INFORMAZIONI CIOFS E CNOS/SCUOLA
3/2020
A cura di d. Bruno Bordignon

42/20 Trattamento di dati personali e cloud computing nella scuola pubblica: criticità, responsabilità, sicurezza
(orizzontescuola.it - di *Avv. Bruno Cantarone)*

Con la frase idiomatica "no silver bullet" nel 1986 Frederick Brooks negò l'esistenza in ambito informatico di un magico rimedio che risolve ogni problema, come il proiettile d'argento che, nel folclore anglosassone, è l'unico modo per uccidere i licantropi.
La stessa affermazione negativa, allora riferita alla difficile gestione del software e del suo sviluppo, potrebbe oggi riguardare il *cloud computing*,al quale molti settori della Pubblica Amministrazione, compreso quello scolastico, fanno sempre maggiore ricorso.
Si tratta, in sostanza, di una modalità di erogazione di servizi offerti *on demand* da un fornitore ad un cliente finale attraverso la rete internet, a partire da un insieme di risorse preesistenti, configurabili e disponibili in remoto, che di fatto si risolve (per l'utente) nella virtualizzazione di hardware e software.
Non una nuova tecnologia quindi, semmai un nuovo modo di erogare o di utilizzare servizi (a seconda che il fenomeno lo si veda dal lato del fornitore o dal lato del cliente), che trova nella scuola pubblica numerose applicazioni, si pensi, ad esempio, al Registro elettronico, alla Segreteria digitale, eccetera, e che presenta innumerevoli ed evidenti vantaggi, tali da farlo apparire - a prima vista - come il proiettile d'argento della tradizione popolare d'oltreoceano: dati sempre consultabili da qualunque luogo, completi e disponibili in formati standardizzati; accessi alle informazioni verificabili e tracciabili; automatizzazione di taluni adempimenti; razionalizzazione delle risorse; maggiore efficienza e riduzione di costi per la Pubblica Amministrazione, e così via.
In concreto, il *cloud computing* può assumere diverse configurazioni a seconda del tipo di servizio offerto e del tipo di utente: IaaS (*Infrastructure as a service*); PaaS (*Platform as a Service*); SaaS (*Software-as-a-Service*).
Nel primo caso (**IaaS**) il fornitore mette a disposizione risorse hardware virtualizzate, ad esempio server virtuali remoti, che il cliente utilizza "a consumo" per creare e gestire la propria infrastruttura sul *cloud*, senza preoccuparsi di dove siano allocate le risorse (spesso in aree geografiche diverse). In pratica l'utente (tipicamente: amministratori di sistemi, sistemisti, ecc.) esternalizza l'infrastruttura IT delegando al fornitore la gestione dell'hardware e le attività per garantire l'accessibilità ai servizi, compresi il monitoraggio sulla sicurezza, l'esecuzione degli aggiornamenti tecnologici e via dicendo.
Attraverso un servizio **PaaS** viene invece messa a disposizione una piattaforma dotata di tutti gli strumenti per ospitare un software, permettendo all'utente (*software house*, *web agency*, ecc.) di sviluppare, sottoporre a test, implementare e gestire le applicazioni aziendali senza i costi e la complessità associati all'acquisto, alla configurazione, all'ottimizzazione e alla gestione dell'hardware e del software di base.
Il modello di *cloud computing* più utilizzato anche dalle istituzioni scolastiche pubbliche è quello **SaaS**, nel quale un software - sviluppato e gestito dal suo produttore - viene messo a disposizione degli utenti (sia *consumer* che *business*) via web attraverso un *login*.
Gli esempi di soluzioni SaaS normalmente adottate in ambito scolastico sono numerosi: si pensi banalmente a Dropbox, Google Drive, OneDrive e simili, spesso usati dai docenti per memorizzare e condividere dati (documenti, immagini, calendari, ecc.), ma ancor di più ai servizi web ed ai software gestionali specifici per le segreterie, apprestati da fornitori specializzati ben noti ad ogni Dirigente Scolastico o DSGA ed al personale amministrativo, allocati su server proprietari o di terzi, accessibili via internet e funzionali agli usi più disparati, come la gestione dei documenti

informatici, dei fascicoli elettronici, del protocollo, la dematerializzazione, la conservazione *cloud* dei dati, la gestione della contabilità, degli stipendi, eccetera.
Alla crescente e capillare diffusione di simili soluzioni in ogni ambito della P.A., comprese appunto le segreterie scolastiche, spesso però non si accompagna da parte degli operatori la piena consapevolezza sia del ruolo che il fornitore del servizio assume in ordine alla protezione dei dati che gli vengono affidati (un ruolo che non sempre viene formalizzato e disciplinato con la nomina a Responsabile del trattamento, ai sensi dell'art. 28 del GDPR), sia dei gravi rischi che fanno da contraltare agli innegabili pregi del *cloud computing*, perché - è bene ribadirlo - il proiettile d'argento non esiste.
Le potenziali **criticità** del trattamento di dati personali effettuato utilizzando in ambito scolastico soluzioni di *cloud computing*, ad esempio SaaS, sono infatti molteplici. Queste le principali:

- perdita, da parte del titolare del trattamento, del controllo esclusivo e diretto sui dati personali che vengono comunicati al fornitore (dal momento in cui le informazioni migrano dal computer locale del titolare verso i sistemi remoti del fornitore del servizio, la tutela della riservatezza, della integrità e della disponibilità dei dati dipenderà anche dai corrispondenti profili di sicurezza che quest'ultimo adotterà, lasciando spesso il primo nella impossibilità di conoscere con assoluta certezza l'esatta ubicazione dei propri dati sulla "nuvola" o se e quando essi verranno spostati da un luogo ad un altro per esigenze tecniche o economiche del fornitore);
- responsabilità in capo al titolare del trattamento per i danni (imputabili al fornitore) eventualmente provocati agli interessati in conseguenza di guasti o malfunzionamenti del software (o della piattaforma, o della infrastruttura) che determinino la perdita dei dati o ne impediscano l'accessibilità (quanti Dirigenti Scolastici sanno, ad esempio, che il servizio "acquistato" dal *provider*, di fatto, non è altro che il risultato di una catena di trasformazione di servizi forniti, in una filiera tecnologica complessa, da altri *service provider*?);
- uso di software (o tecnologia) *closed source* da parte del fornitore del servizio, che non garantisce la portabilità e l'interoperabilità dei dati trattati e pertanto impedisce o limita il passaggio ad altro fornitore.

A fronte di tali criticità l'Agenzia per l'Italia Digitale (AgID) ha delineato un percorso di qualificazione per i soggetti pubblici e privati che intendono fornire infrastrutture e servizi *cloud* alla Pubblica Amministrazione, proprio affinché queste ultime possano adottare servizi e infrastrutture di *cloud computing* omogenei e, soprattutto, che rispettino elevati standard di sicurezza, efficienza ed affidabilità, in linea con le previsioni delle circolari AgID n. 2 e n. 3 del 9 aprile 2018.
A decorrere dal 1 aprile 2019 tutte le PP.AA. possono acquisire esclusivamente i servizi IaaS, PaaS e SaaS qualificati dalla stessa Agenzia per l'Italia Digitale e pubblicati nel *Cloud Marketplace* AgID.
Questo annulla tutti i rischi? No di certo!
Come ha autorevolmente riconosciuto il nostro Garante per la protezione dei dati personali "il *cloud computing* non è un fenomeno temporaneo o una moda, ma il passo successivo dell'evoluzione del modo in cui si utilizza la Rete Internet, che da strumento per la sola condivisione documentale (la pagina *web* resa disponibile dal sito *web* remoto) diviene la porta d'accesso alle risorse elaborative di un *provider* di servizi (l'applicazione resa disponibile in modalità web)."
Siamo di fronte ad una trasformazione irreversibile che "prefigura problematiche ben difficilmente risolvibili a livello nazionale che richiedono, invece, una riflessione condivisa a livello sia europeo sia internazionale".
Nell'attesa che tale alta riflessione giunga a completa maturazione, è auspicabile però che, dal basso, tutti i soggetti coinvolti nel trattamento di dati personali per le finalità istituzionali della scuola pubblica non perdano mai di vista alcuni aspetti fondamentali.
Il termine "*cloud*" è una *chatchword*,ossia una parola d'ordine, un richiamo con finalità di marketing, ed il riferimento alla "nuvola", che immediatamente allude ad una entità immateriale, evanescente ed eterea, un "non luogo" fluttuante nel web, non deve indurre in errore.

Come ha osservato James Bridle, scrittore e giornalista esperto di tecnologie, nel recente saggio "Nuova era oscura" (*New Dark Age. Technology and the End of the Future*; Roma, Produzioni Nero, 2019), ciò che chiamiamo *cloud* è in realtà"un'infrastruttura fisica composta di linee telefoniche, fibre ottiche, satelliti, cavi sul fondo dell'oceano e giganteschi magazzini pieni zeppi di computer che consumano quantità ingenti di acqua e di energia, e che dal punto di vista legale fanno capo a giurisdizioni nazionali. Quella del *cloud* è un nuovo tipo di industria ed è un'industria particolarmente famelica".

In altri termini, occorre sempre ricordare che i dati personali trattati in modalità *cloud computing* non finiscono tra le nuvole ma risiedono in un luogo fisico, all'interno di potenti elaboratori allocati da qualche parte nel mondo, assoggettati alle scelte imprenditoriali dei fornitori ed esposti a rischi non direttamente controllabili da parte del titolare del trattamento, e che tale parziale perdita di sovranità sui dati non alleggerisce affatto le responsabilità di quest'ultimo nei confronti degli interessati ai quali i dati appartengono, semmai le accresce.

Bruno Cantarone: *Avvocato cassazionista, Privacy Officer, consulente e formatore privacy nonché Responsabile della Protezione dei Dati per numerose istituzioni scolastiche pubbliche di ogni ordine e grado.*