

Gestione informatica, privacy e diritti: serve chiarezza.



Nazionale, 02/02/2026

L'inchiesta trasmessa dalla trasmissione Report il 25 gennaio 2026 ha acceso i riflettori sull'installazione del software informatico ECM su circa 40.000 computer del Ministero della Giustizia. Una notizia che non può lasciare indifferenti e che pone interrogativi legittimi anche rispetto a quanto avviene all'interno degli Uffici centrali e periferici di questa Amministrazione.

Dall'inchiesta emerge che ECM è un software commerciale di Microsoft, utilizzato per la gestione centralizzata dei sistemi informatici e per il controllo remoto dei dispositivi.

Non si tratta di un virus né di un trojan, ma lo stesso produttore evidenzia come il suo utilizzo richieda attenzione, cautele e misure di sicurezza adeguate, soprattutto quando viene impiegato in contesti che trattano dati estremamente delicati e che, potenzialmente, possono incidere anche sulle modalità di svolgimento dell'attività lavorativa.

Ogni giorno il Ministero dell'Interno gestisce una quantità enorme di informazioni riservate su qualsiasi persona, siano esse cittadini o comunitari, non comunitari, turisti, titolari o beneficiari di istanze, oltre che dati legati all'attività lavorativa di migliaia di dipendenti civili non dirigenti. In presenza di strumenti che consentono la gestione e il controllo remoto, diventa quindi fondamentale chiarire se e in che modo vengano monitorate, anche indirettamente, le attività lavorative quotidiane del personale civile, anche in considerazione

della molteplicità dei servizi affidati a personale informatico esterno non ancora stabilizzato o inserito in progetti di stabilizzazione.

Richiamando l'art. 4 della Legge 300/1970, il cui comma 1 prevede il divieto di controllo a distanza dei lavoratori e il Regolamento UE 679/2016 - Codice della Privacy, è importante fare chiarezza per sapere:

- se il software ECM, o strumenti simili di gestione e controllo remoto, siano presenti sui sistemi informatici dell'Amministrazione, considerando tutte le articolazioni, non solamente il Dpp;
- quali misure di sicurezza siano adottate e quale livello di tutela della privacy venga concretamente garantito ai lavoratori;
- se tali strumenti rispettino pienamente la normativa vigente, in particolare il Regolamento UE 2016/679 (GDPR), le indicazioni del Garante per la protezione dei dati personali e la normativa a tutela dei lavoratori; • se siano stati effettuati controlli, audit o valutazioni di impatto sull'utilizzo di questi software.

USB PI – Coordinamento Nazionale Ministero Interno