Condizioni e limiti del controllo datoriale nel rapporto di lavoro

di
Mario Meucci (*)

1. Premessa

Il contratto di lavoro subordinato si caratterizza - a differenza di quello di lavoro autonomo - per la posizione di supremazia del datore di lavoro e per la corrispondente posizione di soggezione del lavoratore, che rendono il rapporto in questione non paritetico ma del tutto sbilanciato a favore del datore di lavoro che risulta, pertanto, detentore di un potere connotato da elevata discrezionalità che la legislazione del lavoro ha, nel corso del tempo, variamente circoscritto onde prevenire sconfinamenti nell'arbitrio.

La posizione di supremazia datoriale è giuridicamente sancita dal nostro codice civile negli artt. 2086, 2094 e 2014 ove, nel primo, viene attestato il principio di gerarchia ("*L'imprenditore è il capo dell'impresa e da lui dipendono gerarchicamente i suoi collaboratori*"), riprecisato a conferma nell'art. 2094 nonché al comma 2 dell'art.2104, qui con dizione più articolata ed esplicita, che così suona: «*Il prestatore di lavoro...deve inoltre osservare le disposizioni per l'esecuzione e per la disciplina del lavoro impartite dall'imprenditore e dai collaboratori di questo dai quali gerarchicamente dipende».*

Nella sua qualità di creditore di lavoro subordinato, il datore di lavoro esercita nei confronti del lavoratore, oltre al potere direttivo ed al potere disciplinare, anche il potere di controllo volto a verificare l'esatto adempimento degli obblighi del dipendente.

Atteso che nel rapporto è implicata la persona del lavoratore, tale potere di controllo non è assoluto ma è soggetto a vincoli e limiti tesi a garantire il rispetto dei diritti fondamentali della persona, pertanto, del diritto del lavoratore alla propria dignità, libertà e riservatezza.

Di seguito evidenziamo al lettore una delle tipologie – quella del cd. "controllo a distanza" disciplinato dall'art. 4 della l. n. 300/70 e successive modifiche ([1]), trascritto in nota – tramite cui si attualizza il potere di controllo datoriale, rimandando – per motivi di economicità – a successive trattazioni l'esame delle addizionali forme di controllo datoriale e dei relativi limiti ad esse connessi, rinvenibili: ***a)*** nel controllo ad opera delle guardie giurate e delle agenzie investigative private (*ex* art. 2 e 3 Stat. lav.), ***b)*** nel controllo dello stato di malattia dei lavoratori (*ex* art. 5 Stat. lav.), ***c)*** nel controllo personale tramite sistemi selettivi non discriminatori (i cd. "imparziali", *ex* art. 6 Stat. lav.).

2. Controlli a distanza (art. 4 Statuto dei lavoratori)

Per quanto riguarda le modalità del controllo, l'art. 4 Stat. lav. vieta espressamente l'utilizzo di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività lavorativa.

Il divieto di tale controllo trova la propria *ratio* nella sua potenzialità lesiva della dignità e della riservatezza del lavoratore a causa della sua tendenziale continuità e pervasività.

Nel divieto è ricompresa qualsiasi forma di controllo a distanza che sottragga al lavoratore, nello svolgimento delle sue mansioni, ogni margine di spazio e di tempo nel quale egli possa essere ragionevolmente certo di non essere osservato, ascoltato o comunque "seguito" nei propri movimenti.

Il co. 1 del medesimo art. 4, consente espressamente l'utilizzo di apparecchiature quando - pur comportando indirettamente un controllo sull'attività lavorativa dei dipendenti - esso sia richiesto da esigenze organizzative, produttive ovvero di sicurezza del lavoro o di tutela del patrimonio aziendale.

Il controllo, in questo caso, non è l'obiettivo primario del datore di lavoro che installa l'apparecchiatura, ma costituisce un'inevitabile conseguenza dell'utilizzo dell'apparecchiatura medesima, talché si definisce "preterintenzionale", in quanto costituisce la conseguenza non voluta e non prevista dell'utilizzo dell'apparecchiatura.

In ogni caso, ai fini della legittimità di detto controllo "preterintenzionale", è necessario che l'utilizzo delle apparecchiature idonee al controllo sia oggetto di uno specifico accordo con le

rappresentanze sindacali aziendali oppure, in mancanza di queste, con la commissione interna (istituzione oramai superata e sostituita pressoché totalmente dalle r.s.a.). In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro tramite provvedimento autorizzativo contemplante altresì, ove occorra, le modalità per l'uso di tali impianti.
La particolare chiarezza della disposizione lascia poco spazio ad interpretazioni estensive. Ne consegue, pertanto, che:
a) forme di controllo a distanza sull'attività lavorativa sono sempre interdette;
b) è possibile l'installazione di impianti di controllo a distanza – da cui possa derivare anche la possibilità di controllo "preterintenzionale" a distanza dell'attività dei lavoratori – solo per finalità legate ad «*esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale»* e, comunque, previo accordo con le rappresentanze sindacali o dietro provvedimento della Direzione Territoriale del lavoro (DTL); vincoli condizionanti quest'ultimi, ai quali la giurisprudenza della Suprema corte ritiene sottratti quelli che essa stessa creò (in vigenza del vecchio testo dell'art. 4 Stat.lav.) con la qualificazione di "controlli difensivi" a salvaguardia del patrimonio aziendale, di cui tratteremo *funditus* al paragrafo 2.1.
Ad ogni buon conto, la vigilanza sul lavoro anche se necessaria nell'organizzazione produttiva, va mantenuta in una dimensione umana, evitando il ricorso a sistemi e tecnologie che comportino, come conseguenza anche involontaria, l'eliminazione di ogni spazio di riservatezza e di autonomia nello svolgimento del lavoro ([2]).

2.1. La controversa legittimazione dei cd. "controlli difensivi" a tutela del patrimonio aziendale

Una problematica particolare è quella dei cd. "controlli difensivi", nozione e qualificazione creativa di stampo e fonte giurisprudenziale, elaborata sotto la vigenza della vecchia formulazione dell'art. 4 dello Statuto dei lavoratori del 1970 (modificato ad opera del legislatore del governo Renzi, tramite l'art.23 del D.Lgs. n. 151 del 2015). Il comma 2 del superato art. 4, nel vietare, in linea di principio, il controllo sull'attività lavorativa, tuttavia individuava - non difformemente dall'attualmente vigente e per il tramite della seguente formulazione «*Gli impianti e le apparecchiature di controllo che siano richiesti da* ***esigenze organizzative e produttive ovvero dalla sicurezza del lavoro****»* - quelli che, per l'installazione, erano sottoposti alle procedure garantiste per i soggetti controllabili, costituite dall'accordo con le RSA o, alternativamente, dall'autorizzazione amministrativa dell'Ispettorato del lavoro. Stante questa "circoscritta" individuazione non contemplante le apparecchiature installabili a "*tutela del patrimonio aziendale*", la giurisprudenza si ripropose di colmare tale "scopertura" con la loro legittimazione, giustificata dall'affermazione della loro estraneità all'area dell'art. 4, pertanto sottraendole alle procedure garantiste per i lavoratori (accordo con le RSA o autorizzazione amministrativa dell'Ispettorato del lavoro) e qualificandole destinate a meri "controlli difensivi" del patrimonio aziendale (da furti, rapine, comportamenti penalmente illeciti, sia dei dipendenti che di terzi). Al tempo stesso esprimendo, comunque, l'avviso condizionante che le modalità del controllo preterintenzionale emergente in conseguenza da tali forme di "controllo difensivo", non fossero idonee ad infrangere o pregiudicare il rispetto della dignità e riservatezza dei soggetti destinatari del controllo.
Il nuovo legislatore del cd. Jobs act, nel riformulare l'art. 4 (Impianti audiovisivi) dello Statuto dei lavoratori del 1970, estendeva (tuttavia ed incautamente) le procedure garantiste per i controllabili (accordo con le RSA o autorizzazione della dell'Ispettorato del lavoro), anche a quelle poste a "*tutela del patrimonio aziendale*". Tramite la seguente formulazione: «*Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e* ***per la tutela del patrimonio aziendale*** *e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa* (…) *con l'autorizzazione dell'Ispettorato nazionale del lavoro*».

L'inequivocabile formulazione era da leggersi come dissolvente o annullatrice, dal 2015 in poi, della teorica giurisprudenziale sfociata nella creazione dei cd. "controlli difensivi", svincolati – nel vecchio testo, oramai superato, dell'art. 4 Stat. lav. - dall'assoggettamento alle procedure garantiste per i cd. controllati.
Ma la giurisprudenza- anche quella posteriore alla modifica del 2015 - non si è rassegnata, a tumulare i cd. "controlli difensivi" per la tutela del patrimonio aziendale da essa creati e in precedenza svincolati dall'assoggettamento alle procedure garantiste per i controllabili. Dopo alternate vicende e oscillazioni anche in dottrina, li ha mantenuti tramite l'artificiosa distinzione in "controlli difensivi in senso largo" e "in senso stretto" (così, da ultimo Cass. n. 25732 del 22/9/2021, rel. Raimondi). In questa autorevole sentenza si afferma:« *Occorre perciò distinguere tra i controlli a difesa del patrimonio aziendale che riguardano tutti i dipendenti (o gruppi di dipendenti) nello svolgimento della loro prestazione di lavoro che li pone a contatto con tale patrimonio* (controlli difensivi in senso largoi, ndr)*,* ***controlli che dovranno necessariamente essere realizzati nel rispetto delle previsioni dell'art. 4 novellato in tutti i suoi aspetti*** *e "controlli difensivi" in senso stretto, 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* (…). *Si può ritenere che questi ultimi controlli, anche se effettuati con strumenti tecnologici,* ***non avendo ad oggetto la normale attività del lavoratore, si situino, anche oggi, all'esterno del perimetro applicativo dell'art. 4***».
Ne è conseguita, di fatto ed in concreto, una soluzione giurisprudenziale di segno compromissorio, alla stregua della quale i cd "controlli difensivi" in senso stretto (per la tutela del patrimonio aziendale da comportamenti illeciti dei dipendenti e di terzi estranei) - sebbene svincolati dall'assoggettamento all'accordo sindacale con le RSA o all'autorizzazione amministrativa – potranno essere attivati, mediante gli strumenti tecnologici datoriali *ad hoc*, alla condizione che non siano effettuati "a pioggia", cioè in maniera indifferenziata ed *ex ante,* ma solo in presenza di un "fondato sospetto" datoriale della ricorrenza di un comportamento illecito del singolo accertabile *ex post.*
Dove il requisito dell'effettuazione *ex post* ricorre - secondo la precitata sentenza n 25732/2021 (che ha autorevolmente passato in rassegna e fatto il punto sulla tematica dei controlli difensivi prima e dopo le modifiche apportate all'art. 4 Stat. lav.) - « ***(…) 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.*** *Facendo il classico esempio dei dati di traffico contenuti nel browser del pc in uso al dipendente,* ***potrà parlarsi di controllo ex post solo in relazione a quelli raccolti dopo l'insorgenza del sospetto di avvenuta commissione di illeciti ad opera del dipendente, non in relazione a quelli già registrati*****».**

3. Controlli tramite telecamere: condizioni e limiti

A questo riguardo, va detto che l'installazione di telecamere e microcamere a circuito chiuso per indiretto o potenziale controllo dell'attività dei lavoratori è vietata (e attualizza reato) anche quando l'installazione, non concordata con le RSA (cioè effettuata unilateralmente), si attualizzi mantenendo la telecamera spenta, in attesa della successiva, eventuale, autorizzazione della Direzione territoriale del lavoro.
In senso confermativo si è espressa Cass. 30 gennaio 2014, n. 4331, tramite cui la Suprema corte ha precisato, nuovamente, che l'installazione della telecamera puntata sui dipendenti al lavoro - effettuata senza attendere l'autorizzazione dell'Ispettorato (ora D.T.L.) o l'accordo con le rappresentanze sindacali - comporta la responsabilità penale del datore di lavoro. La sentenza ha, peraltro, ritenuto non meritevole di accoglimento l'argomentazione difensiva datoriale secondo cui le videoriprese sul posto di lavoro erano iniziate soltanto dopo il benestare della Direzione provinciale del lavoro. In particolare - ha tenuto a precisare la Cassazione - che, in virtù dell'art. 4, l. n. 300/1970, va tutelato, a priori, il bene giuridico della riservatezza del lavoratore e, di conseguenza, il reato a carico del datore può configurarsi con

la mera installazione non autorizzata dell'impianto di videoripresa, anche se la telecamera rimane spenta. Affermazione nient'affatto nuova, poiché già nel lontano 1983, Cass. 18 febbraio 1983, n. 1236 - seguita poi da Cass. 6 marzo 1986, n. 1490 e da Cass. 16 settembre 1997, n. 9211 - ebbe a stabilire che il divieto (di cui all'art. 4 Stat. lav.) opera anche nel caso in cui le apparecchiature per il controllo siano state installate ma non ancora funzionanti (ed anche qualora il controllo sarebbe stato solo discontinuo, in quanto destinate ad operare in locali in cui i lavoratori possono trovarsi o accedere solo saltuariamente).
In ragione del diritto delle RSA all'accordo, sussiste – in maniera propedeutica e strumentale – in capo ad esse un analogo diritto di pretendere dall'azienda di ispezionare le apparecchiature "sospette", già in atto, specificatamente nel corso del loro funzionamento (e cioè eminentemente, se non esclusivamente, nel corso dell'orario di lavoro), con la conseguenza che l'eventuale rifiuto (od ostruzionismo) frapposto alla richiesta in questione, concreta una limitazione dell'attività sindacale, indubbiamente suscettibile di integrare gli estremi per il ricorso alla tutela approntata dall'art. 28 Stat. lav. per il cd. comportamento antisindacale.
Va inoltre evidenziato come il fatto che determinate strumentazioni o apparecchiature siano in atto da tempo in azienda, con l'acquiescenza dei lavoratori e delle RSA sin dall'epoca della loro installazione, non viene ritenuto idoneo a porre l'azienda nella condizione giuridica di "trovarsi in regola". Infatti la persistente *potenzialità o effettività* di un ambivalente utilizzo (a fini tecnici e, in forma preterintenzionale, a fini di controllo) obbliga l'azienda, in modo permanente, a ricercare un'intesa con le RSA che ne legittimi inequivocabilmente il comportamento, poiché tale accordo, - come ha correttamente ritenuto il Tribunale di Milano([3]) - non può ritenersi scontato e sussistente (per l'avvenuta installazione delle strumentazioni) a causa «*dell'uso pacifico e non contestato […] per un certo periodo di tempo*» sia dalle RSA sia dai lavoratori.
Quindi, per riassumere, il divieto non è escluso né dalla circostanza che le apparecchiature di videosorveglianza, benché installate, non siano ancora funzionanti, né dall'eventuale preavviso della loro prossima installazione dato ai lavoratori, né infine dal fatto che tale controllo sia destinato ad essere discontinuo perché esercitato in locali dove i lavoratori non possono permanere continuativamente ma trovarvisi solo saltuariamente ([4]).
Inoltre, non è sufficiente che i lavoratori siano stati informati o che abbiano addirittura acconsentito all'installazione del telecamere, per far venir meno le specifiche tutele previste dalla normativa o lo stesso divieto di controllo a distanza (così, Garante per la Privacy, newsletter del 31.10.2013).
Va poi precisato, in tema, che per controllo a distanza deve pacificamente intendersi sia quello effettuato in ambito *topografico* lontano dal lavoratore sia quello conseguibile in tempi *non sincronici* (e cioè differiti) con quelli dell'adempimento della prestazione. La dizione è comprensiva, quindi, di una nozione *spaziale* e di un'alternativa o concorrente nozione *temporale.*
Talché, a quest'ultima stregua, risulta oggettivamente riconducibile alla fattispecie vietata (o condizionata all'accordo preclusivo delle RSA), l'installazione di apparecchiature che - tramite la registrazione e memorizzazione di dati suscettibili di analisi o assemblaggio in tempi successivi - consentano al datore di lavoro un controllo "*anche solo a posteriori"* in ordine alla complessiva attività ed al continuativo comportamento dei lavoratori.
In conformità a questa interpretazione è stato, di conseguenza e del tutto correttamente, stabilito che un *software* che sia in grado di registrare il codice di identificazione del lavoratore, il numero di lavori svolti e non, la durata dei medesimi, ecc., rientra nel divieto *ex* art. 4 ([5]).
L'*attività*, oggetto del controllo vessatorio, va intesa in termini più ampi della vera e propria "attività lavorativa" (di cui al precedente articolo 3, legge n. 300/1970) ed è, quindi, riferibile al complessivo comportamento tenuto dal lavoratore in azienda, sia nel tempo in cui è impegnato ad adempiere all'obbligazione lavorativa così come durante le pause di lavoro e negli spostamenti idonei a favorire i contatti con i colleghi, quali, ad es., per iniziative di proselitismo sindacale ovvero per iniziative di libera manifestazione del pensiero *ex* art. 1, Stat. lav., ecc.

Alla luce delle surriferite precisazioni - e prima ancora che tale sottrazione al divieto fosse introdotta dal comma 2 del "modificato" [6] testo dell'art. 4 Stat.lav. che ora dispone «*2. La disposizione* (di divieto, ndr*), di cui al comma 1, non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze»* - la giurisprudenza era giunta, ragionevolmente, a considerare estranei alla fattispecie del divieto assoluto, gli orologi marcatempo o i più moderni lettori di *badges* posti agli ingressi delle unità produttive, in quanto non finalizzati (eminentemente) al controllo vessatorio sul lavoratore. Finalizzati, invece e notoriamente, a registrare i dati temporali necessari per la gestione aziendale e la remunerazione della prestazione (orari di accesso e uscita, rilevazione degli straordinari, evidenziazione della presenza a mensa in correlazione con gli intervalli contrattuali e nel rispetto dei turni aziendalmente stabiliti, rilevazione della presenza in assemblea, *ex* art. 20 Stat. lav., ai *soli fini* del computo delle ore di fatto utilizzate nell'ambito e fino alla concorrenza del tetto massimo individuale delle 10 ore annue retribuite *pro-capite* ([7]).
Pari liceità è stata riconosciuta alle telecamere a circuito chiuso, installate all'interno delle unità produttive con accesso di clientela, onde controllare la loro affluenza ed individuare i responsabili esterni di eventuali furti o rapine. Sono, infatti, legittime le videoriprese dirette a tutelare il patrimonio **al di fuori dell'orario di lavoro**, anche se l'atto illegittimo è posto in essere dal lavoratore che, al di fuori dell'orario di lavoro, viene, correttamente, equiparato al terzo esterno ([8]).
Restano, comunque, assolutamente vietati i cosiddetti controlli occulti, ovvero quelli effettuati celando i sistemi di videosorveglianza (Garante per la Privacy, provvedimento n. 164 del 4.4.2013, relativo ad un sistema di videosorveglianza installato in una sede di una società, all'insaputa dei lavoratori, senza accordo sindacale né autorizzazione della DTL, formato da apparati di ripresa sapientemente nascosti).
Non rientrano nel divieto, i sistemi di videosorveglianza che entrano in funzione al di fuori dell'orario di lavoro, come deterrente per i furti, **purché il sistema non possa essere attivato dal datore di lavoro durante la prestazione lavorativa dei dipendenti**. E' questo il caso di sistemi regolati da temporizzatori che possono essere modificati, per esempio, solo attraverso l'inserimento di una doppia chiave o *password*, di cui una in possesso del datore di lavoro e l'altra del rappresentante dei lavoratori.

4. Controlli sull'utilizzo delle apparecchiature telefoniche aziendali

Mentre è costituzionalmente tutelata (*ex* art. 15 Cost.) la segretezza delle conversazioni telefoniche, il datore di lavoro può lecitamente verificare manualmente i tabulati telefonici per controllare il traffico telefonico dei dipendenti, non rientrando tale attività nei divieti di cui all'art. 4 della legge n. 300/1970.
Si versa, invece, nella fattispecie del controllo vietato in assoluto (giacché all'insaputa e vessatorio) di cui al comma 1° dell'art. 4, nel caso delle pratiche datoriali (o dei capi diretti) consistenti nel «controllo in cuffia», effettuato eminentemente nei confronti e a danno dei centralinisti ed addetti ai *call center* o a mansioni di operatore commerciale telefonico (*teleseller*) e simili.
Già nel lontano 1972 – prima ancora quindi dell'entrata in vigore della l. n. 675/1996 sulla tutela della riservatezza individuale (cd. *privacy*) – il Pretore di Milano ([9]) ebbe a stabilire che: «*A norma dell'art. 4 dello Statuto dei lavoratori, deve ritenersi illegittimo il sistema dei "controlli in cuffia" effettuati nei confronti dei centralinisti telefonici, perché vessatori e contrari al diritto alla "privacy" che deve ritenersi uno degli interessi primari della collettività*».
Circa l'installazione di centralini elettronici ad elaboratore - con memorizzazione della telefonata, del numero esterno chiamato, del giorno e ora delle telefonate, del relativo numero di scatti e del costo - appare indubbia, giuridicamente, l'esigenza di neutralizzare le funzioni di registrazione sia del contenuto della telefonata sia dei meccanismi di individuazione del soggetto chiamante e chiamato; giacché se si consentisse l'attivazione di tali funzioni il datore

di lavoro incorrerebbe, congiuntamente, anche nella violazione dell'art. 8, Stat. lav., che vieta **l'indagine sulle opinioni e su fatti del lavoratore non rilevanti professionalmente.**
Sanzionabili, comunque, sono i comportamenti del dipendente che utilizzi il telefono aziendale per fini personali, salvo ricorrenze di natura emergenziale ed indifferibili temporalmente.

5. Controlli sull'uso della posta elettronica e di internet, aziendalmente concessi per motivi di lavoro

In relazione al controllo della posta elettronica ricevuta o inviata dai lavoratori, si pone - in via preliminare - il problema di stabilire se i messaggi di posta elettronica rientrino nella nozione di corrispondenza, la cui libertà e segretezza è tutelata dall'art. 15 della Costituzione. Quest'ultimo così dispone: «*La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili. La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge*».
Negli anni novanta del secolo scorso, la Corte Costituzionale è intervenuta sul punto con due sentenze (n. 81 dell' 11/3/1993, e n. 281 del 17/7/1998). In tali sentenze la Corte Costituzionale ha ritenuto che rientra nell'ambito di applicazione della garanzia apprestata dall'art. 15 Cost. non soltanto la segretezza del contenuto della comunicazione, ma anche quella relativa ai dati esterni della comunicazione, cioè quella relativa all'identità dei soggetti e ai riferimenti di tempo e di luogo.
L'autorità Garante per la *privacy* ha affermato, pertanto, che la posta elettronica deve essere considerata corrispondenza privata.
La stessa autorità ha, peraltro, escluso l'applicabilità della normativa penale a tutela della corrispondenza qualora il datore di lavoro abbia avvertito i propri dipendenti che qualsiasi messaggio di posta elettronica (in quanto attinente all'attività lavorativa) può essere reso pubblico in qualsiasi momento (in quanto necessariamente registrato nella memoria dell'elaboratore centrale dell'azienda). Il Garante ha, quindi, escluso la protezione delle *mail* come corrispondenza privata nel momento in cui il datore di lavoro ha redatto un regolamento di utilizzo della posta elettronica nel quale venga, chiaramente, precisato che la posta elettronica è strumento aziendale e non è da considerare corrispondenza privata.
Grava quindi sul datore di lavoro l'onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo, degli strumenti messi a disposizione, ritenute corrette e se, in che misura e con quali presidi tecnologici vengano effettuati controlli.
All'onere per il datore di lavoro di prefigurare e pubblicizzare una *policy* interna, relativa al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare, comunque gli interessati, ai sensi dell'art. 13 del Codice della *privacy*. I lavoratori, in quanto potenziali destinatari dei controlli, hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sul trattamento dei dati che possono riguardarli.
Il diritto di informativa preventiva circa la possibilità di controllo datoriale del contenuto della posta aziendale ricevuta e trasmessa dai lavoratori stessi con *account* aziendale, è stato, altresì, asserito come tassativa condizione legittimante, per il datore di lavoro, dalla stessa Corte europea dei diritti umani (Cedu) di Strasburgo nella decisione del 5 settembre 2017 afferente il caso 61496/08.
Peraltro va sgombrato il campo dall'errato convincimento che la strutturazione dell'indirizzo di posta elettronica aziendale con il nome del lavoratore determini il fatto che la casella diventi "proprietà privata" del dipendente assegnatario.
Secondo una sentenza del 2002 del Tribunale di Milano, il datore di lavoro ha facoltà di accedere alla casella di posta elettronica in qualunque momento, in quanto *«...personalità dell'indirizzo non significa necessariamente privatezza del medesimo, dal momento che l'indirizzo aziendale, proprio perché tale, può sempre essere nella disponibilità di accesso e lettura da parte di persone diverse dall'utilizzatore consuetudinario - ma sempre appartenenti all'azienda (a prescindere dalla identità o diversità di qualifica o funzione: ipotesi, frequentissima, è quella del lavoratore che "sostituisce" il collega per qualunque causa: ferie,*

malattia, gravidanza) e che va ad operare, per consentire la continuità aziendale, sul personal computer di quest'ultimo …».
Allo stesso modo, una sentenza del Tribunale del capoluogo lombardo ha, altresì, escluso che la posta elettronica aziendale possa essere assimilata a quella tradizionale cartacea e su di essa possa vigere il principio di segretezza di cui all'art. 616 del Codice Penale, esprimendosi in questi termini: *«… né, si può ritenere che l'assimilazione della posta elettronica alla posta tradizionale, con la relativa affermazione generalizzata del principio di segretezza, si verifichi nel momento in cui il lavoratore utilizzi lo strumento per fini privati - ossia extra lavorativi -, atteso che giammai un uso illecito - o, al massimo, semplicemente tollerato, ma non certo favorito - di uno strumento di lavoro può far attribuire, a chi questo illecito commette, diritti di sorta …».*
Con una sentenza del 2006, il Tribunale penale ordinario di Torino, sezione distaccata di Chivasso, ha confermato il citato orientamento giurisprudenziale, stabilendo che «*Le attrezzature lavorative e, tra queste, quelle informatiche, devono considerarsi direttamente correlate alla funzione del soggetto che rappresenta l'impresa e, solo in via mediata, devono reputarsi assegnate al singolo dipendente, comunque fungibile nel rapporto con lo strumento aziendale. L'indirizzo di posta elettronica aziendale, al di là dell'uso solo* ***apparentemente*** *personale da parte del dipendente quale principale utilizzatore aziendale, può sempre essere a disposizione di soggetti diversi, appartenenti alla sua stessa impresa. Anche se nell'estensione dell'indirizzo di posta elettronica compare il nome del dipendente che procede all'invio, i messaggi inviati attraverso l'e-mail aziendale rientrano nel normale scambio di corrispondenza che l'impresa intrattiene. Pertanto, in caso di accesso alla casella di posta elettronica aziendale del dipendente da parte dell'impresa, non può ravvisarsi una violazione dell'art. 616 c.p., che contempla il reato di violazione, sottrazione e soppressione di corrispondenza. Non sussiste, infatti, un diritto esclusivo del lavoratore ad accedere* ***in via esclusiva*** *al proprio computer aziendale e ad utilizzare* ***in via esclusiva e riservata*** *la propria casella di posta elettronica aziendale*».
In tema, la Cassazione (sent. n. 47096 del 19.12.2007) ha escluso che possa configurarsi il reato di cui all'art. 616 c.p. nel caso in cui il datore o il superiore gerarchico del lavoratore legga le *mail* aziendali di quest'ultimo, qualora sia previsto che la *password* debba essere portata a loro conoscenza.
Infatti, per la Suprema Corte, nel caso di corrispondenza elettronica, la medesima può dirsi «chiusa» solo nei confronti dei soggetti che non siano legittimati all'accesso dei sistemi informatici di invio o ricezione dei singoli messaggi; pertanto, anche quando la corrispondenza è protetta da *password*, si deve ritenere che la stessa sia legittimamente conoscibile da tutti coloro che possiedono la chiave di accesso a tale sistema informatico.
Ad ogni buon conto il controllo datoriale circa l'uso della posta elettronica o degli accessi ad Internet da parte dei dipendenti è da ritenersi legittimo solo se consegue, in maniera preterintenzionale e **comunque *ex post*** - da strumentazioni installate dal datore di lavoro a salvaguardia del patrimonio aziendale (strutturato dai beni materiali e immateriali, quali immagine e reputazione sul mercato), **non già per il controllo preordinato *ex ante***, mirato alla sorveglianza della prestazione lavorativa.
Precisazione, quest'ultima, correttamente effettuata, in precedenza da Cass. 22 settembre 2021 n. 25732 (adesiva al precedente, conforme, pensiero di Cass. 23.02.2010 n. 4375), per la quale: «*Sono consentiti i controlli anche tecnologici posti in essere dal datore di lavoro finalizzati alla tutela di beni estranei al rapporto di lavoro o ad evitare comportamenti illeciti, in presenza di un* ***fondato sospetto*** *circa la commissione di un illecito, purché sia assicurato un corretto bilanciamento tra le esigenze di protezione di interessi e beni aziendali, correlate alla libertà di iniziativa economica, rispetto alle imprescindibili tutele della dignità e della riservatezza del lavoratore,* ***sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto.*** *Non ricorrendo le condizioni suddette, la verifica della utilizzabilità*

a fini disciplinari dei dati raccolti dal datore di lavoro andrà condotta alla stregua dell'art. 4, l. n. 300/1970, in particolare dei suoi commi 2 e 3».
La possibilità di tali controlli si ferma, dunque, dinanzi al diritto alla riservatezza del dipendente *«al punto che la pur insopprimibile esigenza di evitare condotte illecite da parte dei dipendenti [non] può assumere portata tale da giustificare un sostanziale annullamento di ogni forma di garanzia della dignità e riservatezza del lavoratore. Tale esigenza (...) non consente di espungere dalla fattispecie astratta i casi dei cd.* ***controlli difensivi*** *ossia di quei controlli diretti ad accertare comportamenti illeciti dei lavoratori quando tali comportamenti riguardino (...) l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro e non la tutela di beni estranei al rapporto stesso, ove la sorveglianza venga attuata mediante strumenti che presentano quei requisiti strutturali e quelle potenzialità lesive, la cui utilizzazione è subordinata al previo accordo con il sindacato o all'intervento dell'Ispettorato del lavoro. In tale ipotesi, è stato precisato, si tratta di un controllo c.d. preterintenzionale che rientra nella previsione del divieto flessibile di cui all'art 4, c. 2 (Cass. 23.02.10 n. 4375), così correggendosi una precedente impostazione che riteneva* ***in ogni caso*** *legittimi i c.d. controlli difensivi, a prescindere dal loro grado di invasività (Cass. 3.04.02 n. 4746)»* [10].
Attraverso la tracciabilità della navigazione in internet, poi, il datore di lavoro può potenzialmente controllare a distanza il lavoratore, compresi i suoi periodi di lavoro e le eventuali pause. Stante il divieto *ex* art. 4 della legge n. 300/1970, è, pertanto, da considerarsi pacificamente vietato installare sui computer dell'azienda assegnati ai lavoratori *software* finalizzati alla registrazione ed al controllo delle attività del lavoratore, mentre devono essere oggetto di accordo con le Rsa o autorizzazione della Direzione territoriale del lavoro i programmi che hanno altre finalità ma che incidentalmente permettano anche il controllo della navigazione.

6. Controlli tramite apparecchiature di geolocalizzazione

L'innovazione tecnologica ha consentito anche - tramite l'installazione di sistemi di geolocalizzazione (GPS) per la gestione delle flotte aziendali - un'ulteriore modalità di potenziale controllo indebito sui lavoratori (da ricondurre sotto la disciplina definita nell'art. 4, Stat. lav.), atteso che tali sistemi hanno idoneità non solo a consentire la localizzazione delle auto affidate ai dipendenti, ma anche di fornire online *report* storici dei tragitti, chilometri percorsi, soste effettuate.
Al riguardo si registra un caso - giunto all'esame di Cass. 5 ottobre 2016 n. 19922 – di un lavoratore licenziato a seguito del controllo a distanza tramite GPS sull'autovettura, invalidato dalla Suprema corte per carente rispondenza dell'asserito (ma insussistente) "controllo difensivo" ai requisiti di legittimità giurisprudenzialmente consolidati. Requisiti consistenti nel fatto di non dover essere, gli asseriti "controlli cd difensivi", disposti in maniera generalizzata *ex ante*, - con evidente lesione della dignità e riservatezza del prestatore – ma *ex post* al ricorrere di un **fondato sospetto** di pregiudizi o danni alle componenti del patrimonio aziendale. La citata decisione così si espresse: «*appare evidente che il controllo permesso dal sistema GPS sulle autovetture della società permetteva un controllo a distanza dell'ordinaria prestazione lavorativa,* ***non la tutela di beni estranei al rapporto di lavoro****; non si può, infatti, accedere, alla tesi per cui fossero in gioco il patrimonio e l'immagine dell'azienda posto che eventuali pregiudizi agli stessi sarebbero in realtà derivati solo dalla non corretta esecuzione degli obblighi contrattuali e non già da una condotta specifica quale appropriazioni indebite del patrimonio aziendale, furti, lesione della riservatezza di dati societari etc. Diversamente opinando si finirebbe per estendere, senza ogni ragionevole limite, il concetto di controlli "difensivi", perché quasi sempre la violazione degli obblighi contrattuali dei dipendenti può generare danni alla società (ed alla sua reputazione) che però costituiscono il "rischio naturale" correlato all'attività imprenditoriale* ***che la legge non consente di limitare attraverso sistemi invasivi della dignità dei lavoratori e comunque senza autorizzazione sindacale***».

L’applicazione delle sofisticate tecnologie informatiche (videoterminali, computer, ecc.) induce a ulteriori riflessioni e cautele.
Spesso il *software* è strutturato (dall’uomo) in modo tale da consentire non solo la ricostruzione di tutti i passaggi, fasi e transazioni compiute per realizzare un certo programma o prodotto, ma anche per risalire all’identità di colui che ha compiuto le varie operazioni, il momento esatto del loro compimento, i tempi spesi per la realizzazione del lavoro nel suo complesso e nelle singole fasi intermedie e strutturalmente costitutive. Non è un segreto che - a seguito della potenzialità di accesso ad Internet da parte dei lavoratori fruitori per lavoro dei computer aziendali - le aziende si siano dotate di uno specifico *software* da installare nei computer dei dipendenti o nel calcolatore centrale, tramite il quale monitorare gli accessi (indirizzi, url, siti visionati, ecc.) effettuati dal singolo lavoratore e quindi verificare se ciò sia avvenuto per esigenze di lavoro ovvero per uso privato, aziendalmente non consentito e sanzionabile disciplinarmente.
Si versa, a fronte di tale potenzialità – se non ricorrono le esigenze di tutela del patrimonio aziendale nelle sue molteplici componenti tecniche ed economiche – nella ipotesi vietata dal comma 1° dell’art. 4 Stat. lav.. Trovandosi in questa ipotesi, è necessario e vincolante che, a livello aziendale, si raggiungano accordi tra RSA e datore, tramite cui si stabilisca che il *software,* i tabulati ed i programmi attivati dai lettori di *badges* (tesserine magnetiche) o da *password*, debbano – in linea di principio ed a priori – escludere la facoltà aziendale di «occhiuta» individuazione dell’operatore che effettua le transazioni routinarie (o gli accessi ad Internet) e limitarsi a rilevare, ad es., soltanto la di lui appartenenza al «gruppo» abilitato alle transazioni o agli accessi alla rete. Per tale via realizzando un necessario stemperamento dell’altrimenti personalizzato controllo dell’attività del singolo operatore. Ciò normalmente avviene attraverso la sostituzione del codice individuale (nei *badges* abilitanti alle transazioni) con il codice di «gruppo» o di reparto (e per l’accesso ad Internet, consentendolo con la *password* «collettiva» o, meglio, senza *password*).
A conclusione va precisato che, secondo la Suprema corte - espressasi tramite Cass., 17.6. 2000 n. 8250, Cass. 17.7.2007 n. 15892 e Cass., 23.2. 2010 n. 4375 - i dati registrati, i riscontri o fotogrammi, acquisiti tramite installazioni illegittime, sono inutilizzabili processualmente ai fini di giustificare le sanzioni disciplinari irrogate da parte datoriale.

Roma aprile 2022

(*) Giuslavorista

[1]() Art. 4. Impianti audiovisivi.
1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.
2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.
3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196.
[2]() Cfr. Cass. n. 4375 del 23.2.2010.
[3]() Sentenza del 7.7.1977, in *Or. giur. lav.* 1977, 718.
[4]() Cfr. Cass. 6.3.1986, n. 1490 e Cass. 16.9.1997, n. 9211.
[5]() Nel caso di specie – riscontrato da Pret. Milano 5/12/84 - i dirigenti furono comunque assolti per asserita assenza di ogni consapevolezza del disvalore "sociale" del controllo in questione.
[6]()Modificato da parte del legislatore del Jobs act, tramite l' art. 23 del d.lgs. n. n. 151 del 2015.
[7]() Cfr. Pret. Napoli, 15.3.1990, in *Not. giurisp. lav.* 1990, 226; in precedenza, nello stesso senso, Pret. Milano, 12.7.1988, in *Or. giur. lav*. 1988, 936.
[8]() Cfr. Cass. 3.7.2001, n. 8998.
[9]() Sentenza del 12.5.1972, in *Foro it.* 1972, I, 2710.
[10]() Così Cass. 2722 del 23.2.2012.