Giudice, che non è soggetto passivo della norma.

Questa distinzione è stata proposta da un'interessante (e per la verità isolata) sentenza del Tribunale di Torino del 2007 con riferimento proprio all'art. 11, secondo comma del Codice Privacy (5). Il caso aveva ad oggetto un procedimento disciplinare per utilizzo improprio da parte di un lavoratore del telefono e del computer aziendali, concluso con il licenziamento per giusta causa. I dati relativi alla contestazione erano stati reperiti mediante accesso ai tabulati dell'utenza telefonica assegnata al dipendente (intestata alla società) e al computer aziendale.

Nel merito, rispondendo a una specifica eccezione di inammissibilità della prova, il Giudice aveva ritenuto che la normativa privacy non fosse stata violata. La sentenza toccava comunque il tema dell'acquisizione della prova precostituita, assunta in violazione di norme di legge – e in particolare in violazione del Codice Privacy. Al riguardo, si legge: «l'inutilizzabilità del trattamento dei dati personali reperiti in violazione della disciplina vigente in materia è riferibile unicamente ai destinatari delle prescrizioni del Codice della privacy, onde non si converte automaticamente in divieto probatorio per il Giudice, ancorché nel processo risultino prodotti atti, documenti o provvedimenti basati su trattamento di dati personali non conforme a disposizioni di legge o di regolamento».

Questo principio, sebbene espresso in relazione all'art. 11, secondo comma del Codice Privacy, potrebbe essere invocato dal datore di lavoro per ottenere l'ammissione in giudizio delle prove reperite in violazione dell'art. 4, terzo comma, Stat. Lav. che, come detto, ha una formulazione in tutto equivalente alla richiamata norma del Codice Privacy.

(4) G.F. Ricci, *Le prove illecite nel processo civile*, *RTDPC*, 1987, 34.

(5) Trib. Torino 28 settembre 2007, in *ADL,* 2008, 1265, con nota di D. Iarussi.

Il principio in questione appare coerente con il contesto normativo e sostenibile con buoni argomenti (in sintesi: l'art. 4 terzo comma – così come l'art. 11 del Codice Privacy – si rivolge al datore di lavoro / titolare del trattamento, non al Giudice, né può attribuirsi rilevanza processuale al divieto di utilizzazione dei dati, in mancanza, nel processo civile e del lavoro, di una norma equivalente al richiamato art. 191 c.p.p.). In concreto, sarà piuttosto difficile che un simile orientamento possa imporsi: se così fosse, la violazione dell'art. 4 nel contesto di licenziamenti disciplinari, finirebbe per non avere, di fatto, alcun effetto (al più si potrebbe identificare un vizio formale nel procedimento disciplinare in quanto fondato su dati che non potevano essere utilizzati, vizio per il quale non è prevista la tutela reintegratoria).

(*ii*) Sullo strumento utilizzato nel secondo procedimento disciplinare: il personal computer

Il secondo licenziamento esaminato dalla Corte di Cassazione è stato dichiarato illegittimo per mancanza di tempestività. Nulla è stato detto circa le modalità con le quali i dati alla base della contestazione sono stati raccolti, ossia mediante accesso diretto ai computer aziendali. Il vizio di tempestività opera in via preliminare, cioè sul contenuto della contestazione per come si presenta, senza necessità di verifica della fondatezza dei fatti. Non è possibile quindi ricavare indicazioni utili dalla sentenza in esame circa l'utilizzabilità dei dati acquisiti mediante personal computer. Nella sentenza in esame manca infatti una riflessione sulla qualificazione, alla luce dell'art. 4 vecchio testo, del personal computer come strumento che può consentire il controllo a distanza.

Su questo punto è di particolare interesse il secondo provvedimento in esame.

2. Garante Privacy, provvedimento 2 aprile 2008.

(a) Il caso risolto dal Garante Privacy

Una società aveva svolto una investigazione interna nei confronti di alcuni dirigenti sospettati di comportamenti illeciti (alcuni dei quali penalmente rilevanti). Tra le varie attività di verifica, veniva esaminato il contenuto della casella di posta elettronica mediante accesso diretto ai singoli computer in dotazione ai dirigenti sottoposti a indagine. I dirigenti in questione erano stati preventivamente informati per iscritto sulle finalità e modalità del controllo. Nessun accordo sindacale era stato stipulato, né era stata ottenuta un'autorizzazione amministrativa ai sensi dell'art. 4, secondo comma, Stat. Lav. in relazione alle

procedure di controllo mediante accesso diretto ai computer aziendali. In tal caso il Garante Privacy ha ritenuto illecito il trattamento di dati affermando che «*con riferimento all'osservanza delle normative di settore (presupposto anch'esso rilevante per la liceità e correttezza del trattamento), occorre rilevare che non risulta acquisita agli atti documentazione comprovante l'avvenuto espletamento, da parte di M. S.p.A., delle procedure previste dall'art. 4 dello statuto dei lavoratori per il controllo a distanza dell'attività lavorativa, ipotesi che nel caso di specie deve ritenersi sussistente ben potendosi, a distanza di tempo, mediante l'elaborazione da parte del team investigativo della K. delle informazioni desumibili dall'invio della corrispondenza (anzitutto esaminandone la cronologia), effettuarsi un controllo dell'attività lavorativa effettuata dal reclamante*».

(b) Possibile risoluzione del caso alla luce del nuovo testo

Applicando il nuovo testo dell'art. 4 Stat. Lav., il caso in esame potrebbe essere risolto in maniera totalmente differente.

Soffermiamoci per un momento sulle conclusioni raggiunte dal Garante. La violazione dell'art. 4 vecchio testo, veniva rilevata per il mancato espletamento delle formalità previste dall'art. 4 *"per il controllo a distanza dell'attività lavorativa"*, ipotesi che nel caso di specie veniva ritenuta sussistente «*ben potendosi, a distanza di tempo, mediante l'elaborazione […] delle informazioni desumibili dall'invio della corrispondenza (anzitutto esaminandone la cronologia), effettuarsi un controllo dell'attività lavorativa effettuata dal reclamante*».

Questa formulazione sintetizzava tutti i limiti applicativi del vecchio testo dell'art. 4. Si trattava infatti di una formulazione oscura che faceva riferimento alle procedure di cui all'art. 4 "per il controllo a distanza" (ma oggetto della norma non era – e non è – il "controllo", bensì lo strumento di controllo).

In altre parole il Garante affermava la violazione dell'art. 4 senza sbilanciarsi sulla natura dello strumento utilizzato per controllare. Non si parlava infatti delle caratteristiche dello strumento in questione ma dei "dati desumibili dall'invio dalla corrispondenza". La decisione non distingueva, come avrebbe dovuto, l'azione del controllo, l'oggetto del controllo (la posta elettronica) e lo strumento usato per controllare (il computer). L'affermazione del Garante si prestava quindi a due interpretazioni:

- l'installazione dello strumento utilizzato (il computer) non è di per sé soggetto a formalità preliminari mentre è la procedura di controllo a dovere essere concordata con le rappresentanze sindacali o autorizzata dall'ispettorato del lavoro;
- il computer, in quanto strumento che ha reso possibile il controllo, deve qualificarsi come strumento che consente il controllo, la cui installazione deve

ritenersi soggetta al previo esperimento delle procedure dell'art. 4, secondo comma, vecchio testo.

La prima interpretazione era chiaramente contraria al testo (e alla funzione della norma). Essa avrebbe implicato una interpretazione dell'art. 4 tale da prescindere dall'esistenza di una apparecchiatura di controllo fino a includere il controllo in sé, ossia l'azione del controllo indipendentemente dallo strumento utilizzato.

La seconda interpretazione, più aderente alla lettera della norma, poneva degli interrogativi di ordine pratico di una certa rilevanza. Si sarebbe infatti dovuto concludere che un'impresa, prima di mettere in funzione dei computer, avrebbe dovuto esperire le procedure di cui all'art. 4, secondo comma Stat. Lav.; Il che, da un punto di vista pratico, non sembra nemmeno ipotizzabile.

Il risultato era una decisione che risolveva il caso concreto senza però fornire indicazioni certe su come comportarsi, in termini generali, circa l'installazione dello strumento in questione. E non parliamo di uno strumento qualunque ma del personal computer ossia dello strumento divenuto ormai la base quotidiana di qualsiasi attività lavorativa.

Come accennato sopra, questo caso evidenzia come la norma, che pure aveva avuto il merito di reggere il passo di quarant'anni di evoluzione tecnologica, fosse entrata in sofferenza rispetto alle caratteristiche degli strumenti di lavoro entrati stabilmente, negli ultimi anni, nell'organizzazione delle imprese.

Il vecchio testo dell'art. 4 risaliva infatti agli anni '70, epoca nella quale era ancora piuttosto precisa la differenza tra strumenti di lavoro e strumenti di controllo. Non a caso la norma nasce sul paradigma degli impianti di videosorveglianza. Allo stesso modo non era un caso che il secondo comma della norma parlasse di "impianti e le apparecchiature *di controllo* che siano richiesti da esigenze organizzative e produttive…". Il perimetro della norma catturava quindi solo strumenti la cui destinazione d'uso fosse controllare qualcosa: videocamere o altri strumenti "di controllo". Il vecchio primo comma vietava gli strumenti di controllo con funzione esclusiva di controllo a distanza dei lavoratori. Il secondo comma, ammetteva l'uso di videocamere e altri strumenti "di controllo" da cui potesse derivare anche la possibilità di controllo a distanza dei lavoratori, a certe condizioni. L'ipotesi che strumenti di lavoro potessero accidentalmente consentire il controllo a distanza dei lavoratori non era nemmeno prevista.

Negli anni, l'evoluzione tecnologica ha prodotto strumenti di lavoro capaci di registrare una tale quantità di dati relativi al comportamento dell'utente da mettere in crisi la distinzione concettuale tra strumento di lavoro e strumento di controllo sulla quale si fondava la disciplina dettata dall'art. 4, vecchio testo. Tra

questi strumenti, il computer è il principale, ma non il solo. I *tablet*, gli *smartphone* e così via, sono strumenti indirettamente capaci di fornire informazioni circa le modalità con cui gli stessi sono utilizzati. Ed essendo strumenti di lavoro sono in grado di fornire molte informazioni su come il lavoratore usa questi strumenti, quindi su come e quanto lavora, in alcuni casi anche su dove si trova fisicamente. Sono strumenti di lavoro ma che consentono il controllo a distanza (sicuramente in termini di controllo retrospettivo, in alcuni casi anche in termini di controllo a distanza fisica).

Questa caratteristica poneva l'interprete di fronte al problema di qualificare lo strumento ai fini dell'applicazione o meno della norma. L'interprete doveva cioè chiedersi se la funzionalità del controllo potesse trasformare – ai fini della norma – lo strumento di lavoro, in strumento di controllo. Questo perché non c'era alcuna deroga per gli strumenti utilizzati nello svolgimento della prestazione di lavoro, deroga presente nel nuovo secondo comma dell'art. 4.

Posta in questi termini la questione, è da ritenere condivisibile la scelta del legislatore di adottare la formula "strumento utilizzato" nella prestazione di lavoro e non "strumento di lavoro". Questa seconda formula non avrebbe fornito utili indicazioni poiché, come detto, è oggi piuttosto difficile trovare uno strumento di lavoro (cioè idealmente impiegabile nel lavoro) che non consenta anche il controllo del relativo utente. Non avrebbe quindi senso parlare oggi di strumenti di lavoro e strumenti di controllo come se si trattasse di categorie distinte. Meglio fare riferimento al caso concreto, quindi, piuttosto che alle caratteristiche astratte dell'apparecchio. Meglio verificare caso per caso se lo strumento (che consente di lavorare e, potenzialmente, di controllare) venga impiegato effettivamente nello svolgimento della prestazione. Solo in questo caso, il senso pratico impone di non imbrigliare l'azione dell'imprenditore in procedure preliminari alla messa in funzione dell'apparecchio: in questo caso, tra la funzionalità di lavoro e quella di controllo prevale quella di lavoro.

La formula "utilizzato" implica dunque un accertamento nel merito che evidenzi l'effettivo utilizzo dello strumento da parte del lavoratore al di là dell'astratta utilizzabilità dell'apparecchio per lavorare.

Questo dovrebbe consentire all'interprete di individuare con maggior precisione gli strumenti soggetti all'ambito di applicazione della norma e quelli esclusi. Vediamo in che termini riprendendo il caso in esame. Se il datore di lavoro deve fare un'indagine sulla posta elettronica dei lavoratori, idealmente ha due scelte: o accedere dai singoli computer, oppure tramite il server aziendale (con rare eccezioni, qualsiasi azienda gestisce la posta elettronica mediante un server che distribuisce la connessione a Internet ai computer aziendali). Ogni email

inviata e ricevuta dai dipendenti resta infatti salvata in copie di backup conservate nel server, anche se il lavoratore le cancella dal proprio browser installato nel singolo computer.

Il server è senz'altro uno strumento di lavoro (serve cioè all'imprenditore per l'attività di impresa ed è in effetti utilizzato dai suoi dipendenti dell'Information Technology aziendale per la loro prestazione di lavoro). Esso però non è uno strumento "utilizzato" dal lavoratore per rendere la prestazione nel senso voluto dalla norma (cioè non è utilizzato dal lavoratore soggetto al controllo). Meglio quindi procedere per mezzo del singolo computer aziendale assegnato al dipendete sotto scrutinio che, viceversa, è sicuramente uno strumento effettivamente utilizzato per lavorare.

Messi così in ordine i fatti, è dunque possibile ritenere operante, nel caso in esame, la deroga del secondo comma del nuovo art. 4.

Per potere accedere alle caselle di posta elettronica, mediante il personal computer aziendale a fini di investigazione interna è dunque sufficiente informare i lavoratori ai sensi dell'art. 13, D. lgs. 196/2003. L'informativa in questione potrà essere fornita sotto forma di policy aziendale sull'utilizzo degli strumenti informatici, a condizione che abbia tutti i requisiti stabiliti dal richiamato art. 13. Una policy completa in tal senso dovrà quindi prevedere – oltre ai limiti e alle modalità di utilizzo del personal computer e della posta elettronica – le finalità e modalità del trattamento connesso all'utilizzo di tali strumenti, la natura del conferimento dei dati, gli estremi del titolare e del responsabile del trattamento, l'ambito di comunicazione e diffusione, i diritti dell'interessato. Con riferimento alla posta elettronica, sarà anche opportuno inserire nella policy una sezione che renda nota al lavoratore la possibilità che il datore di lavoro o suoi incaricati possano accedere, in determinate circostanze (tra cui, ad esempio, le investigazioni interne e la prolungata assenza dal lavoro per malattia) alla posta elettronica aziendale, prevedendo, ove necessario, l'obbligo del lavoratore di fornire la password. Questa previsione consente di completare l'informativa di modo che sia utile non solo ai fini privacy ma anche per scongiurare il rischio di accessi alla posta elettronica passibili di sanzioni penali ai sensi dell'art. 616 c.p. (6).

(6) Art. 616 c.p.: «*Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da trenta euro a cinquecentosedici euro* (*omissis*)». La corrispondenza tutelata dalla norma penale è la corrispondenza qualificabile come "chiusa". Secondo Cass. 19 dicembre 2007, n. 47096, in *MGL*, 2008, 6, 520, con nota di E. Boghetich, non è qualificabile come chiusa la corrispondenza email se in una policy aziendale il datore di lavoro rende noto che l'accesso alla casella non è esclusivamente

Tirando le fila del discorso, se il Garante Privacy avesse deciso questo caso oggi:

- Non avrebbe potuto limitarsi a rilevare l'assenza dell'accordo sindacale e dell'autorizzazione della DPL, che possono ritenersi non necessari perché il controllo è avvenuto per mezzo di strumenti utilizzati dai lavoratori (soggetti al controllo) nello svolgimento della prestazione;
- Avrebbe dovuto valutare se l'informativa data ai dirigenti circa i controlli fosse stata esaustiva ai sensi del Codice Privacy. In caso di completezza delle informazioni fornite, nessuna violazione di legge sarebbe potuta essere rilevata.

Prima di abbandonare questo caso è opportuna una riflessione ulteriore sul concetto di strumento utilizzato nella prestazione. Nel caso in esame, le informazioni che abbiamo sullo strumento utilizzato sono poche: sappiamo che si tratta del computer aziendale assegnato al singolo dipendente. Non sappiamo nulla sui software installati sul computer in questione.

Sulla base delle informazioni disponibili possiamo quindi giungere alle conclusioni sopra riportate. Il caso potrebbe invece complicarsi se, all'esito di un'indagine approfondita sulle caratteristiche dello strumento utilizzato, emergesse che, tra i vari software installati sulla macchina in questione, ve ne fossero alcuni capaci di consentire il controllo a distanza del lavoratore, non utilizzati dallo stesso nello svolgimento della prestazione.

Al riguardo, il Ministero del Lavoro e delle Politiche Sociali, lo scorso 18 giugno, ha dato una prima interpretazione della norma, definendo gli strumenti di lavoro come i mezzi che "servono" al lavoratore per adempiere la prestazione, e specificando che l'eccezione del secondo comma del nuovo art. 4 Stat. Lav., non trova applicazione se gli strumenti in questione subiscono modifiche volte a controllare il lavoratore (es. aggiunta di software di localizzazione).

La distinzione non sembra cogliere nel segno perché non valorizza il senso pratico della deroga. Ipotizziamo che, nel computer utilizzato per svolgere le indagini difensive sulla posta elettronica dei dipendenti sia anche installato un software di controllo come, ad esempio, il SuperScout – software preso in considerazione nel primo caso esaminato. Non vi è alcun dubbio che si tratti di un software di controllo non utilizzato per rendere la prestazione. L'installazione di questo software determinerebbe la trasformazione del computer da strumento per cui vale la deroga del nuovo secondo comma a strumento soggetto alle formalità preliminari del primo comma? Non credo sia così. Il significato di

riservato al lavoratore. Nel caso di specie, è stata ritenuta sufficiente la previsione di una policy aziendale che imponeva la dipendente di fornire la password al superiore gerarchico in caso di assenza dal lavoro.

maggior senso (anche pratico) della deroga del secondo comma, è stabilire una prevalenza tra funzionalità di lavoro e funzionalità di controllo, per decidere in quale situazione prevale l'esigenza del controllo sulla tutela della riservatezza del dipendente.

In altre parole, la deroga non dovrebbe essere letta come una ulteriore, anacronistica distinzione concettuale tra strumento di lavoro e strumento di controllo. Come già detto, questa distinzione non ha più molto senso.

Il senso della deroga in esame è che, quando ci troviamo di fronte a una funzionalità mista (cioè strumento di lavoro che può consentire il controllo), se lo strumento viene effettivamente utilizzato per lavorare, quest'ultima funzionalità deve caratterizzare lo strumento in via prevalente e determinare l'operatività della deroga.

Questo tipo di interpretazione non trova, per la verità, un riscontro nella lettera della norma. Così sarebbe se il legislatore avesse utilizzato una terminologia identica nel primo comma (dove parla di strumenti che possono consentire il controllo) e nel secondo comma (dove parla di strumenti utilizzati per rendere la prestazione). Meglio sarebbe stato riferirsi, anche nel secondo comma, a strumenti "che possono consentire il controllo" ma che sono utilizzati per rendere la prestazione. In questo modo, il senso della deroga sarebbe stato evidente. In particolare sarebbe stato più chiaro il fatto che il perimetro della norma comprende gli stessi strumenti, cioè quelli che possono consentire il controllo (soggetti alle formalità del primo comma), con l'eccezione di quegli strumenti che, pur con questa potenzialità, sono in concreto utilizzati dal dipendente.

Proviamo a testare con l'esempio appena fatto questa interpretazione e quella fornita dal Ministero e vediamo a che conseguenze arriveremmo: il datore di lavoro deve fare un controllo sul computer che contiene la posta elettronica (cioè un software che fa funzionare la posta elettronica) e il SuperScout. Né l'installazione del computer, né quella del SuperScout (nel computer) è stata preceduta dalle formalità del primo comma del nuovo art. 4. Può il datore di lavoro comunque controllare la posta elettronica attraverso il personal computer per finalità difensive (idealmente comprese nel primo comma dell'art. 4 quindi soggette a previo accordo sindacale o autorizzazione amministrativa) avvalendosi della deroga del secondo comma? Secondo l'interpretazione proposta dal Ministero, l'installazione del SuperScout (un software di controllo) cambia la natura dello strumento, quindi la deroga del secondo comma non dovrebbe operare.

Questa interpretazione non sembra condivisibile. Il computer, nella sua interezza, rimane – con o senza l'installazione del SuperScout – uno strumento a

natura mista. Nel senso che viene usato per lavorare ma consente anche il controllo a distanza. Non ha quindi senso parlare di "software che cambiano la natura dello strumento". La natura dello strumento (il computer, il *tablet*, lo *smartphone* ecc.) non cambia affatto perché, come detto sopra, anche quei software che vengono utilizzati per lavorare possono comunque consentire il controllo a distanza. È piuttosto da chiedersi che cosa si intenda per "strumento", se il computer, oppure i singoli software che lo rendono operativo. Per capire meglio torniamo all'esempio fatto pocanzi: il SuperScout non verrebbe affatto utilizzato per il controllo della posta elettronica (ricordiamo che il SuperScout è un software di controllo degli accessi a Internet). Non vi è quindi ragione di negare l'utilizzo del computer (meglio, del software di gestione della posta elettronica installato nel computer) per controllare la corrispondenza email dei lavoratori. Il semplice fatto che nello stesso computer sia installato un altro software, il SuperScout, che certamente ha mera funzione di controllo, non cambia la natura del personal computer che, come detto, rimane una macchina con funzionalità mista lavoro-controllo.

Allo stesso modo un *tablet*, con varie funzionalità usate per lavorare (connessione a Internet, posta elettronica, pacchetto office ecc.), non smette di essere uno strumento usato per rendere la prestazione per il solo fatto che venga installato un software che consente di localizzarlo. Sarà, piuttosto, questo software a dover essere specificamente inteso come "strumento" che consente il controllo. E poiché questo specifico software non viene impiegato nell'utilizzo della prestazione (il lavoratore utilizza il *tablet* nelle altre sue funzionalità mentre non si può dire che il software di geolocalizzazione sia un software utilizzato per lavorare) solo l'installazione di questo software dovrebbe essere soggetta alle formalità del primo comma della norma, non il *tablet* in sé.

3. Cass., V sez. penale, 1 giugno 2010, n. 20722.

(a) Il caso risolto dalla sentenza

Una società aveva installato, senza previo esperimento delle procedure di cui all'art. 4, secondo comma, Stat. Lav. vecchio testo, delle videocamere al fine di accertare la condotta di una dipendente, con mansioni di cassiera, sulla quale si erano appuntati sospetti di appropriazione indebita di somme di denaro. Dalle registrazioni effettuate dalle videocamere così installate, i sospetti del datore di lavoro risultavano confermati.

All'esito del processo penale instaurato a carico della lavoratrice, il Tribunale di Treviso riteneva sussistente il reato di furto aggravato

successivamente derubricato dalla Corte d'Appello di Venezia in appropriazione indebita aggravata. I Giudici di merito fondavano la propria decisione sulle prove emerse dalle videoriprese effettuate dal datore di lavoro respingendo l'eccezione sollevata dalla difesa della lavoratrice di inutilizzabilità *ex* art. 191 c.p.p. (7) di tali prove in quanto acquisite in violazione dell'art. 4, secondo comma, Stat. Lav..

La Corte di Cassazione, confermando la decisione della Corte d'Appello, ha ritenuto utilizzabili le registrazioni effettuate mediante le telecamere installate senza previo accordo sindacale né autorizzazione della competente DPL, non rilevando, nel caso di specie la violazione degli artt. 4 e 38 Stat. Lav. In particolare, la Suprema Corte, richiamando il principio di cui alla sentenza n. 4746/2002, ha ritenuto che la finalità di controllo a difesa del patrimonio aziendale non è da ritenersi sacrificata dalle norme dello Statuto dei Lavoratori. La conclusione che la Corte ne trae e che «*gli artt. 4 e 38 dello Statuto dei Lavoratori implicano l'accordo sindacale a fini di riservatezza dei lavoratori nello svolgimento dell'attività lavorativa, ma non implicano il divieto dei cd controlli difensivi del patrimonio aziendale da azioni delittuose da chiunque provenienti. Pertanto in tal caso non si ravvisa inutilizzabilità ai sensi dell'art. 191 c.p.p. di prove di reato acquisite mediante riprese filmate, ancorché sia perciò imputato un lavoratore subordinato*».

(b) Possibile risoluzione del caso alla luce del nuovo testo

Questo è il caso che evidenzia le modifiche, potenzialmente, più rilevanti.

Come accennato con riferimento al primo caso esaminato, il nuovo primo comma dell'art. 4 Stat. Lav. ha aggiunto l'esigenza di "*tutela del patrimonio aziendale* ", tra quelle che possono giustificare l'installazione di strumenti idonei a effettuare un controllo sull'attività lavorativa, soltanto a fronte di accordo sindacale o autorizzazione della DTL.

Per effettuare un controllo finalizzato alla tutela del patrimonio aziendale, con l'ausilio di strumenti che non siano utilizzati nello svolgimento della prestazione, è dunque necessario un accordo sindacale o una autorizzazione amministrativa. Inoltre, è necessario informare i lavoratori.

Sulla base di un'interpretazione letterale, il nuovo art. 4 sembra imporre, per i controlli difensivi, quegli adempimenti che la giurisprudenza escludeva.

(7) Ai sensi dell'art. 191 c.p.p. "le prove acquisite in violazione di divieti stabiliti dalla legge non possono essere utilizzate. L'inutilizzabilità è rilevabile anche di ufficio in ogni stato e grado del procedimento".

Nonostante le critiche in dottrina (8) e alcune sentenze (per la verità poche) di segno contrario (cfr. Cass. 23/02/2010, n. 4375), l'orientamento che sosteneva che i controlli difensivi fossero estranei all'ambito di applicazione dell'art. 4 era decisamente maggioritario. E, tutto sommato, anche se non impeccabile da un punto di vista logico-giuridico, si trattava di un orientamento che aveva il pregio di soddisfare la necessità di punire fatti gravissimi, non prevedibili, che urterebbe la coscienza sociale lasciare privi di sanzione.

Sotto questo punto di vista, è difficile credere che la giurisprudenza non troverà dei correttivi rispetto alla formulazione del nuovo art. 4 che, se applicata alla lettera, condurrebbe a risultati difficilmente accettabili. Ad esempio, nel caso della sentenza in esame, si arriverebbe al paradosso per cui si dovrebbero avvertire i sindacati o l'ispettorato del lavoro e lo stesso dipendente sospettato di appropriazione indebita, del fatto che si ha intenzione di procedere all'installazione di videocamere per accertare che i sospetti siano fondati.

Proviamo allora a ipotizzare quali, tra gli argomenti utilizzati in passato dalla giurisprudenza, potrebbero essere ripresi per ricollocare i controlli difensivi (o almeno parte di essi) fuori dall'ambito di applicazione del primo comma, nuovo testo dell'art. 4.

È difficile che il principale argomento a sostengo della tesi dei controlli difensivi in vigenza del vecchio testo possa essere oggi utilizzato, ossia l'argomento per cui non è il lavoratore in sé soggetto al controllo ma il fatto illecito, da chiunque commesso (9). Il nuovo testo dell'art. 4, impone le procedure preliminari all'installazione per gli strumenti che consentono controlli finalizzati a tutelare il patrimonio aziendale senza specificazione alcuna in merito al soggetto che commetta atti illeciti in danno dell'azienda. Nel nuovo testo non se sembra esserci dunque spazio per questo argomento che, per la verità, non era convincente nemmeno in vigenza del vecchio testo. Come efficacemente puntualizzato da Mannacio (10), se si utilizza uno strumento di controllo per verificare se un illecito viene commesso durante l'attività lavorativa, ciò che viene

(8) Tra gli altri, cfr. G. Mannacio, *Uso di internet in azienda e tutela della privacy*, nota ad App. Milano n. 688/2005, in *DPL*, 10, 2006, 566.

(9) Cfr. Trib. Milano 5 luglio 2006, in *OGL*, 2006, 611; Trib. Perugia, 20 febbraio 2006, in *Dir. Inf.*, 2007, 1, 200, con nota di Gallus; Trib. Torino 9 gennaio 2004, *GP*, 2004, 131. In dottrina cfr. anche F. Rotondi, *Controllo a distanza dell'attività lavorativa*, *DPL*, 2006, 33, 1821, secondo cui «quando lo strumento di controllo non incide sui beni protetti dall'art. 4 Stat. lav., essendo finalizzato esclusivamente all'individuazione dell'autore dell'illecito di rilevante gravità, non si verte nella fattispecie prevista (e vietata) dall'art. 4 Stat. Lav».

(10) *DPL*, 10, 2006, 566, cit.

controllato è quello che il lavoratore fa nel tempo in cui è al lavoro: in altre parole, l'attività del lavoratore.

L'argomento utilizzato dalla precedente giurisprudenza che invece potrebbe essere ripreso, è quello secondo cui è necessario distinguere tra controlli *ex ante* e controlli *ex post*. Al riguardo, Cass. 23 febbraio 2012, n. 2722 (11) ha affermato che è estraneo all'ambito di applicazione dell'art. 4 il controllo effettuato *ex post* «ovvero dopo l'attuazione del comportamento addossato al dipendente, quando erano emersi elementi di fatto tali da raccomandare l'avvio di una indagine retrospettiva».

Anche alla luce del nuovo testo, si potrebbe sostenere che la finalità di tutela del patrimonio aziendale menzionata dal nuovo primo comma è da intendersi come necessità generica di protezione *ex ante* nei confronti di una generalità non identificata di atti illeciti e di soggetti che possano commetterli. Per capire meglio la distinzione riprendiamo ancora l'esempio del SuperScout. Questo strumento viene installato per tutelare la sicurezza informatica, quindi una parte del patrimonio aziendale. Questa esigenza, così come la possibilità di utilizzare questo strumento anche per controllare a distanza i lavoratori, è ben individuabile *ex ante* e non si riferisce a un caso specifico. In questo senso si dovrebbe intendere l'operatività del primo comma del nuovo testo nella parte in cui fa riferimento alle esigenze di tutela del patrimonio aziendale. Si tratterebbe, per così dire, di un controllo difensivo "in astratto". La stessa necessità di controllo difensivo "in astratto" è riscontrabile con riferimento ai sistemi di videosorveglianza del luogo di lavoro: videocamere installate per proteggere in generale il patrimonio aziendale da chiunque e in qualsiasi caso, non da un soggetto determinato in un caso specifico. Di diversa natura potrebbero essere considerati i controlli difensivi *ex post* o "in concreto", la cui necessità sia determinata da fatti contingenti e non prevedibili, che determinano esigenze di controllo puntali. Un esempio sarebbe proprio il caso della terza decisione in esame, in cui l'esigenza di installare una videocamera per monitorare il dipendente era insorta all'esito di sospetti ammanchi di cassa e si era esaurita con la conclusione dell'accertamento del fatto illecito. In definitiva è prevedibile una distinzione tra controlli difensivi in astratto, *ex ante*, inclusi nella norma (soggetti alle formalità preliminari all'installazione) e controlli difensivi in concreto, *ex post*, estranei all'ambito di applicazione del nuovo art. 4.

(11) In *RIDL*, 2013, II, 113, con nota di G. Spinelli.

Questo argomento si presterebbe alle critiche già mosse in vigenza del vecchio testo (12), con, ovviamente, l'aggiunta del rilievo per cui il dato letterale del nuovo primo comma, nel citare la finalità di tutela del patrimonio aziendale, sembra lasciare davvero pochi margini di manovra.

Si tratterebbe di critiche fondate rispetto alle quali, tuttavia, è più probabile che la giurisprudenza si riveli impermeabile, come già ha fatto in passato, trovando soluzioni interpretative capaci di evitare che la riforma dell'art. 4 si riveli più garantista degli obiettivi che si era prefissata.

Bibliografia.

Cairo L., *L'ambito di applicazione dell'art. 4 ... finalità difensiva e caratteristiche delle apparecchiature di controllo*, in *OGL*, 2010, 323

Mannacio G., *Uso di internet in azienda e tutela della privacy*, nota ad App. Milano n. 688/2005, in *DPL*, 10, 2006, 566

Ricci G.F., *Le prove illecite nel processo civile*, *RTDPC*, 1987, 34;

Rotondi F., *Controllo a distanza dell'attività lavorativa*, *DPL*, 2006, 33, 1821

(12) Sul punto si rinvia a L. Cairo, *L'ambito di applicazione dell'art. 4 ... finalità difensiva e caratteristiche delle apparecchiature di controllo*, in *OGL*, 2010, 323: «sebbene correttamente utilizzato ex post, quel determinato strumento che per le sue caratteristiche tecniche sia idoneo a consentire un controllo anche sull'attività del lavoratore, avrebbe potuto essere installato (e quindi utilizzato) solo a condizione dell'espletamento ex ante delle procedure di cui al secondo comma dell'art. 4. Rispetto a tale considerazione, non avrebbe, pertanto, alcun rilievo che successivamente alla (illegittima) installazione di un simile apparecchio se ne sia fatto un uso lecito in quanto si sarebbe utilizzato correttamente uno strumento che, in mancanza delle condizioni poste dal secondo comma dell'art. 4, non avrebbe nemmeno dovuto essere installato».