

*ADAPT - Scuola di alta formazione sulle relazioni industriali e di lavoro*

*Per iscriverti al **Bollettino ADAPT** [clicca qui](#)*

*Per entrare nella **Scuola di ADAPT** e nel progetto **Fabbrica dei talenti** scrivi a:  
[selezione@adapt.it](mailto:selezione@adapt.it)*

*Bollettino ADAPT 25 ottobre 2021, n. 37*

La categoria dei controlli datoriali c.d. “difensivi” era stata elaborata dalla giurisprudenza sul duplice presupposto che detti controlli a distanza fossero finalizzati specificamente ad accertare determinati **comportamenti illeciti** del lavoratore e che questi ultimi fossero **lesivi del patrimonio o dell’immagine aziendale**. In presenza di tali requisiti, la giurisprudenza non riteneva necessaria la sussistenza dei presupposti di legittimità stabiliti dall’art. 4 St. Lav..

A seguito delle modifiche introdotte dal d.lgs. 14 settembre 2015, n. 151 (c.d. *jobs act*), si è molto dibattuto sulla possibilità di effettuare ancora i suddetti controlli difensivi, in quanto il nuovo art. 4 St. Lav. assoggetta ai presupposti di legittimità ivi previsti anche i controlli finalizzati alla “*tutela del patrimonio aziendale*”, mentre tale finalità non era indicata nella precedente versione del 1° comma: pertanto, si è posta la questione se i “controlli difensivi” non debbano ormai ritenersi completamente attratti nell’area di operatività dell’art. 4 St. Lav..

Sul punto è intervenuta di recente la Corte di Cassazione (Cass. 22 settembre 2021, n. 25732), la quale ha affermato che “*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 libertà e della riservatezza del lavoratore, sempre che il controllo riguardi dati acquisiti successivamente all’insorgere del sospetto*”.

Tale principio risulta del tutto in linea con la pronuncia della Corte Europea dei Diritti dell’Uomo, Grande Camera del 17 ottobre 2019 (caso L.R. e altri c. Spagna), che ha accertato la legittimità dei controlli a distanza effettuati dal gestore di un supermercato dopo che lo stesso aveva riscontrato diverse mancanze dal magazzino e aveva il ragionevole sospetto che ciò dipendesse da illecite condotte aziendali poste in essere da alcuni dipendenti (sospetto poi confermato dai controlli effettuati). In particolare, tale pronuncia aveva confermato la compatibilità dei controlli difensivi con la tutela della riservatezza di cui all’art. 8 della Convenzione europea dei diritti dell’uomo.

In estrema sintesi, quindi, i controlli difensivi del datore di lavoro sono ancora possibili alle seguenti condizioni:

- a) che vi sia un “fondato sospetto” di commissione di un illecito, che deve sorgere in base a circostanze già verificatesi (ad esempio, l’inspiegabile mancanza di merce dal magazzino);
- b) che il controllo avvenga in un momento successivo al sorgere del predetto “fondato sospetto”.

In particolare, nel caso esaminato dalla Corte di Cassazione, una lavoratrice era stata licenziata in quanto il datore di lavoro aveva rilevato, nella cartella di download del disco fisso del pc aziendale a lei assegnato, non solo la presenza di un virus che aveva infettato la rete aziendale, ma anche numerosi accessi a siti internet visitati dalla dipendente per ragioni private e per considerevoli periodi di tempo, tali da integrare una sostanziale interruzione della prestazione lavorativa.

Ebbene, la Suprema Corte ha cassato la sentenza di merito che aveva ritenuto legittimo l’utilizzo di tutte le informazioni raccolte a fini disciplinari con la sola motivazione che l’accesso era stato effettuato per un fondato sospetto di attività illecita indotto dalla scoperta del virus, non avendo verificato la Corte di appello se il controllo “*avesse ad oggetto **esclusivamente dati informatici raccolti successivamente all’insorgere del fondato sospetto***”.

Alla luce di quanto precede, si può affermare che i controlli difensivi sono ancora oggi possibili, ma con limiti molto stringenti. Ciò anche in ragione del principio di bilanciamento d’interessi a cui fa

riferimento la sentenza in esame: infatti, sarà sempre necessario verificare, caso per caso, se il controllo a distanza sia stato effettuato in modo eccessivamente invasivo - rispetto all'interesse tutelato dall'imprenditore - o comunque se vi sia stata un'eccessiva compressione della sfera privata del lavoratore, in applicazione dei principi ricavabili dalla normativa in materia di privacy (in particolare, i principi di necessità, correttezza, pertinenza e non eccedenza).

Di conseguenza, il datore di lavoro che intenda svolgere anche **controlli in via preventiva** per tutelare il patrimonio e l'immagine aziendale - nel contesto dell'attuale versione dell'art. 4 Stat. Lav. - dovrà anzitutto inviare ai propri dipendenti una chiara informativa ai sensi dell'art. 4, comma 3, Stat. Lav., al fine di poter utilizzare tutte le informazioni raccolte, tramite gli strumenti di lavoro, anche a fini disciplinari.

Principio di diritto che la Corte, in una vicenda simile, ha ribadito (Cass. 22 settembre 2021, n. 25731), dichiarando l'inutilizzabilità dei dati raccolti in una chat aziendale (ritenuta pacificamente uno "strumento di lavoro", poiché "funzionale alla prestazione lavorativa") in quanto, pur avendo considerato legittimo l'accesso aziendale dovuto a specifiche esigenze di manutenzione del sistema, "*era mancata l'adeguata informazione preventiva del lavoratore*" ai sensi dell'art. 4, comma 3, St. Lav..

In conclusione, è opportuno porre sempre la massima attenzione a tale adempimento, al fine di poter poi intervenire in modo efficace su eventuali comportamenti scorretti dei dipendenti, al di fuori degli stringenti limiti a cui sono tuttora ricondotti i c.d. controlli difensivi.

**Federico Ubertis**

ADAPT Professional Fellow