IPSOA Quotidiano

L'EDITORIALE DI LUCA FAILLA-12 APRILE 2025

Controlli difensivi sul luogo di lavoro. Cosa dice la giurisprudenza

Luca Failla - Professore a contratto di Diritto del Lavoro presso l'Università degli Studi LUM

La disciplina dei controlli difensivi dei lavoratori si deve sempre adeguare alle esigenze dell'organizzazione d'impresa. Le implicazioni non sono di poco conto e gli orientamenti del Garante della Privacy e dell'ultima giurisprudenza stanno sollevando più di un interrogativo sull'influenza della disciplina del GDPR. Oggi più che mai, anche a seguito del massiccio ingresso dell'intelligenza artificiale nella gestione di molte attività lavorative. Cosa dice la recente giurisprudenza? Sono inutilizzabili a fini disciplinari, le informazioni acquisite (senza adeguata informativa al lavoratore) sulla base di indagini tecnologiche svolte relativamente a periodi antecedenti l'insorgenza del sospetto. Ma negarne la possibilità costituisce per le aziende un'ingiustificata limitazione della legittima facoltà dei controlli difensivi finalizzati sì a prevenire gli illeciti, ma anche a tutelare il patrimonio aziendale allorché gli illeciti siano già stati commessi!

Con l'entrata in vigore del nuovo testo dell'art. 4 dello Statuto dei Lavoratori si è aperto un nuovo capitolo nella disciplina dei **controlli difensivi**, ancorché nel quadro di una esigenza - sentita da tempo - di adeguamento della disciplina di riferimento (risalente ormai agli anni '70) alle esigenze della moderna **organizzazione d'impresa**.

La norma, nel testo novellato nel 2015, ha voluto da questo punto di vista operare una **distinzione** fondamentale tra **strumenti e apparecchi** dai quali possono derivare **forme di controllo a distanza** (come le videocamere), per i quali è richiesta apposita autorizzazione amministrativa e gli **strumenti di lavoro** (quali ad esempio il personal computer o il laptop) per i quali l'uso - anche a fini disciplinari - delle informazioni raccolte non integra una forma di controllo (altrimenti vietato) dell'attività lavorativa, ma è presupposto per garantire la legittimità di quelli che sono normalmente definiti come "controlli difensivi", ossia quelle forme di **controllo** che sono dettate da **esigenze organizzative, produttive o dalla sicurezza del lavoro**, finalizzate anche alla protezione dei beni e del know how aziendali e ciò anche al di fuori del perimetro previsto dall'art. 4 dello Statuto.

Il vigente testo normativo dell'art. 4 L. n. 300/1970 costituisce la chiara espressione di un'**esigenza di bilanciamento** tra la necessità (e opportunità) di far cadere alcune **rigidità normative** connesse con l'uso e la pervasività della tecnologia nel normale svolgimento della prestazione lavorativa e la **potenziale raccolta di dati** da parte delle **aziende** - utilizzabili eventualmente anche a fini disciplinari - che determina la fondamentale necessità del **rispetto** di alcuni **principi fondamentali** di **tutela** non solo della **privacy** (richiamata peraltro anche nel testo novellato dell'art. 4 L. n. 300/1970), ma soprattutto della **riservatezza** e della **dignità morale** del lavoratore. Principi questi sanciti dall'art. 1 e dall'art. 8 dello Statuto dei lavoratori, oggi integrati dalla disciplina in materia di privacy di cui al Reg. UE n. 679/2016 (**GDPR**) e dagli orientamenti del **Garante della Privacy** i quali, peraltro, con lo sviluppo dei sistemi di **Intelligenza Artificiale** assurgono a principi fondamentali per un **uso etico e accorto** della **tecnologia**, anche nel quadro del Regolamento (UE) 2024/1689 (AI Act).

In questo scenario va detto che la **formulazione della norma** che conosciamo oggi ha da subito **posto** alcuni **fondamentali interrogativi** in termini di **tutela dei dati e di privacy del lavoratore**. Le implicazioni non sono di poco conto e gli **orientamenti** del **Garante della Privacy** e dell'ultima **giurisprudenza** stanno sollevando più di un interrogativo sull'influenza che la **disciplina** posta dal Regolamento UE n. 679/2016 (**GDPR**) **ha** in questa delicata materia. Ed oggi più che mai, anche a seguito del massiccio **ingresso** dell'**Intelligenza Artificiale** nella **gestione** di **molte attività lavorative**, come ad esempio il **lavoro attraverso**

piattaforma (che non coinvolge solo i riders).

L'accelerazione che negli ultimi anni si è registrata in campo tecnologico, con la diffusione di strumenti (*hardware* e *software*) che stanno rivoluzionando anche l'organizzazione del lavoro, sta infatti aprendo nuovi scenari di interpretazione delle norme che da anni governano questa materia. E sono proprio gli **strumenti di ultima generazione** quelli che presentano maggiori **potenzialità di rischio** non solo in termini di violazione delle disposizioni dell'art. 4 dello Statuto, ma anche in termini di violazione delle regole deputate alla protezione dei dati, con alta probabilità di sanzioni da parte del Garante della Privacy: si pensi ai sistemi di **riconoscimento biometrico** (su cui si vedano ad esempio News Garante Privacy 28 marzo 2024, n. 520; News Garante Privacy 6 giugno 2024, n. 338), **oggi vietati** perché considerati ad alto rischio anche in base all'AI Act.

Ma si pensi anche alla maggior parte degli **strumenti oggi utilizzati** per la gestione delle **attività di logistica**, nelle quali entrano anche gli strumenti di **geolocalizzazione**, sempre più sofisticati e oggetto di attento monitoraggio in fase di autorizzazione alla loro installazione e di loro non corretta utilizzazione (v. da ultima News Garante Privacy n. 533/2025). Ma, altresì, alla possibilità che molte delle attività lavorative oggi estremamente automatizzate rendano tracciabile - e quindi in astratto **controllabile** - ogni **singola azione posta in essere dal lavoratore**, anche se non direttamente connessa con l'esecuzione della prestazione lavorativa.

Ascolta il podcast di Pierluigi Rausei Controlli a distanza dei lavoratori. Cosa rischia l'impresa che utilizza l'AI e il GPS?

E' chiaro, quindi, come gli strumenti di lavoro (principalmente il personal computer, il laptop ma soprattutto la posta elettronica ormai abitualmente utilizzata ed i tanti applicativi e software ivi installati) stiano diventando la testa di ponte per la stessa evoluzione della giurisprudenza in questa materia, proprio perché la maggiore apertura da parte dell'ordinamento giuridico nel non richiedere autorizzazioni specifiche con riguardo agli strumenti di lavoro, deve trovare adeguata garanzia nell'adozione di buone pratiche di gestione delle informazioni che possono essere raccolte dagli strumenti di lavoro. Legittimando, di conseguenza, i **controlli difensivi solo** se il rispetto di tali presupposti riceve **adeguata garanzia**, anche in termini di **comportamenti responsabili** supportati da **adeguata informativa** e dal **rispetto delle policy e dei regolamenti interni** che vanno costantemente monitorati.

Su questo fronte, le **esigenze di tutela della privacy** hanno di fatto guidato il nuovo comma 3 dell'art 4 dello Statuto. Si fa riferimento al richiamo espresso, oggi contenuto nella norma, agli **obblighi di corretta informazione** al **lavoratore** in ordine ai **rischi del controllo** derivanti dall'uso degli strumenti di lavoro, che acquista particolare rilevanza sul piano organizzativo e quale presupposto generale per la gestione e manutenzione dei regolamenti interni, anche ai fini dell'esercizio del potere disciplinare.

La norma dell'art. 4 nel testo novellato afferma infatti che "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 d.lgs. 30 giugno 2003, n. 196".

Ed è su questo aspetto che **sta intervenendo** in modo consistente l'**ultima giurisprudenza**.

Si afferma, infatti, soprattutto con riguardo ai **controlli "difensivi" sulla posta elettronica** (che è - ricordiamolo - principalmente uno strumento di lavoro concesso talvolta in uso anche per fini privati ai dipendenti), che le **indagini** del **datore di lavoro** - pure in assenza di informativa al diretto interessato - possono **riguardare solo** le **informazioni temporalmente successive** al momento in cui sia **insorto** un "**fondato sospetto**" circa la **commissione di un illecito**.

Sulla base di tale orientamento, non sarebbero ammessi da parte delle aziende i controlli difensivi e sarebbero, quindi, inutilizzabili a fini disciplinari, le informazioni acquisite (senza adeguata informativa al lavoratore) sulla base di indagini tecnologiche svolte relativamente a periodi antecedenti l'insorgenza del sospetto (cfr. da ultima Cass. civ., Sez. lav., 13 gennaio 2025, n. 807).

Come a dire, in altre parole, che **solo l'insorgenza di un sospetto** circa la **commissione futura di un illecito** a **danno dell'azienda** (e quindi anche in un'ottica preventiva del potenziale illecito). **giustificherebbe** la compromissione della **sfera privata del lavoratore**, autorizzandone la lettura della casella di posta elettronica a propria insaputa.

Ma il punto è proprio questo: proprio perché si tratta di strumenti di lavoro in relazione ai quali il **datore di lavoro** è **legittimato a monitorare** la **correttezza del loro uso** (purché tale circostanza sia stata portata a conoscenza del lavoratore con dettagliata ed **esaustiva informativa** nonché attraverso il costante monitoraggio dei regolamenti interni – cfr. il mio Editoriale "Conservazione delle e-mail aziendali. E' necessaria un'adeguata informativa per evitare sanzioni"), quando vi è **certezza (e non il solo sospetto)** della **commissione di un illecito** (per esempio la certezza dell'avvenuta fuga di notizie verso un competitor ormai già realizzatasi), l'**indagine** circa l'identificazione del **dipendente infedele** - ad avviso di chi scrive - ben potrebbe essere **estesa** in ipotesi a **tutta la casella di posta elettronica** e, di conseguenza, anche alle **e-mail** ed alle informazioni **antecedenti** al momento in cui l'azienda sia venuta a conoscenza dell'illecito.

E ciò in quanto **non si gravita** più nell'ambito del **semplice "fondato sospetto"** circa la **commissione futura** di **un illecito** (che rende lecito il controllo della posta da lì in avanti), ma ci si trova nell'ambito di una **indagine necessaria** a dare conto del fatto che un **illecito è stato effettivamente commesso** e, soprattutto, che lo strumento di lavoro sia stato utilizzato da un dipendente infedele per finalità estranee all'attività lavorativa ed in **violazione** degli **obblighi di diligenza, fedeltà e non concorrenza** di cui agli artt. 2104 e 2105 c.c.

Negarne la possibilità costituirebbe per le aziende una ingiustificata limitazione della legittima facoltà di controllo, finalizzata a prevenire la reiterazione degli illeciti allorché commessi.