GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

I lavoratori devono essere informati. Il datore di lavoro non può spiare le mail

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali

("L'Huffington Post", 13 gennaio 2016)

Ma davvero, da oggi, i lavoratori europei potranno essere spiati dai loro datori di lavoro? La sentenza del 12 dicembre della Corte europea dei diritti umani sancisce la fine della privacy in ambito lavorativo? È bene chiarirlo: assolutamente no.

La sentenza di ieri decide il ricorso di un ingegnere romeno licenziato per inadempimento contrattuale, provato anche dall'utilizzo per fini personali, in orario di lavoro, della mail aziendale. Con la pronuncia, la Corte si è limitata a ritenere non irragionevole il bilanciamento tra privacy dei dipendenti ed esigenze datoriali, affermato dalla giurisdizione romena. E questo perché: a) l'azienda aveva informato i dipendenti delle condizioni d'uso della mail aziendale, che non ne consentivano l'utilizzo per fini personali. Ragione, questa, che avrebbe quindi ridotto l'aspettativa di riservatezza riposta dai lavoratori rispetto alle loro comunicazioni via e-mail; b) il monitoraggio delle mail è stato limitato nel tempo e nell'oggetto, nonché strettamente proporzionato allo scopo di provare l'inadempimento contrattuale del lavoratore (desunto da altri elementi), la cui scarsa produttività aveva determinato e legittimato il licenziamento; c) l'accesso alle e-mail del lavoratore da parte datoriale è stato legittimo proprio perché fondato sul presupposto della natura professionale del contenuto delle comunicazioni (come da contratto avrebbe dovuto essere); d) l'identità degli interlocutori del lavoratore non è stata rivelata in sede giurisdizionale; e) l'azienda non ha avuto accesso ad altri documenti archiviati sul computer del lavoratore; il contenuto delle comunicazioni non è stato oggetto di sindacato da parte datoriale nel giudizio, ma soltanto il carattere personale delle mail inviate nell'orario di lavoro, con conseguente riduzione della produttività del dipendente; f) il dipendente non ha motivato la ragione dell'utilizzo della mail aziendale per fini personali.

La Corte ha dunque riaffermato, nel caso concreto, che i controlli datoriali sull'attività lavorativa sono ammissibili soltanto nella misura in cui siano strettamente proporzionati e non eccedenti lo scopo di verifica dell'adempimento contrattuale. Essi devono essere inoltre limitati nel tempo e nell'oggetto; mirati (dunque non massivi) e fondati su presupposti (quali in particolare l'inefficienza dell'attività lavorativa del dipendente) tali da legittimarne l'esecuzione. Infine, devono essere già previsti dalla policy aziendale, di cui il dipendente deve essere adeguatamente edotto.

Questa valutazione è in linea con la Raccomandazione sulla protezione dei dati in ambito lavorativo, approvata il 1° aprile scorso dallo stesso Consiglio d'Europa, che in particolare auspica la minimizzazione dei controlli difensivi o comunque rivolti agli strumenti elettronici; l'assoluta residualità dei monitoraggi, con appositi sistemi informativi, sull'attività e il comportamento dei lavoratori in quanto tale. Ed è in linea con la giurisprudenza italiana e con gli stessi principi affermati dal Garante, in particolare con le Linee guida del 2007. Con questo provvedimento si è prescritto al datore di lavoro di informare i lavoratori delle condizioni di utilizzo della mail aziendale (e anche della stessa rete, in orario di lavoro o comunque con gli strumenti messi a disposizione dal datore), dei controlli che il datore di lavoro si riserva di effettuare per fini legittimi, nonché delle eventuali conseguenze disciplinari suscettibili di derivare dalla violazione di tali regole.

Principi che restano validi anche dopo la riforma dei controlli datoriali operata dal Jobs Act e anche rispetto agli strumenti di lavoro che, pur sottratti alla procedura concertativa, restano comunque soggetti alla disciplina del Codice privacy. E, in particolare, ai principi di necessità, finalità, legittimità e correttezza, proporzionalità e non eccedenza del trattamento, nonché all'obbligo di previa informativa del lavoratore e al divieto di profilazione, ribaditi proprio dalla Corte europea dei diritti umani, con la sentenza di ieri.

Come abbiamo avuto modo di affermare in sede di audizione, dinanzi alle Commissioni parlamentari, sullo schema di decreto legislativo attuativo del Jobs Act in questa materia, sarà proprio il rispetto dei principi del Codice privacy il principale argine a un utilizzo pervasivo dei controlli sul lavoro. E questo, anche in assenza delle modifiche che le Commissioni parlamentari, in conformità alle indicazioni da noi rese in audizione, avevano suggerito al Governo di apportare al testo del decreto per rafforzare le garanzie dei lavoratori, pur nel rispetto delle legittime esigenze datoriali.

Dunque, anche dopo il Jobs Act, i controlli datoriali devono comunque essere improntati a gradualità nell'ampiezza e nella tipologia con assoluta residualità dei controlli più invasivi, legittimati solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori. E così, ad esempio, ove il datore di lavoro riscontrasse la presenza di virus sui pc aziendali, dovrebbe dotarli di sistemi di filtraggio/blocco dei siti a rischio e non procedere al monitoraggio dei siti visitati. Del resto, come il Garante ha affermato in più occasioni, il datore di lavoro è tenuto all'individuazione preventiva della lista dei siti considerati correlati alla prestazione lavorativa, nonché dell'adozione di filtri per il blocco dell'accesso a determinati siti o del download di alcuni file. E non sono comunque consentite al datore di lavoro la lettura e registrazione sistematica delle e-mail e delle pagine web visualizzate dal lavoratore, la lettura e registrazione dei caratteri inseriti tramite tastiere e dispositivi analoghi, nonché l'analisi occulta di computer portatili affidati in uso.

In questa prospettiva, assai utile può essere l'adozione di una soluzione di privacy-by-design, ovvero la progettazione degli stessi strumenti mediante i quali effettuare i controlli in modo da minimizzare, fino ad escludere, il rischio di controlli invasivi o comunque di incisive limitazioni della riservatezza di chi a quei controlli possa essere sottoposto. Ed è significativo che tali soluzioni siano valorizzate dal nuovo Regolamento Ue sulla protezione dati, che delinea il nuovo quadro giuridico europeo in una materia, come questa, su cui si giocano le sfide più importanti per le nostre democrazie.