7. POSTA ELETTRONICA AZIENDALE E CONTROLLI SUI LAVORATORI - I LIMITI DEL GARANTE PRIVACY

Il Garante per la protezione dei dati personali, con provvedimento n. 476 del 18 giugno 2026, è intervenuto in materia di trattamento dei dati relativi alla posta elettronica aziendale, soffermandosi, in particolare, sui limiti alla conservazione dei messaggi e dei relativi log e sull'utilizzo di tali informazioni per finalità di controllo dei lavoratori.

Il provvedimento trae origine dai reclami presentati da due ex dipendenti, in relazione all'accesso da parte del datore di lavoro alla corrispondenza transitata sui rispettivi account aziendali e al successivo utilizzo di alcuni messaggi nell'ambito di procedimenti disciplinari. La società aveva qualificato tali verifiche come controlli difensivi, finalizzati ad accertare specifiche condotte illecite.

Nel definire il procedimento, il Garante ha ribadito alcuni principi di carattere generale applicabili alla gestione della posta elettronica nel rapporto di lavoro. In particolare, il contenuto dei messaggi e i dati esteriori delle comunicazioni, compresi i log, costituiscono informazioni rispetto alle quali sussiste una legittima aspettativa di riservatezza anche nel contesto lavorativo. La circostanza che la posta elettronica costituisca uno strumento utilizzato per lo svolgimento della prestazione non determina, quindi, il venir meno delle garanzie previste dalla disciplina sulla protezione dei dati personali.

Particolare rilievo assume il principio di limitazione della conservazione. Il datore di lavoro deve individuare tempi di conservazione dei messaggi e dei log proporzionati alle specifiche finalità perseguite, nel rispetto dei principi di necessità, minimizzazione e proporzionalità. La raccolta e la conservazione sistematica della posta elettronica per periodi particolarmente estesi, in assenza di finalità preventivamente individuate e di un idoneo presupposto di liceità, risultano incompatibili con i principi stabiliti dagli artt. 5 e 6, Regolamento (UE) 2016/679.

Il Garante ha, inoltre, richiamato i limiti relativi ai c.d. controlli difensivi. Secondo l'orientamento giurisprudenziale richiamato nel provvedimento, i controlli tecnologici finalizzati alla tutela del patrimonio aziendale o all'accertamento di condotte illecite possono essere effettuati, in presenza di un fondato sospetto, assicurando un adeguato bilanciamento tra gli interessi aziendali e la dignità e riservatezza del lavoratore. Il controllo deve, tuttavia, riguardare dati acquisiti successivamente all'insorgere del sospetto: nel caso esaminato, invece, la ricerca aveva interessato comunicazioni risalenti anche a circa 2 anni prima.

La conservazione sistematica di e-mail e log può, inoltre, consentire la ricostruzione dell'attività svolta dai dipendenti e assumere rilievo ai fini della disciplina sui controlli a distanza. Il trattamento deve, pertanto, rispettare anche le garanzie previste dall'art. 4, Legge n. 300/1970, richiamato dall'art. 114, Codice privacy, qualora dagli strumenti utilizzati derivi la possibilità di controllo a distanza dell'attività lavorativa.

Con riferimento alla cessazione del rapporto, l'Autorità ha ricordato che il datore di lavoro deve procedere alla disattivazione e successiva rimozione dell'account individualizzato, adottando sistemi automatici che informino i mittenti della cessazione dell'account e

forniscano eventuali indirizzi alternativi, impedendo nel contempo la visualizzazione dei messaggi in arrivo.

Il provvedimento richiama, inoltre, l'obbligo di fornire ai lavoratori un'informativa preventiva e trasparente, nella quale siano adeguatamente rappresentate le caratteristiche essenziali dei trattamenti effettuati, comprese le finalità e i criteri relativi alla conservazione della posta elettronica e dei log.

Alla luce delle violazioni riscontrate, il Garante ha dichiarato illecito il trattamento effettuato, rilevando la violazione degli artt. 5, par. 1, lett. a), b), c) ed e), 6, 12, 13, 17 e 88, Regolamento (UE) 2016/679 e dell'art. 114, Codice privacy. L'Autorità ha, quindi, disposto il divieto di accesso al contenuto dei dati raccolti e conservati sui sistemi aziendali relativi alla posta elettronica e ha applicato alla società una sanzione amministrativa pecuniaria pari a 460.000 euro, determinata tenendo conto, tra gli altri elementi, della natura e gravità delle violazioni, della durata della conservazione dei dati, delle condizioni economiche della società e delle misure successivamente adottate per porre rimedio alle criticità riscontrate. È stata, inoltre, disposta la pubblicazione dell'ordinanza ingiunzione sul sito del Garante.