



**Ministero Istruzione Università e Ricerca**  
**ISTITUTO SUPERIORE "EUCLIDE"**

*C.da Monoscalco - 89035 Bova Marina Segreteria tel. 0965/499401 fax 0965-499400*

*Indirizzo E-mail [RCIS01600E@istruzione.it](mailto:RCIS01600E@istruzione.it) - C.F.: 92002670807*

**Sezioni:** Liceo Scientifico - I.T. per Geometri - I.T. Commerciale - I.P. Alberghiero

---

4086

Prot. n. del 17/09/2019

Al personale docente

Al personale Ata , ITP; assistenti tecnici

Sede

**Oggetto: informativa sull'utilizzo degli strumenti tecnologici di proprietà dell'Istituzione Scolastica**

Il datore di lavoro, direttamente o attraverso la propria struttura, può verificare l'effettivo e corretto utilizzo degli strumenti di lavoro ed il conseguente adempimento della prestazione lavorativa (cfr. artt. 2086, 2087 e 2104 cod. civ.); ritenuto, tuttavia che, nell'esercizio di tale prerogativa, nel rispetto della libertà e la dignità dei lavoratori, nonché, con specifico riferimento alla disciplina in materia di protezione dei dati personali, i principi di correttezza, (secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori), di pertinenza e non eccedenza di cui all'art. 11, comma 1, del Codice; ciò, può determinare il trattamento di informazioni personali, anche non pertinenti, o di dati di carattere sensibile.

Le disposizioni del decreto legislativo 151/2015, conosciuto anche come Jobs Act, hanno modificato il vecchio Statuto dei lavoratori, comprendendo così la sicurezza informatica, in osservanza alle nuove procedure previste per il controllo dei lavoratori. Si è così inserita una disciplina speciale per gli strumenti di lavoro e per gli strumenti di rilevazione accessi e presenze. Nello specifico, l'articolo 23 del D.Lgs. n. 151/2015 si incarica di modificare l'articolo 4 della Legge n. 300 del 1970 – anche nota come Statuto dei Lavoratori – per rimodulare la fattispecie integrante il divieto dei controlli a distanza, nella consapevolezza di dover tener conto, nell'attuale contesto produttivo, oltre agli impianti audiovisivi, anche degli altri strumenti «dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori» e di quelli «utilizzati dal lavoratore per rendere la prestazione lavorativa». Tra i dispositivi «utilizzati dal lavoratore per rendere la prestazione lavorativa» si trovano: PC, smartphone, tablet ma anche la rete aziendale.

Per tutti gli strumenti di lavoro (PC, smartphone, tablet... ma anche la connessione a Internet) o di rilevazione accessi e presenze, la legge stabilisce una deroga espressa per il loro utilizzo, secondo la quale il datore di lavoro può effettuare controlli sui dispositivi forniti, il tutto nel rispetto del codice della Privacy.

La legge vieta l'utilizzo di strumenti tecnologici per la finalità diretta di controllare a distanza la prestazione di lavoro del dipendente [Art. 4 co. 1 L. n. 300/1970.]. Può tuttavia accadere che uno strumento tecnologico venga utilizzato in azienda non con lo specifico fine di controllare i dipendenti ma per altre finalità, tutte lecite, come l'organizzazione del lavoro, la sicurezza del personale, la tutela dei beni aziendali, etc. ma dal suo utilizzo si possa anche ricavare un eventuale controllo a distanza del dipendente, in quanto la tecnologica consente di usare il PC aziendale anche come strumento di controllo della prestazione di lavoro. Tramite semplici strumenti tecnologici, infatti, il datore di lavoro potrebbe entrare nel PC dato in uso al dipendente e vedere come viene usato dal lavoratore, quindi vedere, in tempo reale, cosa sta facendo il lavoratore, su quali siti web sta navigando, su quali file sta lavorando, etc. Dopo il controllo, il datore di lavoro potrebbe usare le informazioni raccolte per assumere dei provvedimenti nei confronti dei dipendenti.

Si avvisa dunque, ponendosi nelle condizioni di legittimità del controllo [Cass. n. 26682 del 10.11.2017; Cedu causa n. 61496/08; Garante Privacy provv. del 29.03.2018], che:

- 1) il datore di lavoro si riserva la possibilità di controllare gli strumenti di lavoro concessi in uso ai lavoratori e l'uso che ne viene fatto; il controllo si limiterà a quanto strettamente necessario per la finalità del controllo e saranno comunicati al dipendente i dati per la sua tracciabilità. Se ad esempio, il controllo deve verificare i siti web visitati da quel PC in data 10 aprile 2018, perché in quella data c'è stata la connessione ad un sito web pericoloso, sarebbe illegittimo controllare tutti i siti web visitati dal dipendente nel mese di aprile 2018.
- 2) E' esplicitamente consentito l'uso di tutti gli strumenti di lavoro (PC, smartphone, tablet... ma anche la connessione a Internet) mai per fini personali, ma solo lavorativi. Stesso discorso va fatto con riferimento alla possibilità di installare nel PC di lavoro un supporto esterno come, ad esempio, cuffie, una chiavetta USB, un hard-disk esterno, etc.: questi comportamenti sono vietati perché da questi supporti potrebbero pervenire delle minacce al PC di lavoro ed alla rete interna.
- 3) Sussiste la giusta causa di licenziamento nel caso in cui il lavoratore abbia trascorso il tempo destinato al lavoro, e come tale retribuito, a collegarsi per scopi personali ad Internet ed a consultare i documenti scaricati, con la rete telefonica pagata dall'azienda, integrando tale comportamento una grave violazione degli obblighi contrattuali (Corte d'appello Ancona 1/8/2003).
- 4) Con sentenza n. 17859 del 13 agosto 2014, la Cassazione ha ritenuto legittimo il licenziamento di un lavoratore che, per fini personali, si era connesso, con il computer aziendale, ad internet ed aveva scaricato films ed altro materiale con l'uso di programmi di file-sharing, anch'essi scaricati da internet.
- 5) E' vietato lo svolgimento di attività parallela in favore di terzi mediante utilizzo di strumenti aziendali (Sentenza Corte di Cassazione, Sez. lavoro, 28.01.2013, n. 1813 ).
- 6) E' vietato l'accesso abusivo ad un sistema informatico o telematico (Cassazione penale , sez. V, sentenza 15.02.2007 n° 6459 e Sentenza della Corte di Cassazione n. 40303/2013) e l'accesso abusivo ad un sistema informatico anche per chi consulti senza permesso la casella di posta elettronica di un collega (sentenza 15 dicembre 2014, n. 52075).



Dirigente scolastico

Carmela Lucisano