LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 1 / 2023

Roberto Romei

Il “ragionevole sospetto” in Cassazione

Il "ragionevole sospetto" in Cassazione

Roberto Romei

SOMMARIO: 1.La saga dei controlli difensivi. – 2. La distinzione tra controlli difensivi in senso lato ed in senso stretto.- 3. Il "ragionevole sospetto". 4. L'estensione temporale del controllo

1.L'occasione rappresentata dalla presentazione di un articolato studio curato da due colleghi e da una collega [1] fornisce anche l'occasione non per fare il punto, dal momento che un punto definitivo eccede le ambizioni e le capacità di chi scrive, ma per svolgere qualche breve considerazione sul tema dei limiti dei controlli a distanza del lavoratore, ed in particolare sui cd. controlli difensivi.

Come è ampiamente noto, la formulazione originaria dell'art. 4 della l.n. 300/1970 predisponeva una disciplina assai semplice, coerente del resto con una realtà tecnologica che, con gli occhi di adesso, può certamente definirsi come elementare.

La norma prevedeva un assoluto divieto di utilizzazione di impianti audiovisivi o di altre apparecchiature all'esclusivo fine di controllo dell'attività del lavoratore. Il secondo comma dell'art. 4 consentiva però la installazione di strumenti di controllo dell'attività lavorativa ricorrendo determinate esigenze ed a patto che le modalità della installazione e del funzionamento fossero regolate da un accordo preventivo con le rappresentanze sindacali (o vi fosse una autorizzazione amministrativa).

La norma visse di vita tranquilla fino a quando, alla metà degli anni '80 dello scorso secolo, non si verificò l'impatto con le nuove tecnologie che schiudevano, grazie all'utilizzo di determinati software, possibilità di controllo nemmeno immaginate nel 1970.

Ne è scaturita, nell'assenza (colpevole) del legislatore, un'opera (necessaria) di adattamento da parte della giurisprudenza del contenuto precettivo di una norma concepita per una certa realtà ad una realtà completamente diversa.

[1] Il riferimento è al volume curato da Carlo Pisani, Giampietro Proia ed Adriana Topo, *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, Giuffrè, 2022. Lo scritto riproduce l'intervento dell'autore al seminario di presentazione del volume tenutosi presso la Facoltà di Giurisprudenza di RomaTre e ne conserva lo stile discorsivo.

Un adattamento, per la stessa fonte di provenienza, per forza di cose incerto e non privo di contraddizioni, di fughe in avanti e di repentine retromarce. È su questo terreno che nasce la categoria, di origine giurisprudenziale, dei controlli difensivi, finalizzata a creare un'area di immunità, rispetto ai divieti scanditi dall'art. 4, di particolari tipologie di controllo dirette ad accertare condotte illecite dei lavoratori lesive del patrimonio aziendale [2].

La categoria del controllo difensivo, insomma, si situava su un'area lasciata scoperta dal legislatore del 1970, quella dei controlli destinati alla tutela del patrimonio aziendale. Si ritenne infatti che l'area coperta dall'art. 4 fosse solo quella che avesse ad oggetto, direttamente o indirettamente, l'attività lavorativa; mentre i controlli difensivi dovevano considerarsi estranei a quest'ambito, essendo invece finalizzati ad accertare condotte illecite, e che dunque, in quanto tali, dovevano considerarsi estranee all'attività lavorativa [3].

Nonostante fosse destinata ad operare un compromesso con le istanze provenienti da una realtà organizzativa in forte mutamento ed a dare udienza ad interessi meritevoli di tutela, la categoria dei controlli difensivi è stata oggetto di forti critiche da parte della dottrina che non ha mancato di evidenziare la intrinseca contraddittorietà di una categoria di controlli che proprio perché diretta a verificare la commissione di condotte illecite finiva con l'estendersi anche a condotte lecite, accogliendo una distinzione - tra controllo della condotta (illecita) extracontrattuale, e controllo della condotta (lecita) - che non solo non era presente nella lettera dell'art. 4, ma era di difficile se non impossibile distinzione pratica [4].

Ora il primo comma dell'art. 4 ammette il controllo a distanza non più solo per esigenze organizzative, produttive o di sicurezza, ma anche per la tutela del patrimonio

[2] Si veda Cass. 3 aprile 2002, n. 4746, secondo la quale "ai fini dell'operatività del divieto di utilizzo di apparecchiature per il controllo a distanza dell'attività dei lavoratori previsto dall'art. 4 legge n. 300 del 1970, è necessario che il controllo riguardi (direttamente o indirettamente) l'attività lavorativa, mentre devono ritenersi certamente fuori dell'ambito di applicazione della norma sopra citata i controlli diretti ad accertare condotte illecite del lavoratore (cosiddetti controlli difensivi), quali, ad esempio, i sistemi di controllo dell'accesso ad aule riservate o, come nella specie, gli apparecchi di rilevazione di telefonate ingiustificate". Nei medesimi termini Cass. civ, sez. lav. 4 aprile 2012, n. 5371 e Cass.3 luglio 2001 n. 8998 che ritengono legittimo il controllo con registrazioni effettuate da un soggetto estraneo al di fuori dei locali aziendali; Cass.1° giugno 2010, n. 20722, che circoscrive il controllo difensivo come quello volto a proteggere il patrimonio aziendale dalle azioni delittuose e, in quanto tale, estraneo all'ambito di applicazione dell'art. 4 St. lav.; In qualche occasione si è ancorata la legittimità del controllo alla condizione che esso fosse disposto in un momento successivo al verificarsi del comportamento illecito.

[3] Osserva correttamente V. Maio, *I controlli difensivi e la tutela del patrimonio aziendale*, in C.Pisani, G. Proia, A.Topo, *Privacy e lavoro*, cit., 416, che l'emersione della categoria del controlli difensivi è stata preceduta, ed in qualche maniera agevolata, dal riconoscimento della estraneità al campo di applicazione dell'art. 3 della l. n. 300/1970 dei controlli posti in essere dal datore di lavoro o da agenzie investigative per fini di tutela del patrimonio aziendale o quando rappresentassero l'unica forma di controllo sull'attività dei lavoratori.

[4] P.Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *Riv.it.dir.lav.*, 2009, I, 323

aziendale, espressione questa molto ampia, ed anzi, tanto ampia da essere interpretata come comprensiva anche del controllo sulle attività illecite del lavoratore assorbendo così al proprio interno anche i controlli difensivi .

Le novità introdotte nel 2015 dunque non hanno esattamente contribuito a chiarire il quadro all'interno del quale inserire i controlli difensivi, alimentando anzi le divisioni dottrinarie e giurisprudenziali [5], che risultano più polarizzate che in passato: "da un lato, c'è chi ritiene che i controlli difensivi siano stati ormai pienamente assorbiti nella nuova regolamentazione legale, con la conseguenza che gli stessi sono consentiti solo tramite impianti debitamente autorizzati, quando necessario, e comunque nel rispetto degli obblighi informativi. Dall'altro chi, invece, propone un aggiornamento del concetto di controllo a distanza al fine di sostenerne la sopravvivenza, in deroga all'art. 4 dello Statuto, in una prospettiva di ineliminabile bilanciamento dei contrapposti interessi" [6].

Si è così ritenuto che la formulazione letterale del primo comma non lasciasse dubbio alcuno in ordine alla inammissibilità dei controlli difensivi data l'esplicita inclusione della tutela del patrimonio aziendale tra le esigenze che consentono la installazione di sistemi di controllo, a dimostrazione di come il legislatore avrebbe ricondotto anche i controlli difensivi nel campo di applicazione dell'art. 4. Con il che anche i controlli diretti a reprimere o ad accertare l'autore della commissione di illeciti dovrebbero soggiacere alle condizioni di utilizzo stabilite dal primo comma dell'art. 4. Tanto equivarrebbe però a rendere nei fatti impossibile o inutile la installazione di apparecchiature dirette ad accertare la commissione di illeciti, la cui efficacia richiede segretezza e rapidità di utilizzo. Condizioni che certo non sarebbero soddisfatte ove si dovese ricorrere la stipulazione di un accordo sindacale [7].

[5] C. Colapietro, A.Giubilei, *Controlli difensivi e tutela dei dati del lavoratore: il nuovo punto della Cassazione*, in *Labour law issues*, 2021, 187 ss.; senza pretese di esaustività: P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali dei lavoratori*, Giappichelli, 2017; più di recente, Ead., *I controlli aziendali per finalità difensive nella giurisprudenza*, in *Riv.it.dir.lav.*,2022, I, 221; C. Colosimo, *La moderna declinazione del potere di* controllo, in P.Curzio, L. Di Paola, R.Romei (a cura di), *Diritti e doveri nel rapporto di lavoro*, Giuffrè, vol. II, 2018,75 ss.; A. Sitzia, *Personal computer e controlli ''tecnologici'' del datore di lavoro nella giurisprudenza*, in *Arg.dir.lav.*, 2017, 804; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori*, in *Riv.it.dir.lav.*, 2016, I, 513; R. Del Punta, *La nuova disciplina del controllo a distanza sul lavoro (art. 23 D.Lgs. n. 151/2015)*, *ivi*, 2016, I, 77 ss.; A. Ingrao, *Il controllo a distanza sui lavoratori e la nuova disciplina privacy: una lettura integrata*, Cacucci, 2018.; da ultimo A. Bellavista, *Controlli tecnologici e* privacy *del lavoratore*, in A. Bellaviasta, R.Santucci (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*,Giappichelli, 2022, p. 99, ss.

[6] M. Marazza, *I controlli a distanza del lavoratore di natura "difensiva"*, in P. Tullini (a cura di), *Controlli a distanza* cit.

[7] Resterebbe poi da chiedersi la ragione di un trattamento di così accentuato favore nei confronti di chi commetta degli illeciti magari anche aventi una rilevanza penale solo perché commessi in occasione dello svolgimento di una prestazione di lavoro, rispetto alla restante parte degli altri cittadini o anche rispetto alle stesse persone una volta dismessi i panni del lavoratore subordinato

Fatto si è comunque, che la giurisprudenza, sia pur tra non poche oscillazioni [8], sembrerebbe non avere abbandonato le posizioni che aveva elaborato prima del 2015, riconoscendo ai controlli difensivi un residuo diritto di cittadinanza all'interno del nostro ordinamento.

2. Una recente ed importante sentenza della Corte di Cassazione, la n. 25732 del 22 settembre 2021, si sforza di fare il punto su questa delicata materia.

La vicenda all'origine della sentenza è piuttosto complicata, ma merita che ad essa si faccia cenno, sia pur brevemente.

Una lavoratrice era stata licenziata a seguito di una serie di accertamenti effettuati dalla Fondazione per cui lavorava sul suo computer. Gli accertamenti traevano origine dalla diffusione di un virus nella rete della Fondazione, poi risultato introdotto da un file rinvenuto nel computer utilizzato dalla lavoratrice ed evidentemente da quest'ultima utilizzato o scaricato. I controlli avevano accertato che la lavoratrice aveva effettuato diversi accessi a siti che nulla avevano a che vedere con lo svolgimento dell'attività lavorativa, e che tali accessi si erano protratti lungo un arco temporale significativo, "tale da integrare una sostanziale interruzione della prestazione lavorativa".

Appare evidente che la consapevolezza da parte della Fondazione dell' adempimento da parte della lavoratrice è stata raggiunta solo a seguito della effettuazione dell'accesso al computer aziendale sul quale svolgeva la sua prestazione di lavoro.

Dal canto suo, la lavoratrice si era rivolta all'Autorità Garante per la protezione dei dati personali che aveva ordinato alla Fondazione di astenersi dall'effettuare qualsiasi ulteriore trattamento dei dati acquisiti dalla cronologia dei browser utilizzati, eccettuata la mera conservazione degli stessi ai fini della loro eventuale acquisizione in sede giudiziaria.

Il Tribunale, in sede di opposizione aveva ritenuto che la pronuncia del Garante non fosse di ostacolo alla utilizzazione dei dati estratti dal computer aziendale e che comunque l'accesso operato dalla Fondazione non potesse considerarsi alla stregua di un controllo a distanza, espressione questa che, come è noto, abbraccia sia la distanza in senso spaziale che in senso temporale. Secondo il Tribunale, insomma, il controllo non aveva ad oggetto

[8] Una rapida rassegna si trova in V. Maio, *I controlli difensivi,* cit.,433 ss. L. Cairo, *Controlli a distanza: passato e presente di un tema ancora controverso, in Lav.giur.,* 2018, 2.

l'attività della lavoratrice, bensì era strumentale alla bonifica del sistema informatico interno. Nondimeno, il Tribunale aveva disposta la reintegrazione della lavoratrice.

La Corte di appello, pur confermando la sentenza di primo grado, quanto alla finalità del controllo aveva ritenuto al contrario che la sanzione espulsiva fosse proporzionata alla gravità del comportamento della lavoratrice, dal momento che gli accessi a siti privati evidenziavano una discontinuità della prestazione di lavoro ritenuta tale da giustificare il licenziamento.

La lavoratrice ha poi fatto ricorso per cassazione lamentando che le informazioni sullo svolgimento della sua prestazione di lavoro erano state raccolte in maniera illegittima, non avendo provveduto la Fondazione ad informare preventivamente la lavoratrice sulle modalità di effettuazione dei controlli, ciò che renderebbe i dati raccolti, inutilizzabili.

La Corte nel decidere il caso adotta ed introduce la distinzione tra controlli difensivi in senso lato e controlli difensivi in senso stretto. I primi sarebbero posti a tutela del patrimonio aziendale e "riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto di tale patrimonio". I secondi invece sono quelli "diretti ad accertare specificamente condotte illecite ascrivibili – in base a concreti indizi – a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro"

Mentre i primi rientrerebbero senza dubbio nella nozione di controllo disciplinata dal primo comma dell'art. 4, i secondi invece ne sarebbero estranei, dal momento che non avrebbero ad oggetto il normale svolgimento dell'attività di lavoro, ma anzi, troverebbero la loro ragion d'essere in eventi di natura straordinaria o eccezionale, in quanto correlati alla necessità di accertare degli illeciti.

Se è abbastanza chiaro, almeno in linea di principio, quale sia l'area occupata dal controllo difensivo in senso stretto; rimane per contro un po' nell'ombra lo spazio in cui si situa il controllo difensivo in senso lato. Ed in particolare se esso coincida con il controllo di cui al primo comma dell'art. 4, ovvero, se rappresenti un cerchio concentrico a quest'ultimo.

Come sia, la Corte comunque si premura di introdurre una serie di *caveat* al controllo difensivo in senso stretto.

Innanzitutto, precisazione peraltro ovvia, il controllo difensivo non può tradursi in un annullamento dei margini di riservatezza del lavoratore.

Meno ovvia è invece una seconda precisazione, secondo la quale il potere di controllo deve essere bilanciato con il diritto alla riservatezza dei lavoratori: da ciò la Corte trae la conseguenza che il controllo deve rispettare i principi di proporzionalità e di minimizzazione [9].

Secondo la sentenza, inoltre, il controllo difensivo deve essere deve un controllo a posteriori, dovendo fondarsi su un ragionevole sospetto della commissione di un illecito da parte del lavoratore: solo da questo momento, e cioè solo dall'insorgenza di un sospetto, il datore di lavoro potrà provvedere alla raccolta delle informazioni. L'insorgenza di un fondato sospetto individua non solo il momento in cui il controllo può essere attuato, bensì anche circoscrive l'ambito della raccolta delle informazioni, che può avvenire solo da quel momento in avanti e non può riguardare informazioni afferenti a momenti precedenti. Ciò per evitare, sostiene la Corte, che l' area del controllo difensivo si estenda fino ad abbracciare a ritroso tutto l'arco, o gran parte dell'arco, durante il quale si snoda il rapporto di lavoro.

3. La sentenza si pone in una linea di una certa continuità con la giurisprudenza che la aveva preceduta e che si era pronunciata, in più di una occasione, nel senso della legittimità dei controlli difensivi a condizione che essi fossero stati predisposti, anche in maniera occulta, al fine di impedire la commissione di illeciti, anche se il quadro indiziario è formato da elementi tratti non dallo svolgimento del rapporto di lavoro [10]. E sembra voler portare a sistema, in parte arginandoli, una serie di spunti già presenti nella giurisprudenza ad essa precedente.

Non chiude però ogni interrogativo.

La Cassazione ritiene in primo luogo necessario, ai fini della legittimità del controllo difensivo, che esso sia originato da "un ragionevole sospetto dell'esistenza di condotte vietate".

Formulazione questa assai ambigua e che solleva più di una domanda circa la sua esatta portata

[9] Nell'occasione la Corte si riallaccia alla sentenza della Corte EDU del 5 settembre 2017, sul caso *Bārbulescu c. Romania,* si cui G Consonni, *Il caso Bārbulescu c. Romania e il potere di controllo a distanza dopo il Jobs Act: normativa europea e italiana a confronto,* in *Dir.rel.ind.*, 2016, 1771 ss.

[10] T.Roma, 24 marzo 2017 in *Dir.rel.ind.*,2018, 264; App. Roma, 14 ottobre 2019, in *Lav.prev.oggi*, 2020, 172; T. Padova, 24 dicembre 2018 in *Nuova giur,civ.*, 2919, 649; T Torino, 19 settembre 2018, (inedita, ma citata da Maio, *I controlli difensivi*, cit. 434, nota n. 66);T. Padova, 22 gennaio 2018, in *Riv.giur.lav.*, 2018, II, 593.

Innanzitutto, potrebbe chiedersi cosa debba o possa intendersi per "ragionevole sospetto" [11]. La Corte non ritiene opportuno diffondersi su cosa si intenda per "ragionevole sospetto", perdendo così una buona occasione per diminuire il già notevole tasso di incertezza che connota la materia dei controlli difensivi. A onor del vero, non era semplice individuare la soglia di ragionevolezza del sospetto, né se esso debba poggiare solo sul convincimento del datore di lavoro, ovvero, se siano richiesti degli indizi materiali e riconoscibili. Ma l'accertamento della sussistenza di un ragionevole sospetto, come appare evidente, non è un dato secondario ai fini della legittimità dei controlli. Quando ed a quali condizioni infatti può dirsi che vi sia un ragionevole sospetto? Appare evidente che almeno un sospetto vi debba essere. Il che conduce a ritenere che delle apparecchiature di controllo occulte, ad esempio, una telecamera nascosta che riprenda una cassaforte o un deposito ove le persone incaricate ripongono o custodiscono determinati oggetti di valore, non sarebbe legittimo, in assenza di una qualsiasi ragione che giustifichi la installazione. In un caso siffatto, non essendosi verificato alcun ammanco o furto, verrebbe meno la ragione stessa del controllo occulto, posto che la medesima finalità di tutela e protezione del patrimonio aziendale potrebbe essere raggiunta attraverso una semplice telecamera installata ai sensi del primo comma dell'art. 4. Il fatto stesso che vi sia un sistema di ripresa e che questo sia conosciuto da tutti vale a preservare dalla commissione di illeciti, dato che questi sarebbero registrati. All'opposto, potrebbe però dubitarsi della stessa esistenza di una forma di controllo sull'attività dei lavoratori, posto che il controllo verrebbe a cadere su una frazione minima della attività lavorativa, da non potersi ritenere tale da annullare ogni margine di riservatezza del lavoratore, per dirla con le parole della Cassazione. Ed anzi, potrebbe dubitarsi che margini di invasione nella sfera di riservatezza possano venire in considerazione, data la pochezza della frazione di attività oggetto del controllo [12].

Comunque, per la Cassazione è necessario un ragionevole sospetto, quale che sia il significato dell'espressione.

Il che vale ad introdurre una domanda ulteriore, in ordine al momento in cui il controllo può cadere, se cioè esso debba esser successivo o possa essere anche preventivo.

[11] Il principio di ragionevolezza sembra riscuotere da ultimo un certo successo nella giurisprudenza: del criterio infatti fa uso anche la Corte di Giustizia nella sentenza del 17 marzo 2022, C-232/20, *Daimler*, ed anche Cass., 21 luglio 2022 n. 22861 e Cass. 27 luglio 2022 n.23494,quest'ultima di prossima pubblicazione su *Riv.it.dir.lav,* con nota di G. Casiello, *La somministrazione di lavoro ovvero della temporaneità ragionevole*

[12] Si veda Cass. pen, sez.III, 14 dicembre 2020 n. 3255 che parla di un "significativo controllo sull'ordinario svolgimento dell'attività lavorativa".

La Cassazione sembra essere decisamente orientata nel secondo senso; ciò che implica che una lesione del patrimonio vi deve essere stata: diversamente, un sospetto, come si è detto, mancherebbe del tutto.

Del resto, come si osservato, se si vuole evitare ogni possibile lesione al patrimonio aziendale, potrebbe utilizzarsi la via del primo comma dell'art.4.

Anche la CEDU, nel noto caso *Lopez-Ribalda c. Spagna* [13] fa uso di un concetto similare, parlando di fondati sospetti: in quell'occasione, come è noto, il datore di lavoro (gestore di un supermercato), avendo registrato una serie di discrepanze tra i livelli delle scorte di magazzino e gli introiti giornalieri, aveva installato delle telecamere ben visibili rivolte vero le entrate e le uscite; e delle altre telecamere, la cui esistenza era stata celata al personale, rivolte verso il personale addetto alle casse. Queste ultime avevano appunto registrato gli illeciti commessi da cinque lavoratrici addette alla casse, talvolta anche con la complicità dei clienti. In tale ipotesi, quand'è che si potrebbe dire che si sia raggiunto il ragionevole sospetto che alcuni dipendenti stiano commettendo dei furti in danno al supermercato?

In un simile frangente, il rimedio cui prima si è accennato non potrebbe essere utilizzato.

Un conto infatti è installare una telecamera che riprenda, per pochi istanti, chi entra e chi esce da un magazzino, altro conto è riprendere le persone addette alla cassa di un supermercato in via continuativa, a prescindere dal verificarsi di un illecito.

In tale ipotesi, potrebbe, dirsi con la Cassazione, che il controllo annullerebbe ogni forma di riservatezza dei lavoratori, anche se è vero che questi ultimi, proprio perché addetti alle casse di un supermercato sono quasi naturalmente esposti ad una forma di compressione fin quasi all'annullamento dei margini di riservatezza.

La realtà è che il criterio del fondato sospetto – o del ragionevole sospetto, che dir si voglia – presuppone un bilanciamento tra i contrapposti interessi che dà per scontato che il datore di lavoro possa e debba sopportare un danno patrimoniale prima che i sospetti raggiungano un livello tale da dirsi fondati o ragionevoli. Ed infatti, nel caso deciso dalla CEDU, il gestore del supermercato ha dovuto accettare che per un certo periodo di tempo gli ammanchi restassero impuniti.

[13] Espressione analoga si rinviene nella sentenza della Corte EDU 17 ottobre 2019 *Lopez-Ribalda e al.c. Spagna,* cui si rinvia per un commento a S. Ciriello, F.Ariante, *Videosorveglianza "occulta" sul luogo di lavoro: il caso López Ribalda e altri c.Spagna e la giurisprudenza della Corte Europea dei Diritti dell'Uomo,* in *Lav.dir.Europa,* n.3, 2019.

Oppure, nel caso deciso proprio dalla Cassazione, ove l'accesso a siti privati venga compiuto durante l'orario di lavoro e ciò abbia comportato l'introduzione di virus che abbiano bloccato il funzionamento del sistema per un certo periodo di tempo, o peggio, abbiano prodotto danni di una certa entità, il criterio del ragionevole sospetto potrebbe produrre conseguenze anche peggiori, dal momento, appunto, che i danni potrebbero essere anche di entità grave.

Onde evitare conseguenze di questo genere, il datore di lavoro potrebbe in via preventiva proibire l'uso dei computer aziendali per fini privati, informando i dipendenti del divieto di accesso a siti di qualsiasi genere per finalità non connesse allo svolgimento della prestazione di lavoro. Si tratta di una facoltà senza dubbio legittima, ma il datore di lavoro potrebbe anche controllare che i propri dipendenti rispettino il divieto? In tal caso si potrebbe ritenere che il controllo cada su un'area estranea al controllo difensivo, posto che il controllo non sarebbe finalizzato ad accertare degli illeciti, ma semplicemente a verificare il rispetto di una modalità di utilizzo dei computer aziendali la cui finalità è evitare che nel sistema vengano immessi dei virus.

È questa una ipotesi diversa da quella oggetto di una sentenza del Tribunale di Roma, citata anche dalla sentenza della Cassazione, secondo il quale " È legittimo il controllo c.d. difensivo del datore di lavoro sulle strutture informatiche aziendali in uso al lavoratore, a condizione che esso sia occasionato dalla necessità indifferibile di accertare lo stato dei fatti a fronte del sospetto di un comportamento illecito e che detto controllo prescinda dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa essendo, invece, diretto ad accertare la perpetrazione di eventuali comportamenti illeciti" [14]. Anche in questo caso, infatti, il controllo cade *ex post*, dopo cioè che il presunto illecito è stato commesso.

Dunque, sviluppando il pensiero della Cassazione, il controllo difensivo predisposto senza che vi sia un ragionevole sospetto, o detto in altri termini, prima che si sia prodotta una lesione del patrimonio aziendale, non sarebbe da considerarsi legittimo. Il bilanciamento, dunque, implica la produzione di un danno al patrimonio aziendale, condizione questa necessaria affinché si possa dar corso ad un controllo difensivo.

In una fase antecedente, ciò che solo si può fare è attivare una procedura di controllo alle condizioni richieste dall'art. 4. Sarebbe dunque necessario che sussistessero le finalità

[14] T Roma, 24 marzo 2017, in *Dir.rel.ind.*, 2018, II, 265.,

indicate dal primo comma dell'art. 4 e fosse raggiunto un accordo sindacale, in assenza del quale, dei controlli difensivi preventivi, non sarebbero possibili.

Nel caso deciso dalla Cassazione è difficile pronosticare se le organizzazioni sindacali avrebbero prestato il loro consenso alla effettuazione di controlli casuali sui computer aziendali al fine di accertare il rispetto del divieto di connettersi a siti esterni.

Del resto, ci si potrebbe domandare se davvero un accordo sindacale sia necessario: nell'esempio fatto, il controllo avrebbe un oggetto diverso, e cioè non le modalità di effettuazione della prestazione di lavoro, ma solo l'eventuale accesso a siti esterni. E comunque, potrebbe sempre ritenersi che il computer sia uno strumento utilizzato per la esecuzione della prestazione di lavoro, il che renderebbe non necessario l'accordo.

Non vi sarebbe dunque alcun controllo sulla prestazione di lavoro, ma solo su un dato certamente esterno ad essa. Né vi sarebbe violazione della riservatezza del lavoratore - sotto forma della salvaguardia del principio alla autodeterminazione informatica [15] - posto che i lavoratori, per espressa previsione aziendale, non dovrebbero collegarsi con siti esterni, e dunque non vi sarebbe la possibilità di violare la riservatezza dei dipendenti accertando ad esempio quali siti essi abbiano visitato.

E se si ammettesse il controllo difensivo diretto alla repressione di un illecito, ci si potrebbe domandare se, a certe condizioni, potesse essere ritenuto legittimo anche il controllo difensivo preventivo.

La Cassazione nella sentenza in commento non si occupa direttamente di questo profilo.

Vale però la pena di rammentare come in due sentenze di non molto tempo addietro [16] la Cassazione si fosse espressa in senso molto restrittivo. Chiamata a pronunciarsi sulla legittimità di un software utilizzato dal Poligrafico dello Stato per monitorare gli accessi esterni dei propri dipendenti - meccanismo tra le altre cose necessario al fine di assicurare intuibili ragioni di integrità e di sicurezza dei sistemi informatici interni - la Cassazione ritenne che anche i controlli difensivi rientrassero nel novero dei controlli cui trovava applicazione l'art. 4. Nella seconda sentenza la Cassazione ha ritenuto illegittimo il licenziamento di un vigilante che era accusato di non avere svolto completamente le

[15] Di cui parlano Colapietro-Giubilei, *Controlli difensivi*, cit, p. 193 sulla base di una risalente giurisprudenza del *Bundesverfassungsgericht*.

[16] Cass. 18 settembre 2016, n. 183202 in *Riv.it.dir.lav.*,2017,II, con note di C. Criscuolo, *Controlli difensivi e codice della privacy* e di A. Ingrao, *Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act*

ispezioni programmate nel turno di lavoro come comprovato dalle risultanze del sistema GPS che attestava come la sua vettura si trovasse in altri luoghi.

Al di là delle peculiarità dei due casi, è importante ciò che si legge soprattutto nella seconda sentenza allorché si precisa come i dati tratti dal sistema GPS non potessero essere utilizzati a fini disciplinari dal momento che il sistema era stato installato *ex ante* e ben prima che insorgessero dei sospetti su una eventuale violazione del lavoratore e che esso consentiva il controllo sulla attività lavorativa e non sui beni estranei al rapporto di lavoro.

Senza voler entrare nel merito delle due decisioni, è però indubbio che la Corte di Cassazione nelle due sentenze appena citate prenda chiaramente posizione contro la possibilità di effettuare dei controlli difensivi prima ed indipendentemente dalla commissione di un illecito.

5. L'altro interrogativo sollevato dalla sentenza riguarda l'estensione del controllo.

Secondo la Cassazione il controllo difensivo non può "…riferirsi all'esame ed all'analisi di informazioni acquisite in violazione delle prescrizioni di cui all'art. 4 St.lav.", precisando che "Può, quindi, in buona sostanza, parlarsi di controllo ex post solo ove, a seguito del fondato sospetto del datore circa la commissione di illeciti ad opera del lavoratore, il datore stesso provveda, da quel momento, alla raccolta delle informazioni".

Dunque, non solo è necessario un fondato sospetto, ma le informazioni possono essere raccolte solo da quel momento, e, soprattutto, non possono riferirsi alla attività scolta in precedenza.

La precisazione, di grande importanza, si attaglia perfettamente al caso deciso dalla sentenza *Lopez-Ribalda*, in cui venivano in considerazione delle azioni, il furto di materiale di proprietà del supermercato, che per loro stessa natura non lasciavano traccia alcuna, e dunque una volta commesse non erano tracciabili: il controllo insomma non poteva che avere effetti da un certo momento in avanti. Ma ciò dipendeva, come si è detto, dal tipo di azione che si doveva accertare.

La Cassazione enuncia invece una regola, vestendo un dato fattuale e contingente dei panni della giuridicità.

L'operazione però non è indolore né priva di conseguenze..

In verità, una volta che sia insorto un sospetto in ordine alla commissione di un illecito, il che legittima il controllo difensivo, non è chiara la ragione per la quale non dovrebbe essere consentita una indagine che abbracci anche ciò che è avvenuto in un momento precedente, posto che di illecito si tratta e che la repressione dello stesso va ritenuta ammissibile. Nell'esempio portato sopra – dell'accesso a siti esterni che determinano l'importazione di virus informatici all'interno del sistema aziendale – la limitazione temporale introdotta dalla Cassazione rischia di rendere del tutto inutile il controllo. Dal momento in cui il virus è penetrato nel sistema, infatti, la sua presenza è nota e ciò indurrà l'autore del fatto ad astenersi in futuro dall'accedere a siti esterni. Ma la impossibilità di accertare se vi erano stati degli accessi all'esterno e chi sia stato il loro autore sarebbe completamente preclusa dalla illegittimità di operazioni che consentano di risalire a quanto era stato fatto pima dell'importazione del virus.

A prescindere dalle conseguenze pratiche, la sentenza sul punto non elimina ogni dubbio, non essendo del tutto chiaro se e perché il requisito sostanziale abbia o debba avere anche una dimensione temporale.

Perché questo sembrerebbe il pensiero della Corte, sempre che esso sia stato rettamente inteso.

Ma un conto è il momento dal quale il controllo difensivo può attivarsi; altro conto è la sua estensione nel tempo.

La limitazione alle sole informazioni raccolte dopo che vi sia un fondato sospetto di illecito, si giustifica perché, diversamente, si rischierebbe di legittimare l'uso di strumenti di controllo senza autorizzazione alcuna e in possibile violazione del diritto alla riservatezza, consentendo, sono parole della sentenza, al datore di "acquisire per lungo tempo ed ininterrottamente ogni tipologia di dato, provvedendo alla relativa conservazione, e, poi, invocare la natura mirata (ex post) del controllo incentrato sull'esame ed analisi di quei dati".

Ora, l'acquisizione per lungo tempo ed ininterrottamente di ogni tipo di dato sembra non avere nulla a che vedere con la regola della limitazione temporale all' acquisizione di dati che la Corte circoscrive solo a quelli attingibili dopo che sussiste un ragionevole sospetto in ordine alla commissione dell'illecito. Detto in altre parole, il ragionevole sospetto legittima il controllo difensivo ed anche occulto, ne costituisce la ragione sostanziale, ma non anche la ragione della limitazione temporale. Il pericolo di una

acquisizione lunga ed ininterrotta di dati è eliminato dalla esistenza di un ragionevole sospetto. Ma una volta che tale condizione sia soddisfatta il controllo dovrebbe poter avvenire senza alcuna limitazione temporale, proprio perché legittimato dall'esistenza di un sospetto. L'estensione del controllo anche a momenti anteriori alla insorgenza di un ragionevole sospetto non è logicamente desumibile dalla necessità che vi sia un ragionevole sospetto, dal momento che l'insorgenza di quest'ultimo vale ad escludere che le informazioni possano dirsi "acquisite in violazione delle prescrizioni di cui all'art. 4 St.lav.".

Dunque, quest'ultimo passaggio della sentenza non è chiarissimo.

La giusta esigenza di evitare forme incondizionate di controllo ha indotta la Cassazione a muoversi con grande, e forse troppa, prudenza; mentre un passo in più, nel senso di non limitare temporalmente l'estensione del controllo[17], avrebbe potuto essere compiuto, e si spera che lo sarà, perché non determina le conseguenze paventata dalla sentenza. Ma soprattutto perché, diversamente, si rischia di legittimare, o quanto meno coprire con il velo della impunità, condotte censurabili non solo dal puto di vista della logica interna dei rapporti tra le parti contrattuali, ma prima ancora dal punto di vista etico.

.

[17] Cui si accompagni una chiara ed accurata delimitazione dell'utilizzazione che è consentita degli strumenti di lavoro corredata da una altrettanto chiara informazione sul tipo di controllo che può essere predisposto, onde evitare ciò che è accaduto nel caso deciso da T.Torino, 19 settembre 2018, citata sopra alla nota n.10 che ha ritenuto illegittimo il licenziamento di un lavoratore che aveva trascorso oltre 300 ore su siti di natura finanziaria non avendo il datore di lavoro fornito un'adeguata informativa, in particolare con riferimento alle modalità di effettuazione dei controlli datoriali.

.