# Inadeguata dismissione dei server

Mercredi 4 novembre 2020

Negli Stati Uniti, l'*Office of the Comptroller of the Currency* (OCC) ha annunciato di aver inflitto una sanzione da 60 milioni di dollari a Morgan Stanley, per la **mancata valutazione dei rischi e l'adozione delle misure precauzionali idonee a garantire la sicurezza dei dati della clientela a seguito della disattivazione di *data centers* aziendali**, esponendo così i clienti a violazioni della privacy con **rischio di frodi, furto di identità e messa in vendita delle loro informazioni personali sul *dark web***.

All'inizio dell'anno una *class action* per 5 milioni di dollari era stata intentata su tali basi, sostenendo che Morgan Stanley non fosse riuscita a salvaguardare le informazioni personali identificabili su apparecchiature di sua proprietà precedentemente disattivate. Si sarebbe trattato difatti di **dati non crittografati, quali numeri di previdenza sociale, numeri di passaporto, indirizzi, numeri di telefono, indirizzi e-mail, numeri di conto, date di nascita, reddito e situazione patrimoniale**.

Le pratiche non sicure perseguite dalla banca hanno di conseguenza condotto l'OCC a comminare il 5 ottobre scorso la sanzione record.

Secondo il provvedimento le violazioni si erano articolate in due momenti:

**nel 2016 non avendo esercitato la banca il dovuto controllo sulla cancellazione dei dati e sull'attività della società terza incaricata della dismissione dei *data server*** e

**nel 2019 riscontrando carenze simili nel controllo della gestione dello smantellamento dei dispositivi**.

Palesatasi la possibilità che fossero rimasti registrati alcuni dati dei clienti, **la banca si era limitata a notificare agli interessati i possibili *data breach*, avviando anche tardivamente le attività necessarie per rimediare alle carenze**.

Da non dimenticare che anche in Europa è richiesto il rispetto di particolari obblighi. Il GDPR, piuttosto severo in materia, fa della cancellazione dei dati una componente fondamentale del loro trattamento e impone di procedere alla cancellazione irreversibile dei dati allo scopo di garantirne l'impossibilità di recupero da parte di terzi estranei.

Il Garante per la protezione dei dati personali ha inoltre adottato nel 2008 alcuni suggerimenti pratici pubblicando delle **istruzioni per una cancellazione sicura dei dati**. Vi sono elencate le principali modalità di rimozione, fra le quali appositi software, l'uso di dispositivi di demagnetizzazione (degausser), o la distruzione fisica del supporto.

Il provvedimento dell'OCC.

Le istruzioni pratiche del Garante.