ATTUALITÀ

Controllo dei lavoratori online: la posizione del Garante

di **Fondazione AIDR** · 6 luglio 2021, 19:21

di Federica De Stefani, avvocato e responsabile Aidr Regione Lombardia

Il Garante della protezione dei dati personali sanziona Il Comune di Bolzano per aver monitorato la navigazione internet dei lavoratori in modo indiscriminato.

La vicenda prende le mosse da un procedimento disciplinare a carico di un dipendente al quale veniva contestata la consultazione di Facebook e YouTube durante l'orario di lavoro.

L'Autorità, nel proprio provvedimento, sottolinea alcuni importanti elementi che riguardano non solo il trattamento dei dati, ma anche il modus operandi del Comune, prima e durante il procedimento ispettivo.

Il caso

Dagli accertamenti effettuati dal Garante a seguito del reclamo presentato da un dipendente al quale veniva contestato il collegamento "*con il computer del Comune, per oltre 40 minuti a facebook e per oltre 3 ore a youtube, per seguire attività non istituzionali e che [...] aveva consultato pagine Internet non inerenti il suo lavoro*" è emersa un'attività di monitoraggio e filtraggio della navigazione internet dei dipendenti effettuata dal Comune.

I dati così raccolti venivano poi conservati per un mese e veniva creata apposita reportistica per finalità di sicurezza della rete.

L'analisi della vicenda e delle modalità concrete con le quali il Comune aveva realizzato questo monitoraggio, tra l'altro per un periodo di tempo piuttosto esteso (una decina d'anni circa), ha fatto emergere alcuni importanti aspetti.

1- Mancanza di un'adeguata informativa

Il trattamento effettuato dal Comune è avvenuto in assenza di un'adeguata e specifica informativa ai dipendenti in merito ai possibili controlli sugli accessi a Internet da parte del datore di lavoro.

il sistema adottato dal Comune per finalità di sicurezza della rete, nella configurazione originaria, consentiva operazioni di filtraggio e tracciatura delle connessioni e dei collegamenti ai siti Internet esterni, la memorizzazione di tali dati e la loro conservazione, per trenta giorni, nonché l'estrazione di report, anche su base individuale.

Questo sistema ha consentito l'individuazione diretta del lavoratore e della sua postazione di lavoro e ha dato origine a una raccolta sistematica di dati relativi all'attività e all'utilizzo dei servizi di rete da parte di dipendenti direttamente identificabili.

Il Comune non aveva i fornito ai dipendenti alcuna specifica informativa relativa ai trattamenti dei dati personali né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi.

In altri documenti, messi a disposizione dell'Autorità e analizzati nel corso dell'istruttoria, era presente il riferimento alle operazioni di tracciamento delle connessioni a Internet, ma essendo i documenti redatti per assolvere a obblighi diversi, non contenevano tutti gli elementi informativi essenziali richiesti dall'art. 13 del Regolamento e non potevano pertanto sostituire l'informativa che il titolare deve rendere, prima di iniziare il trattamento, agli interessati.

2 – Principio di minimizzazione

In base al Regolamento, il trattamento deve essere "necessario" rispetto alla lecita finalità perseguita (art. 6, par. 1 del Regolamento) e avere ad oggetto i soli dati "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c), del Regolamento).

A tal riguardo il Garante sottolinea che l'ambito dei controlli (indiretti o preterintenzionali), sebbene effettuati nel rispetto delle normative di settore, non possono essere effettuati in via massiva e devono, in ogni caso, essere effettuati previo esperimento di misure meno limitative dei diritti dei lavoratori.

L'Autorità, rimarcando il labile confine esistente tra ambito lavorativo e professionale e quello strettamente privato, ribadisce inoltre la necessità di proteggere e garantire le aspettative di riservatezza del lavoratore sul luogo di lavoro anche nell'ipotesi in cui il dipendente sia connesso ai servizi di rete messi a disposizione del datore di lavoro o utilizzi una risorsa aziendale anche attraverso dispositivi personali.

Nel caso analizzato, al contrario, è emerso che le modalità concrete con le quali erano effettuati i controlli non rispettavano i principi di necessità e proporzionalità, rispetto alla finalità di protezione e sicurezza della rete interna invocata dall'Ente.

Il sistema utilizzato dal Comune, infatti, "*effettuando una raccolta sistematica dei dati di navigazione dei dipendenti comportava inevitabilmente il trattamento di informazioni anche estranee all'attività professionale, desumibili dagli URL visitati, e risultava, pertanto, in contrasto con il divieto per il datore di lavoro di trattare dati "non attinenti alla valutazione dell'attitudine professionale del lavoratore" e dunque con l'art. 113 del Codice, in riferimento all'art. 8 della l. 20 maggio 1970, n. 300 e all'art. 10 del d.lgs. 10 settembre 2003, n. 276*" (così testualmente l'ordinanza del 13 maggio 2021).

L'esigenza di ridurre il rischio di usi impropri della navigazione in Internet, da parte dei dipendenti, consistenti in attività non correlate alla prestazione lavorativa (ad esempio, la visione di siti web non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa) non può, infatti, giustificare ogni forma di interferenza nella vita privata, ma può essere soddisfatta mediante la predisposizione di misure tecniche e organizzative idonee a prevenire che eventuali informazioni relative alla sfera extralavorativa vengano raccolte, dando luogo a trattamenti di informazioni personali, "non pertinenti" che ricadono nell'ambito di applicazione dell'art. 113 del Codice

3- Limitazione della finalità

Il Regolamento prevede, all'art. 5, che "i dati devono essere "raccolti per finalità determinate, esplicite legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità".

Nel caso analizzato dal Garante questo principio non è stato rispettato, posto che i dati relativi alla navigazione web dei dipendenti, originariamente raccolti e trattati in modo non proporzionato e non conforme alla disciplina in materia di protezione dei dati personali, , e senza un'adeguata informativa ai sensi dell'art. 13 del Regolamento, sono stati successivamente impiegati per contestare addebiti disciplinari.

Per l'Autorità prive di pregio si sono rivelate anche le indicazioni fornite dal Comune in merito all'archiviazione del procedimento disciplinare.

Quest'ultimo, infatti, non aveva comportato l'irrogazione di sanzioni in quanto i dati raccolti non erano attendibili, riportando anche una serie di siti (es. collegati a banner) che non erano stati necessariamente visitati dal lavoratore, senza possibilità di distinzione tra il sito effettivamente visitato e quelli a navigazione indiretta/involontaria.

La circostanza relativa alla scarsa qualità dei dati raccolti non rileva ai fini della valutazione del rispetto del Regolamento, in quanto i dati raccolti sono stati comunque oggetto di trattamento, in quanto utilizzati per avviare il predetto procedimento disciplinare.

L'autorità Garante, infine, rileva la mancanza di una valutazione d'impatto effettuata dal Comune e la inidoneità del nuovo accordo sindacale stipulato per il trattamento dei dati personali dei dipendenti.

Per le violazioni riscontrate e in considerazione dell'atteggiamento collaborativo e propositivo del Comune, la sanzione amministrativa irrogata è stata quantificata in 83.000 €.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/07/06/controllo-dei-lavoratori-online-la-posizione-del-garante/

© 2026 Istituzioni24