Cyber security: l'esperienza del SII

L'esperienza fatta nel Sistema Informativo Integrato è sicuramente uno spunto utile quando si parla di sicurezza dei dati. Per darvi un'idea della complessità, il SII gestisce 60 milioni di clienti, per circa 100 milioni di flussi l'anno. Da sempre Acquirente Unico ha considerato come prioritario l'obiettivo di assicurare la massima sicurezza nella gestione e nello scambio dei dati trattati dal SII, tutelando la privacy e la riservatezza dei clienti finali.

Nel realizzare la piattaforma SII, particolare attenzione è stata rivolta alla sicurezza e alla tracciabilità delle informazioni. Gli aggiornamenti in termini di cyber security sono continui, il sistema è blindato e viene sottoposto a ripetuti test di sicurezza. E' garantita la certezza dei dati scambiati che non possono essere alterati nel tempo; ciascun flusso di dati scambiato con gli operatori è "sigillato informaticamente". E' garantita anche la tracciabilità dei processi: si ha sempre l'identificazione dell'utente che ha generato una informazione e del momento in cui è stata immessa nel sistema, in modo da poter risalire alla catena di responsabilità.

Il SII ha un futuro promettente davanti a sé: potrà infatti diventare una grande piattaforma capace di garantire servizi non solo per gli operatori ma anche per le istituzioni e soprattutto per la domanda, e anche in ambiti diversi. Per il rilevante patrimonio informativo e per i flussi che gestisce e gestirà la piattaforma del SII è, a tutti gli effetti, un asset strategico del Paese. Un'infrastruttura di questa rilevanza, i cui flussi sono destinati a moltiplicarsi, deve basarsi su un aggiornamento costante di sistemi di sicurezza del massimo livello, per ridurre il rischio informatico.

Il lavoro dei singoli, però, non è sufficiente: penso a un qualche tipo di task force sulla cyber security del settore che coinvolga tutti i soggetti interessati: mi riferisco non solo agli operatori, i distributori, ma anche a Terna e alle PA che gestiscono banche dati. Contestualmente, l'intervento di un soggetto pubblico, come il Nucleo per la sicurezza cibernetica, potrebbe coordinare questo lavoro collaborativo e trasformarne gli esiti, ove necessario, in indicazioni a vantaggio di tutti. Potremmo dare un notevole contributo non solo alla sicurezza nazionale, ma anche alle competenze del nostro tessuto industriale e di ricerca, trasformando un obbligo impostoci da una pressione interna nell'opportunità di creare ulteriore sviluppo.