Nel furto di dati personali il dipendente in smart working non è l'unico responsabile

Giovedì 9 Settembre 2021

Il Tribunale amministrativo provinciale di Varsavia ha confermato con sentenza del 13 maggio scorso il provvedimento del Garante polacco e la sanzione di circa 11mila euro irrogata a un ateneo locale, per **non aver adottato misure tecniche e organizzative sufficienti a prevenire l'esposizione di un ingente quantitativo di dati personali di studenti**.

Se infatti, l'università aveva attribuito la colpa al dipendente in smart working, il quale, oltre a subire il furto del proprio notebook, aveva conservato i dati personali poi diffusi oltre il periodo massimo di tre mesi stabilito per il trattamento e la conservazione, **il tribunale ha tuttavia ritenuto sussistere la responsabilità dell'ateneo in quanto titolare del trattamento**. Il dipendente avrebbe infatti operato svolgendo le proprie mansioni nell'alveo degli scopi e delle modalità di trattamento definite dall'istituzione: **le sue azioni (e negligenze) sono state dai giudici considerate imputabili al datore di lavoro, che ne è quindi stato ritenuto responsabile, anche se colposamente**.

La vicenda polacca pone sotto i riflettori, ancora una volta, il problema della protezione di dati presenti sul computer personale del dipendente. Il datore di lavoro che autorizzi la resa di prestazione lavorative a distanza e mediante digital device privati dovrà indubbiamente tenere in conto il rischio insito in tali operazioni, approntandone l'adeguata analisi e valutazione richiesta dall'articolo 32 del GDPR. Seguirà la predisposizione di misure tecniche e organizzative di protezione dei dati personali, in particolare dal rischio di esportazione non autorizzata o intenzionale sottrazione degli stessi, ma non solo.

L'utilizzo di dispositivi mobili in uso ai dipendenti, fenomeno conosciuto sotto l'acronimo BYOD, cioè "*Bring your own device*" (in italiano "Portare il proprio dispositivo"), richiede un livello di approfondimento e dettaglio superiore, completo di prescrizioni vincolanti per i lavoratori (e controllo nei limiti di legge) affinché siano adottate tutte le cautele necessarie, comprese stringenti discipline di memorizzazione e di archiviazione dei dati personali.

Ecco dunque l'obbligo di scrivere una BIA, cioè "*Byod Impact Assessment*", un documento ormai imprescindibile nella normativa privacy applicabile a imprese, scuole e pubbliche amministrazioni.