SMART WORKING E GDPR
LA RESPONSABILITÀ DEL DATORE DI LAVORO

Il datore di lavoro è considerato responsabile nel caso di furto di dati aziendali dal PC personale del dipendente che non è e non agisce come soggetto terzo


di **Paola Gobbi**
e **Silvia Fumagalli**

Fa discutere la decisione del Tribunale Amministrativo di Varsavia del 13 maggio 2021, con cui viene confermato il provvedimento del Garante della Privacy polacco di irrogazione di sanzione amministrativa pecuniaria all'Università di Scienze della Vita di Varsavia perché responsabile del furto di dati personali degli studenti dell'ateneo dal PC privato di un dipendente.

Il caso sottoposto al Garante di Varsavia atteneva al furto di dati aziendali dal pc privato di un dipendente, il quale utilizzava il proprio device per svolgere l'attività lavorativa in smart working e sul quale aveva caricato dati relativi agli studenti dell'Ateneo. Secondo l'Autorità polacca, il datore di lavoro resta responsabile delle condotte del proprio dipendente e, in particolare, del data breach anche se il lavoratore utilizza un PC di sua proprietà perché il lavoratore non può essere considerato un lavoratore autonomo ma opera pur sempre per conto del datore di lavoro e perché ha ritenuto violate plurime disposizioni del GDPR, tra le quali, gli articoli 5, 24 e 32 da parte dell'Università. L'art. 5 stabilisce le regole per il trattamento dei dati personali, che devono essere rispettate dai soggetti che, autonomamente o insieme ad altri, determinano le finalità e le modalità del trattamento di dati personali. In particolare, i dati personali devono essere trattati in modo da garantirne adeguata sicurezza compresa la protezione da trattamenti non autorizzati o illeciti e da perdita, distruzione o danneggiamento accidentali, mediante adeguate misure tecniche o organizzative. Inoltre, i dati personali devono essere conservati in una forma che non consenta l'identificazione dell'interessato se non per il tempo necessario per le finalità per le quali i dati sono trattati. L'art. 24 prescrive che il titolare del trattamento, tenuto conto della natura, dell'ambito, del contesto e delle finalità del trattamento nonché del rischio di violazione di diritti e delle libertà delle persone fisiche, deve attuare misure tecniche e organizzative adeguate a garantire che il trattamento avvenga in conformità al regolamento e che lo possa dimostrare. L'art. 32, infine, dispone che l'amministratore è tenuto ad applicare misure tecniche e organizzative corrispondenti al rischio di violazione dei diritti e delle libertà delle persone fisiche con una diversa probabilità di accadimento e gravità di minaccia. Secondo il Garante polacco, la determinazione delle misure tecniche e organizzative adeguate è un processo in due fasi. In primo luogo, è importante determinare il livello di rischio connesso al trattamento dei dati personali, tenendo conto dei criteri di cui all'art. 32 GDPR e, quindi, occorre determinare quali misure tecniche e organizzative sono idonee a garantire il livello di sicurezza corrispondente a tale rischio. Oltre al rispetto delle suddette disposizioni, che impongono, se necessario, revisioni periodiche delle misure adottate e l'aggiornamento delle garanzie, il datore di lavoro deve verificare che i propri dipendenti osservino le regole adottate in materia di trattamento dei dati personali. Secondo il Garante polacco, proprio in linea con i principi comunitari di privacy by design e accountability, il datore di lavoro, quale titolare del trattamento, non solo deve adottare le misure tecniche e organizzative adeguate per garantire che il trattamento avvenga in conformità al regolamento e che lo possa dimostrare, ma deve altresì monitorare e verificare che le attività svolte dai propri dipendenti siano corrette e conformi a quanto previsto dal regolamento interno: la violazione da parte del lavoratore delle disposizioni assunte per il trattamento dei dati personali non esonera il datore da responsabilità in caso di data breach. Alla luce della decisione in esame e della imperante diffusione (per le note ragioni emergenziali) dello smart working, è quanto mai necessario predisporre procedure e regolamenti idonei a formare e informare i dipendenti sul corretto trattamento dei dati per non incorrere in responsabilità.

Avv.ti Paola Gobbi partner e **Silvia Fumagalli** senior associate
UNIOLEX Stucchi & Partners - www.uniolex.com