CONTROLLO DEL PC AZIENDALE SÌ O NO?

La Cassazione ha fatto chiarezza sulla possibilità di controllare i PC assegnati ai dipendenti, a patto che sia assicurato il corretto bilanciamento tra esigenze di protezione dell'azienda e di tutela del lavoratore

di **Andrea Savoia**
e **Marilena Cartabia**

Risale allo scorso mese di agosto la notizia di un attacco ransomware subito dalla Regione Lazio che ha disabilitato i sistemi informatici, compreso il portale di registrazione alle vaccinazioni COVID-19, e che si presume essere "partito" dal PC di un dipendente. Notizia che, non solo ha fatto il giro del mondo, ma ha riacceso l'attenzione di molte aziende su di un tema correlato alla sicurezza informatica: la possibilità di eseguire controlli sui PC aziendali assegnati ai dipendenti. Ed è di poche settimane fa la notizia che la Corte di Cassazione (sentenza 22 settembre 2021, n. 25732) ha affrontato proprio questo problema, occupandosi della vicenda di una Fondazione "vittima" di un virus inseritosi nella rete aziendale attraverso un file scaricato da una lavoratrice da un sito estraneo l'attività lavorativa. In particolare, la Suprema Corte si è occupata dei controlli cosiddetti difensivi, vale a dire quelli che, secondo parte della giurisprudenza, possono esulare dalle previsioni dell'art. 4 dello Statuto dei Lavoratori (L. 300/1970). Quest'ultima norma, dopo le modifiche del 2015, prevede che gli impianti audiovisivi e gli altri strumenti di controllo possono essere installati per esigenze organizzative e produttive, per la sicurezza sul lavoro e per la tutela del patrimonio aziendale, se viene raggiunto un accordo con la rappresentanza sindacale aziendale (RSU o RSA) oppure, in caso di mancato accordo o di assenza in azienda di strutture sindacali, previa autorizzazione dell'Ispettorato Territoriale del Lavoro. La procedura appena ricordata non si applica invece agli strumenti utilizzati dal lavoratore per rendere la propria prestazione e a quelli di registrazione degli accessi e delle presenze.

Infine, le informazioni raccolte in presenza delle condizioni normative sono utilizzabili a tutti i fini connessi al rapporto di lavoro purché sia data adeguata informazione al lavoratore sulle modalità d'uso e di effettuazione dei controlli, oltre che nel rispetto della privacy.

Chiariti i principi normativi, la Cassazione riconosce l'esistenza di due tipologie di controlli difensivi.

La prima è quella finalizzata alla tutela del patrimonio aziendale e che ha come destinatari tutti i dipendenti (o gruppi di dipendenti che nello svolgimento della loro prestazione possono venire a contatto con il patrimonio aziendale). Questa è soggetta alle previsioni dell'art. 4 dello Statuto: se il datore non rispetta le modalità e procedure previste dalla legge, il controllo sarà ritenuto illegittimo e i relativi risultati inutilizzabili.

La seconda, invece, presuppone la commissione di un grave illecito del lavoratore nello svolgimento della prestazione lavorativa e non è soggetta ai "limiti" dell'art. 4: in questo caso, se si hanno fondati sospetti di un grave comportamento, il datore può svolgere i controlli anche se non ha fornito adeguata informazione sulle modalità d'uso e sulla effettuazione delle verifiche di controllo. In questa seconda ipotesi, per evitare che sia annullata ogni forma di garanzia della dignità e riservatezza del lavoratore, la Corte Suprema raccomanda il rispetto di due limiti: 1) l'attività di controllo deve essere mirata e avvenire "a posteriori", ossia dopo che si è avuto il fondato sospetto del comportamento illecito; 2) i dati utilizzabili sono solo quelli raccolti da quel momento e non altri acquisiti in precedenza. In poche parole, in presenza di un fondato sospetto di illecito con conseguenti gravi danni, potrebbero essere possibili controlli sul PC aziendale, anche in mancanza di preventiva informativa, purché ciò avvenga bilanciando le esigenze di protezione dei beni aziendali con la tutela della dignità e della riservatezza del lavoratore. Anche per tale ragione, il controllo non potrà che riguardare dati acquisiti successivamente all'insorgere del fondato sospetto.

Andrea Savoia partner e **Marilena Cartabia** senior associate
UNIOLEX Stucchi & Partners - www.uniolex.com