LavoroDirittiEuropa
Rivista nuova di Diritto del Lavoro

Numero 1 / 2023

Paolo Tosi

Controlli sul lavoro e tutela del patrimonio aziendale

Controlli sul lavoro e tutela del patrimonio aziendale[1]

Paolo Tosi

1. Il mondo dei controlli sul lavoro (e del relativo contenzioso giudiziario) suole essere diviso in due emisferi a seconda che siano esercitati all'interno dell'azienda o comunque della sua organizzazione produttiva ovvero all'esterno di essa.

Entrambi gli emisferi includono i controlli che sono comunemente definiti difensivi se e quando mirati alla rilevazione di comportamenti illeciti, lesivi di beni aziendali, commessi dai dipendenti.

Non certo per amore delle categorie, che non mi appartiene, ma per chiarezza del quadro tematico, pare anche a me opportuno dividere il primo emisfero in due sezioni.

La prima sezione è quella dell'esercizio del controllo tramite impianti che consentono/comportano la percezione continuativa e diretta dell'attività dei lavoratori e soprattutto la registrazione dei loro comportamenti. È la sezione certamente visualizzata dal legislatore del 1970 (telecamere etc.) cui si è aggiunta qualche apparecchiatura tecnologicamente più sofisticata, come l'ascolto e la registrazione <in cuffia> delle conversazioni con i clienti ad opera del personale a ciò adibito.

La seconda sezione è costituita dai controlli, un tempo solo con sforzo ricondotti alla fattispecie del testo originario dell'articolo 4, esercitati tramite <dispositivi mobili> (cellulari, palmari, ricevitori *gps* etc.) e tramite apparecchiature informatiche in dotazione ai lavoratori o di loro proprietà ma utilizzati anche per rendere la prestazione lavorativa.

Malgrado la complessità crescente del mondo dei controlli esercitati all'interno dell'azienda o comunque della sua organizzazione produttiva, talora in bilico tra le due sezioni, può dirsi senza tema di eccessiva semplificazione che fino al 2015, cioè fin quando referente è stato l'originario testo dell'articolo 4 dello statuto, nonostante l'ingresso nell'ordinamento degli interventi in materia di *privacy* (L. n. 675/1996 e D.lgs. n. 196/2003), la giurisprudenza, pur nella varietà delle argomentazioni, ha per lo più consentito la sanzione degli illeciti. In particolare:

a) quanto ai controlli ex art. 4, cioè tramite mezzi audiovisivi o similari, ha per lo più sanzionato eventuali iniziative disciplinari per carenza di accordo/autorizzazione riconoscendo

[1] È la riscrittura della relazione svolta nella Prima Sessione del Convegno su ***Privacy e rapporti di lavoro*** organizzato dall'Università di ROMA TRE e da FA.RI il 22 novembre 2022. Sarà pubblicata negli *Atti* curati da FA.RI.

implicitamente, ma anche esplicitamente (cfr. Cass. n. 6498/2011), in caso di accordo/autorizzazione, la facoltà di utilizzare i dati al fine della repressione degli illeciti;

b) quanto ai controlli tramite <dispositivi mobili> o apparecchiature informatiche senza l'uso di mezzi audiovisivi e similari, li ha ritenuti estranei all'art. 4 se volti ad accertare condotte "illecite" dei dipendenti lesive di beni estranei al mero credito della prestazione lavorativa purché effettuati successivamente all'insorgere del sospetto di illecito e "mirati" allo specifico accertamento di esso da parte di dipendenti determinati o comunque appartenenti all'area di quelli potenzialmente autori dell'illecito stesso.

Gira voce, tra gli operatori del diritto, che il Legislatore abbia riscritto l'articolo 4 dello statuto al fine di introdurre una disciplina restrittiva quanto all'utilizzo sul piano sanzionatorio dei comportamenti del lavoratore conosciuti tramite i controlli. Dubito però che ad un Governo, il quale aveva appena emanato il *Jobs act*, si possa attribuire il perseguimento di tale intento nella redazione di un decreto legislativo *omnibus*, deputato ad introdurre "disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporti di lavoro e pari opportunità".

Piuttosto è opportuno tener conto che il Legislatore delegato del 2015, in generale, non ha brillato per la limpidezza ed interna coerenza dei suoi enunciati normativi.

La riscrittura, nel 2015, dell'articolo 4 dello statuto, opportuna o meno che fosse, ha puntualmente riaperto, segnatamente, la questione della utilizzabilità sul piano disciplinare, e a quali condizioni, dei dati acquisiti tramite gli strumenti utilizzati dai lavoratori per svolgere la propria prestazione. Ciò anche perché non tutte le aziende sono solite adottare accorte *policy* relativamente al loro uso.

Avverto subito che non intendo interloquire qui con le molte disquisizioni dottrinali versate nella materia, ad esempio, con quelle relative alla portata del riferimento alla tutela del patrimonio aziendale contenuto nel comma 1 (dal quale taluno vorrebbe desumere l'intervenuta preclusione dei controlli <difensivi>) o, ancora, con quelle sull'ambito degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" di cui al comma 2. Me ne sono occupato in un recente scritto e ad esso mi permetto di fare rinvio (P. TOSI-E. PUCCETTI, *Sulla legittimità dei c.d. controlli difensivi* in *Arg. Dir. Lav.*, 2021, p. 1297 e ss.).

Negli evidenti limiti di una relazione preferisco concentrare l'attenzione sull'orientamento risultante da alcune sentenze emesse da un Collegio della Suprema Corte che pare avviato a divenire il Collegio di riferimento per questo genere di contenzioso.

Le prime due sentenze sono state emesse nella stessa udienza ed hanno quale Presidente ed Estensore Guido Raimondi.

2. Delle due, la più significativa è sicuramente la n. 25732/2021 giacché diffusamente argomentata in dichiarata funzione nomofilattica. Può quindi essere considerata la capostipite dell'orientamento in via di formazione.

Questo il caso. Essendo stato il sistema informatico aziendale aggredito da un *virus* presumibilmente entrato attraverso un computer di lavoro, a seguito dei relativi controlli era emerso che ciò si era verificato per la frequentazione di siti non affidabili, eufemisticamente definiti "privati", da parte di una lavoratrice; la quale per questo era stata licenziata e aveva impugnato il licenziamento lamentando la violazione dell'art. 4, comma 3.

La sentenza, quanto alla legittimità dei controlli difensivi, ha, come vedremo, quale referente sostanziale, pur se non esplicitato, il comma 3 del nuovo art. 4 Stat. lav.

La Corte muove infatti dalla autonoma premessa che quei controlli sopravvivono alla riforma, esternamente al perimetro segnato da tale articolo, ma devono essere circoscritti nei confini imposti dal "corretto bilanciamento", richiesto dall'art. 8 della Convenzione europea dei diritti dell'uomo come interpretato dalla giurisprudenza della CEDU, "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" (par.38).

A tale stregua, la Corte afferma che l'interprete deve dividere i controlli difensivi in due categorie (ohimè, le categorie!), quelli "in senso lato" e quelli "in senso stretto" (par. 29).

I primi sono "quelli 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 che devono necessariamente essere realizzati nel rispetto dell'art. 4 novellato in tutti i suoi aspetti". I secondi 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" (par. 31).

Può allora ritenersi, continua la sentenza (par. 32), che questi ultimi, "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".

Subito dopo, però, la Corte vuole i controlli difensivi in senso stretto assoggettati a condizioni di legittimità che non sono certo meno invasive di quelle previste dal comma 3 dell'art. 4, ed anzi sono da quelle ispirate. Da qui il mio <sostanziale> di poc'anzi.

La Corte stessa finisce infatti per ammetterlo quando muove la censura conclusiva alla sentenza impugnata: "avendo ritenuto la fattispecie inquadrabile nei <controlli difensivi>, ritenuti compatibili con la nuova formulazione dell'art. 4 Statuto dei lavoratori, **la Corte territoriale non ha poi verificato la compatibilità del comportamento datoriale, e quindi della utilizzabilità dei dati informatici raccolti a fini disciplinari, con quest'ultima disposizione"** (par. 49, neretto mio)

Insomma, solo nella forma ma non nella sostanza è scongiurato il paradosso, o vizio logico, di un ragionamento che colloca i controlli difensivi in senso stretto all'esterno dell'art. 4 sulla base di un suo comma, il terzo, in realtà strutturato per stabilire quali controlli, stando dentro l'articolo, consentano l'utilizzazione dei dati "raccolti" per gli effetti statuiti dal suo secondo comma.

Del resto la Corte già nel precedente par. 26 pone l'assunto secondo cui, "come si era ritenuto con riguardo alla superata disposizione dell'art. 4 St. lav. [ma di ciò è lecito dubitare alla luce dell'informazione offerta al riguardo da Cass. n. 32760/2021, est. Balestrieri, come poi vedremo], può continuare a ritenersi che ove il controllo sia invece legittimo, le informazioni raccolte in esito ad esso possano essere utilizzate dal datore di lavoro per contestare al lavoratore ogni sorta di inadempimento contrattuale".

Comunque, ovviamente, il *punctum dolens* è costituito dalla proiezione, nel concreto dell'operazione ermeneutica circa la legittimità dei residui controlli difensivi "in senso stretto", di condizioni tratte (se non, formalmente, dal comma 3 dell'articolo novellato) dalla giurisprudenza europea.

Orbene, la Corte, richiamando variamente le sentenze della CEDU, né può sorprendere, giunge alla conclusione che i dati di cui il datore di lavoro è venuto a conoscenza sono utilizzabili solo se esplorati dopo l'insorgenza del sospetto di illecito e, di più, esclusivamente se acquisiti altresì dopo tale insorgenza. Ciò, sebbene il controllo di dati dormienti, a rigore, venga esercitato solo quando essi sono esplorati e utilizzati.

Sul merito di questo orientamento fermerò ulteriormente l'attenzione più avanti. Prima ritengo opportuno completare la sua ricostruzione considerando le altre sentenze ad esso ascrivibili.

3. La coeva sentenza redatta dal Presidente Raimondi (n. 25731/2021) mi pare, come anticipato, meno significativa. Riguarda un caso in cui, a seguito delle investigazioni su un *software* aziendale finalizzate ad assicurare la conservazione di eventuali *files,* importanti per l'azienda, in sede di disattivazione del *software* medesimo, erano emerse conversazioni di una dipendente con una collega in cui venivano pesantemente denigrati un superiore gerarchico ed altri colleghi.

Anche in questo caso la lavoratrice lamentava la violazione del comma 3 per omessa informativa allegando anche altri motivi di doglianza, accolti essi pure dalla Corte d'appello, attinenti all'inidoneità dei dati rilevati a giustificare il licenziamento.

Qui la Suprema Corte non affronta la questione della sopravvivenza dei controlli difensivi, sollevata dall'azienda, ritenendola inammissibile per novità. Essendo quindi stata accertata nei giudizi di merito la mancanza di informativa, la Corte conferma la sentenza d'appello, peraltro, come detto, fondata anche su altri motivi, limitandosi a rilevare che la "chat aziendale" era uno strumento di lavoro in quanto funzionale alla prestazione lavorativa.

Assai più significativa la sentenza n. 34092/2021, emessa dal medesimo Collegio (Est. Pagetta), avente ad oggetto un caso in cui, a seguito di controlli mirati, era emerso l'"inoltro all'esterno a mezzo della posta elettronica aziendale" di delicati documenti riservati dell'azienda. Il lavoratore sosteneva che il datore aveva strumentalmente provocato l'*alert* per invocare il controllo difensivo.

Più significativa, perché si colloca esplicitamente nel solco tracciato dalla sentenza n. 25732 riproducendone quasi integralmente la parte motiva quasi a solidificarla. Perviene così all'identico risultato di cassare la sentenza della Corte d'appello, che aveva considerato legittimo il licenziamento, per non avere adeguatamente valutato se i dati esplorati dopo l'insorgenza del sospetto fossero stati acquisiti altresì posteriormente ad esso.

Va pure segnalata, sebbene vertente su un caso verificatosi nel vigore del vecchio testo dell'art. 4, un'altra sentenza, poc'anzi menzionata, emessa sempre dal medesimo Collegio (n. 32760/2021). Qui i dati contestati erano emersi da una apparecchiatura finalizzata alla limitazione della quantità di traffico via *internet* disponibile per ciascun dipendente in rapporto alla sua professionalità.

Orbene, la sentenza si segnala in quanto muove dall'assioma secondo cui la novella del 2015 ha "modificato in senso più restrittivo la L. n. 300 del 1970, art. 4, stabilendo che <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>".

La Corte spiega i termini dell'assioma con una frase in sequenza di quella appena riportata: "In sostanza, dopo il cd. Jobs Act gli strumenti raccolti tramite tali strumenti possono essere utilizzati anche per verificare la diligenza del dipendente nello svolgimento del proprio lavoro, con tutti i risvolti disciplinari e di altra natura connessi. Nel precedente quadro normativo [osserva, concludendo, la sentenza] l'orientamento di questa Corte (Cass. n. 16622/12, Cass. n. 19922/16) da cui non si ha motivo di discostarsi, evidenziava l'effettività del divieto di controllo a distanza dell'attività dei lavoratori anche per i controlli difensivi".

Entrambe le sentenze citate affermavano infatti l'inutilizzabilità, per sanzionare meri inadempimenti contrattuali, dei dati acquisiti, in un caso, tramite il rilevamento delle telefonate con il *software bluès* 2000, nell'altro, tramite il *GPS* installato nell'auto di servizio del lavoratore.

4. V'è ancora da chiedersi se l'orientamento formatosi intorno ai controlli sugli strumenti di lavoro sia suscettibile di estensione ai controlli esercitati tramite impianti audiovisivi adottati, previo accordo sindacale o autorizzazione amministrativa, per prevenire e documentare eventuali illeciti dei clienti.

Anche questi controlli, ripeto, possono essere considerati difensivi se l'esplorazione, e la successiva utilizzazione a fini disciplinari, delle registrazioni trattenute da tali impianti avvengono a seguito del serio sospetto di un illecito commesso da un dipendente. Da questa angolazione, stando all'orientamento della Suprema Corte fin qui ricostruito, non v'è alcuna distinzione, nel prisma del nuovo art. 4, tra dati tratti da mezzi audiovisivi e similari ovvero da strumenti di lavoro.

È il caso considerato dal medesimo Collegio della Cassazione nella sentenza n. 32683/2021 (Est. Cinque). Qui, a seguito della mancanza al bar, in un *autogrill*, di determinati prodotti, erano state visionate le registrazioni delle telecamere ed era emerso che un lavoratore, andato in magazzino a prelevarli, ne aveva sottratto alcuni.

La Suprema Corte conferma la sentenza d'appello che aveva considerato legittimo il licenziamento. Precisa però che a ciò può determinarsi *de plano* giacché in contestazione era solo la validità dell'autorizzazione rilasciata dall'Ispettorato prima della modifica legislativa dell'articolo 4 e non era invece "in contestazione, nel caso *de quo*, l'insussistenza delle condizioni di utilizzabilità, cioè, che sia stata data al lavoratore adeguata informazione delle modalità di uso

degli strumenti e di effettuazione dei controlli e che sia stato rispettato quanto disposto da D. lgs. n. 196 del 2003".

Il Collegio insomma ci tiene ad avvertire, nella prospettiva nomofilattica, che per l'utilizzabilità dei dati acquisiti attraverso gli strumenti di cui al comma 1 [per sanzionare gli illeciti, visto il caso in questione] non è sufficiente l'autorizzazione all'installazione ma è necessaria la ricorrenza delle condizioni individuate dalle proprie precedenti sentenze, lì, nella sostanza, qui, direttamente, dal comma 3 dell'art.4.

5. È tempo ormai di trarre le fila del discorso condotto sin qui e di vedere fino a punto l'orientamento disegnato dalla Suprema Corte <regga>.

Anzitutto può rilevarsi come la sua valenza sia vistosamente espressa già dall'esito del giudizio nelle sentenze n. 25732 e n. 340'2, cioè dalla disposta cassazione delle sentenze di appello che avevano considerato legittimo il licenziamento in ragione della gravità degli illeciti contestati.

Nella sentenza capostipite la cassazione è preceduta (par. 51) dalla fissazione esplicita del "principio di diritto" contenente la prescrizione, alla Corte del rinvio, di accertare che **fosse, in concreto, rinvenibile il bilanciamento di cui al par. 38 della motivazione** (neretto mio), "sempre che il controllo riguardi dati acquisiti successivamente all'insorgere del sospetto".

Nella sentenza n. 34092 la prescrizione rimane implicita nel motivo della cassazione (par. 21.10), ma non è meno perentoria.

Insomma, non basta neppure che i dati siano posteriori all'insorgenza del sospetto. Occorre anche che siano raccolti nel rispetto delle condizioni (ormai vien da dire, direttamente, chiedendo venia) di cui al comma 3 dell'art. 4.

Ad es., dalla lettura della sentenza n. 32760/2021, prima considerata, si ricava che il datore di lavoro avrebbe dovuto provare che l'obiettivo della limitazione del traffico via *internet* dei dipendenti in relazione alla professionalità di ciascuno non fosse conseguibile senza l'accesso alla loro posta elettronica.

Dunque, il contemperamento delle contrapposte esigenze di tutela del patrimonio aziendale e della dignità e riservatezza individuali si traduce, alla stregua del descritto orientamento, nella assoluta prevalenza delle seconde e, detto senza veli e senza eleganza, nella impunità degli illeciti.

Per cogliere fino a quali estremi tale sbilanciamento potrebbe condurre si supponga che un autista di autobus, guidando di notte, investa un pedone e che dall'esplorazione della memoria

del cellulare di servizio risulti una sequenza di *chat* di contenuto erotico intrattenute nello stesso torno di tempo dell'incidente.

Già per essere stati acquisiti prima dell'insorgenza del sospetto tali dati dovrebbero ritenersi inutilizzabili per sanzionare l'illecito.

Di più, dovrebbero ritenersi inutilizzabili anche perché fissati nella memoria del cellulare di servizio senza che di ciò, e del loro eventuale utilizzo per sanzionare comportamenti illeciti, l'autista fosse stato informato.

Al medesimo risultato si dovrebbe pervenire, per fare un altro esempio, in caso di dati attestanti comportamenti di *mobbing* posti in essere, mediante gli strumenti di lavoro, nei confronti di colleghi ed acquisiti tramite le indagini intraprese a seguito della doglianza delle vittime.

Credo non occorrano parole per argomentare che simili risultati sarebbero eticamente inaccettabili; ma lo sarebbero anche nei casi di comportamenti illeciti meno appariscenti di quelli appena esemplificati.

L'insegnamento metodologico cui cerco di ispirarmi vuole che l'interprete sia fedele ai canoni fondamentali dell'ermeneutica giuridica (testo, sistema, *ratio legis*) ma, ove possibile, tenga conto dei valori in gioco e del risultato dell'interpretazione (rinvio a P. TOSI, *l metodo nel diritto del lavoro. La lezione di Luigi Mengoni*, in *Arg. Dir. Lav.*, 2007, p. 874 ss.).

Nel rispetto di questo insegnamento l'interprete ritengo debba rinunciare ad individuare ciò che sta fuori del perimetro dell'art. 4 utilizzando (nella sostanza) gli elementi che la norma offre, nel comma 3, in positivo e non in negativo, in funzione cioè degli effetti previsti dal comma 2; segnatamente in funzione della sanzionabilità di meri inadempimenti contrattuali.

Del resto è proprio la sentenza n. 25732/2021, con proposizioni chiare che ho già riportato in precedenza ma che mi pare utile riproporre qui, a muovere dalla premessa che "i <controlli difensivi in senso stretto>, diretti cioè ad accertare specificamente condotte illecite ascrivibili -in base a concreti indizi- a singoli dipendenti, anche se questo si verifica durante la prestazione di lavoro…[ed] 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" (parr. 31 e 32; neretto mio).

Non essendo, notoriamente, anche per la CEDU, quello alla dignità e alla riservatezza un diritto assoluto, il valore della repressione degli illeciti deve essere preservato e non assorbito, come nel criticato orientamento, dalla preoccupazione che "il datore di lavoro, in presenza di un sospetto di attività illecita, possa avere mano libera nel porre in essere controlli sul lavoratore

interessato" (par. 36); segnatamente, che possa, "in difetto di autorizzazione e/o adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, nonché senza il rispetto della normativa sulla *privacy,* 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" (par. 48).

La tutela della dignità e riservatezza del lavoratore non è affatto liberamente compromettibile dal datore di lavoro né è compromessa quando sanziona comportamenti del lavoratore illeciti in sé, per il loro contenuto lesivo, e non perché costituiscono anche, come pure normalmente accade, inadempimenti degli obblighi contrattuali.

L'esplorazione infatti può avvenire solo a seguito di un "oggettivo sospetto" (per usare la formula della sentenza capostipite). È poi <fatto notorio> (ma le aziende sarebbero prudenti se lo rammentassero ai propri dipendenti) che i dati del traffico intrattenuto restano impressi nella memoria dei <dispositivi mobili> e, per le apparecchiature informatiche, nel *server* o nel browser utilizzato. Ancora, i dati estratti devono essere trattati alla stregua dei principi di *privacy* che presiedono alla trattazione dei dati sensibili: quelli non strettamente attinenti alle condotte illecite devono essere immediatamente distrutti; gli altri, utilizzati all'esclusivo fine della repressione degli illeciti, senza divulgazione alcuna, per essere poi distrutti una volta conseguito tale fine.

6. È d'altronde quanto si dovrà continuare a ritenere per i controlli esterni, i cui limiti pacificamente non sono desumibili (né direttamente né indirettamente) dall' art. 4 bensì dagli artt. 2 e 3 dello statuto, ai sensi dei quali al datore di lavoro è precluso affidare alle guardie giurate compiti diversi dalla "tutela del patrimonio aziendale" mentre "i nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa debbono essere comunicati ai lavoratori interessati" affinché la vigilanza stessa non possa essere esercitata in modo occulto.

Da dette norme viene dedotto, infatti, implicitamente, che gli stessi limiti non possono non valere anche per l'attività lavorativa svolta all'esterno dei locali aziendali, con la conseguente inutilizzabilità a fini disciplinari dei dati attinenti alla prestazione lavorativa.

Così, è richiamando il consolidato orientamento giurisprudenziale che Cass. n. 25287/2022 (Pres. Tria, Est. Esposito) cassa la sentenza di appello per aver giudicato legittimo il licenziamento di un dipendente di Banca il quale, nel corso di una vigilanza commissionata ad una agenzia investigativa per il controllo di una sua collega che avrebbe dovuto trovarsi al lavoro

in azienda, era stato sorpreso mentre si accompagnava con lei in palestre, *hotels* etc., cioè in luoghi non pertinenti alla propria attività lavorativa.

Coerentemente con l'orientamento richiamato, la Corte motiva la cassazione della sentenza d'appello impugnata osservando che per quel dipendente tale attività "era connotata da una certa flessibilità riguardo all'orario e alla sede di svolgimento" della stessa. Pertanto, secondo la Corte, nei suoi confronti il controllo finiva per vertere, sostanzialmente, sull'adempimento della prestazione lavorativa e quindi le informazioni acquisite, in quanto non strettamente attinenti alla commissione di un illecito, dovevano ritenersi inutilizzabili a fini disciplinari.

7. Sintetizzando, dunque, è mia opzione che il bilanciamento tra le esigenze di tutela del patrimonio aziendale e le esigenze di tutela della dignità e riservatezza del dipendente debba pendere verso le prime, senza riserve ed eccessi di garantismo individuale, quando il patrimonio aziendale è leso da comportamenti illeciti del dipendente che non attengono all'adempimento in sé della prestazione lavorativa.

Questa opzione, successivamente allo svolgimento della mia relazione, ha trovato conforto in una recentissima sentenza della CEDU (Gramaxo c. Portogallo, 13 dicembre 2022, richiesta n. 26968/16).

Tramite il sistema di geolocalizzazione installato sull'auto messa a disposizione di un rappresentante medico era stata rilevata e sanzionata una serie di inadempimenti della prestazione lavorativa nonché la mendace indicazione dei chilometri percorsi per uso personale, per i quali era dovuto un rimborso a favore del datore di lavoro.

Orbene, la Corte europea avalla la decisione del giudice nazionale sulla legittimità del licenziamento osservando anzitutto che "la cour d'appel n'a pas invalidé l'ensemble des donnés de gèolocalisation litigieuses mais seulement celles qui consistaient à opérer un contrôle sur l'activité professionelle de l'employé" (par. 119).

Quel che poi conta, ed è decisivo per la Corte, è che poi, nell'ambito di quei dati, "en retenant uniquement les données de géolocalisation concernant le kilométrage parcouru, la cour d'appel de Guimarães a réduit l'empleur de l'intrusion dans la vie privée du requérant à ce qui était strictement necessaire au but légitime poursuivi, à savoir le contrôle des depenses de l'entreprise" (par. 120).

La CEDU, insomma, nella sostanza ha considerato prevalente, nel bilanciamento delle esigenze, quella di punizione della truffaldina esposizione, da parte del dipendente, di un maggior numero di chilometri percorsi per servizio rispetto a quelli percorsi per uso personale.

La sentenza è particolarmente significativa perché esamina nel dettaglio la motivazione della sentenza della Corte d'appello portoghese ed inoltre perché è resa dal Collegio della Corte europea, può immaginarsi, a faticosa maggioranza. I Giudici di minoranza hanno infatti voluto esporre, in calce alla sentenza, la propria "opinion dissidente commune".

Filo conduttore di tale "opinione" è questa frase <chiave>: "la balance était ici [nella sentenza della Corte nazionale] mal étalonnée car l'ingérence de l'employeur dans la vie privée du salarié est très serieuse".

Significativo, il tutto, giacché gli argomenti spesi dai Giudici dissenzienti a valle di tale premessa, alcuni dei quali ricorrenti nelle criticate sentenze della nostra Suprema Corte, offrono testimonianza della capacità di resistenza, nelle operazioni ermeneutiche, degli <*a priori*> ideologici.