Spesometro: le banche dati della PA ancora a rischio sicurezza.

Mancano ormai poche settimane alla scadenza per l'adempimento della comunicazione dei dati delle fatture attraverso lo **Spesometro -** strumento di controllo fiscale che impone agli operatori finanziari e ai commercianti l'obbligo di comunicare all'Agenzia delle Entrate il codice fiscale di chi effettua acquisti per un importo superiore a una data cifra stabilita per legge - ed i commercialisti denunciano nuove difficoltà nella gestione del sistema. Intanto il Garante della Privacy, a fronte di quanto accaduto, ha inviato una lettera al Presidente del Consiglio per analizzare e mettere in luce le debolezze del sistema stesso.

Il recente incidente (***data breach***) accaduto alla Sogei, società di Information and Communication Technology del Ministero dell'Economia e delle Finanze, in cui sono conservati i dati fiscali di milioni di cittadini, ha messo in luce - come sottolineato nella lettera che il Garante della Privacy ha inviato al presidente del consiglio Paolo Gentiloni - i rischi derivanti dalla gestione dei sistemi informativi, laddove la stessa non sia costantemente accompagnata da un'adeguata attenzione agli aspetti di sicurezza e protezione dei dati personali.

L'Autorità sta facendo i dovuti accertamenti, ma ciò che sta emergendo in questa vicenda, come è stato affermato da Soro è che, "*in un tempo caratterizzato dalla ineludibile necessità di ricorrere sempre più allo scambio telematico dei dati e all'interconnessione delle banche dati pubbliche,* ***mancano spesso un'adeguata consapevolezza e competenze idonee a far fronte all'incremento dei rischi per i diritti e le libertà delle persone coinvolte***."

L'innovazione tecnologica delle pubbliche amministrazioni è molto importante, ma deve inderogabilmente accompagnarsi alla garanzia di tutela dei diritti inalienabili dei cittadini, fra i quali certamente è ricompreso il diritto alla tutela dei propri dati personali. Dunque, risulta fondamentale per i soggetti pubblici onde evitare fenomeni di **data breaches:**

- La costante attenzione nella gestione dei sistemi informativi;
- L'impegno nella osservanza degli obblighi di sicurezza e di qualità dei dati;
- Il rispetto dei principi di riservatezza ed integrità.

Il riferimento al nuovo **GDPR** (*General Data Protection Regulation -* ***Regolamento UE 2016/679****)* è chiaro ed Antonello Soro ha spiegato chiaramente che *"a decorrere dal maggio prossimo le amministrazioni dovranno adeguarsi agli standard di sicurezza previsti dal* ***Regolamento generale per la protezione dei dati personali****, basato, tra l'altro, sull'accresciuta responsabilizzazione dei titolari del trattamento e sull'idea della prevenzione del rischio e della protezione dei dati a partire dalla stessa configurazione dei sistemi. In vista di questo obiettivo e alla luce delle richiamate preoccupazioni, appare inderogabile una forte iniziativa, da parte delle diverse istituzioni coinvolte nei processi decisionali relativi all'innovazione tecnologica del Paese, per una verifica puntuale dello stato di sicurezza delle banche dati pubbliche e dei processi in corso di attuazione dell'Agenda digitale".*

Soltanto un grande investimento nella materia di protezione dei dati, infatti, come ribadito da Soro nella parte finale della lettera, renderà possibile la garanzia che tali trasformazioni tecnologiche si svolgano nel pieno rispetto dei diritti dei cittadini e senza esporre in alcun modo a pregiudizio la stessa sicurezza del Paese.

[Fonti: Garante Privacy; Il Sole 24 Ore]