PRIVACY E SCUOLA

TRA LE NUVOLE

MANUALE PRIVACY PRATICO-GIURIDICO PER UNA SCELTA CONSAPEVOLE DI SOLUZIONI CLOUD IN AMBITO SCOLASTICO: CRITERI DI INDIVIDUAZIONE DEI DATI PERSONALI, DEFINIZIONE DEI RUOLI PRIVACY E INDICAZIONI PER EFFETTUARE SCELTE OPERATIVE CORRETTE

Autori: avv. Luca Bolognini – avv. Enrico Pelino

A chi si rivolge questo contributo, che cosa si propone, a quali criteri si ispira

La breve riflessione sviluppata in questo manuale ha come ideali destinatari **docenti** e **dirigenti scolastici** chiamati a effettuare scelte in materia di soluzioni tecnologiche o in generale di software applicativi che comportino l'utilizzo di tecnologia cloud computing.

L'obiettivo che si propone è quello di **accompagnare per mano** in una prima comprensione e individuazione delle soluzioni cloud, evidenziando i passaggi sui quali occorre prestare maggiore attenzione, suggerendo strategie di approccio alle soluzioni cloud e criteri pratici di scelta. In definitiva, si propone come **uno strumento di pronta consultazione e di primo orientamento giuridico**, che, senza avere pretese di completezza o di dettaglio nell'approfondimento, privilegia un approccio pratico.

Del resto, **non constano** nello specifico settore dell'"educazione" lavori mirati in materia di cloud computing. Lo stesso Garante per la protezione dei dati personali, che pure ha affrontato nel corso della sua attività varie tematiche legate al mondo della scuola[1] e, negli ultimissimi anni, ha avviato un lavoro di inquadramento tecnico-giuridico sulla tecnologia cloud[2], non ha finora affrontato congiuntamente questi argomenti, offrendo una posizione di sintesi per utilizzo pratico.

Gli autori sono naturalmente ben consci del fatto che nel settore dell'istruzione esiste consapevolezza e attenzione al trattamento dei dati personali e che vengono di regola seguiti programmi di formazione, per cui il *quid* veramente nuovo di questo manualetto sta nelle caratteristiche specifiche di focus sul "cloud" e nella particolare declinazione che esse determinano nell'approccio alla disciplina sul trattamento dei dati personali.

Cercando una chiave pratica per ordinare schematicamente l'esposizione, si è ritenuto che il criterio più diretto e immediato potesse essere quello di articolarla attorno a quattro momenti chiave di un percorso espositivo, ossia: **il che cosa, il chi, il perché, il come**.

1 Va segnalata anche l'opuscolo dal titolo *"La privacy tra i banchi di scuola"*, del 2010 doc. web n. 1723730.

2 Cfr. i due opuscoli dal titolo *"Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*, del 2011 (doc. web n. 1819933) e *"Cloud computing. Proteggere i dati per non cadere dalle nuvole"*, del 2012 (doc. web n. 1895296).

CHE COSA

Il cloud computing

"Cloud", "nuvola" è ovviamente una *catchword*, un termine di richiamo per finalità di marketing, che tuttavia allude alla caratteristica più tipica e distintiva di questa tecnologia, ossia il fatto di basarsi su un'estrema virtualizzazione, di smaterializzare l'esistente, almeno nella prospettiva dell'utente. Nella prospettiva del fornitore del cloud c'è invece un forte radicamento concreto: un'infrastruttura articolata, diffusa e ben organizzata di elaboratori (*server*), configurabili in maniera dinamica in base alle esigenze del momento, dotati, nella loro reciproca integrazione, di un'impressionante potenza computazionale e in grado di offrire un servizio ubiquo e pressoché indipendente dal luogo fisico in cui si trova l'utente. "Dove sono i miei dati?" Sono sulle nuvole, non in luogo preciso dello spazio, ma in una sorta di bolla dalla configurazione variabile che alleggerisce per l'utente l'esecuzione di tutta una serie di compiti.

Cloud computing: intersezione con tematiche privacy[3]

Ciò comporta evidentemente che i dati si "muovano molto", siano cioè **trasferiti velocemente da un luogo all'altro** e siano potenzialmente **replicati in più copie** (la ridondanza soddisfa in molti casi esigenze di sicurezza). Quando un dato viene trasferito rapidamente da un paese all'altro e replicato, e si tratta di un dato *personale* (vedasi più avanti per una definizione), sorgono in via automatica e necessitata esigenze di approfondimento in materia di tutela dei dati personali.

Vale la pena evidenziare, da subito, che il testo normativo in vigore, il d.lgs. 30 giugno 2003, n. 196 (di seguito indicato anche come "Codice privacy") **vieta** all'art. 45 il trasferimento di dati personali in paesi non appartenenti all'Unione Europea, a meno che non ricorrano alcune tassative ipotesi di esonero. Agli stati membri della UE sono parificati i paesi dello Spazio Economico Europeo (SEE), ossia Liechtenstein, Norvegia e Islanda, e una manciata di stati il cui livello di protezione dei dati personali è stato considerato "adeguato" dalla Commissione europea.

3 Per praticità, nel presente lavoro ci si conformerà all'uso corrente che utilizza il termine "privacy" come sinonimo di "protezione dei dati personali". In realtà, a un livello più tecnico, le due espressioni individuano aree concettualmente diverse, sebbene in parte sovrapposte.

Al di fuori perciò della UE/SEE o dei paesi con livello di protezione adeguato, ogni trasferimento di dati personali deve considerarsi illegittimo, a meno che non ricorrano le già accennate ipotesi di esonero o si faccia uso di particolari strumenti (es. BCR e *model clause*), sui quali si tornerà più avanti nella sezione di questo manuale dedicata al "come". Con un'espressione pratica potremmo chiamarle qui "condizioni di liceità".

Per calare il discorso nella concretezza del tema che ci occupa, se un docente o un dirigente scolastico fanno uso di tecnologia cloud che impiega server collocati ad esempio in India (possibile che questo accada anche nell'uso di una semplice *app* basata su cloud), ne deriva un trasferimento di dati personali (ad esempio i dati di alunni) dall'Italia all'India. Ebbene, se non constano le già dette condizioni di liceità, questo trasferimento di dati si pone in violazione di legge. Ciò determina **precise conseguenze** per il docente o per il dirigente scolastico che hanno fatto ricorso allo strumento tecnologico che ha posto in essere in essere un trasferimento vietato di dati personali.
Nessuna conseguenza potrebbe invece sorgere in capo al fornitore di servizi cloud, in quanto potrebbe trattarsi di soggetto nei cui confronti non si applica la normativa nazionale o quella europea e che dunque, a meno di non esservi vincolato contrattualmente, non è tenuto a osservare le medesime disposizioni sul trattamento dei dati personali.

Quali offerte di cloud possono interessare il settore dell'"educazione"?

Si possono immaginare varie applicazioni della tecnologia cloud nel settore dell'"educazione".
Per necessità di semplificazione di catalogazione, in questo manualetto si sono ipotizzate tre categorie di applicazioni:

- applicazioni cloud che facilitano il lavoro di organizzazione dell'istituto scolastico, ad esempio l'attività di segreteria e contabile, che forniscono "suite per ufficio" concepite sulle esigenze della scuola, servizi di organizzazione della biblioteca o servizi di accesso a risorse di studio virtuali, servizi di protocollo virtuale, adesione a progetti ministeriali che prevedono l'integrazione tra diverse strutture per la realizzazione di macro-trattamenti di dati. In definitiva, si tratta di servizi informatici non del tutto dissimili da quelli disponibili in altri ambiti d'ufficio o di quelli disponibili per la pubblica amministrazione. La decisione di dotarsi di questi servizi è in parte necessitata, in parte rimessa al dirigente scolastico, in parte collocabile a livello gerarchico più alto;

- applicazioni cloud ugualmente riconducibili all'area dell'amministrazione, ma che coinvolgono direttamente anche profili connessi con lo svolgimento dell'attività didattica dei docenti: si pensi ad esempio un registro online per i docenti. In questo caso la decisione interessa anche l'organo collegiale dei docenti.
- applicazioni cloud che integrano direttamente l'offerta didattica, quali applicazioni online che permettono di sviluppare percorsi di approfondimento, condividere ricerche o utilizzare particolari strumenti di organizzazione e di ripasso delle informazioni, risorse online per il calcolo e la progettazione, la consultazione di riviste e articoli, la partecipazione a gruppi di ricerca condivisa, a programmi di scambio di conoscenze linguistiche, ecc.. La decisione di avvalersi di questi servizi può essere a seconda dei casi riconducibile al singolo docente, come anche all'organo collegiale dei docenti, oppure anche dal dirigente scolastico, qualora si tratti di dotazioni informatiche acquisite dalla scuola e messe in generale a disposizione di tutti i docenti.

Anche in considerazione della sommaria classificazione di cui sopra, sembra agli scriventi che la formula di erogazione di servizi cloud più adatta nel settore considerato possa essere in definitiva appunto ravvisata nel modello **SaaS (*Software as a Service*)**, ossia quella nella messa a disposizione di servizi cloud di tipo applicativo.

Altra ipotizzabile modalità di erogazione di servizi cloud potrebbe essere, per grandi volumi documentali (all'interno per esempio di un più ampio progetto di archiviazione o di virtualizzazione di biblioteche), un servizio di *cloud storage*, definibile con l'acronimo **STaaS (*Storage as a Service*)**, da considerare come una declinazione più specifica di un servizio infrastrutturale, vale a dire di un'offerta cloud di tipo **IaaS (*Infrastructure as a Service*)**, nel quale cui l'elemento caratteristico è appunto la messa a disposizione di un hardware, di uno spazio di memorizzazione.
Come emerge anche da queste abbreviazioni, elemento peculiare del cloud è la trasformazione di ogni soluzione proposta in un'offerta resa fruibile all'utente in termini di servizio, come tale acquistabile secondo le sue effettive esigenze. Si tornerà su questo aspetto al termine del manualetto.

Ultimo dei classici modelli di erogazione di servizi cloud è il **PaaS (*Platform as a Service*)**, che consiste nella messa a disposizione di una piattaforma di sviluppo di applicazioni software e in risorse per il loro hosting. Si tratta in effetti di una soluzione di particolare interesse anche nel settore dell'"educazione", perché può liberare risorse di creatività, tuttavia richiede conoscenze tecniche superiori a quelle di chi acquista un servizio software già predeterminato e pronto all'uso, e ciò ne lascia immaginare un utilizzo leggermente più settoriale, per utenti in un certo senso smaliziati, quali potrebbero essere quelli che partecipano a laboratori informatici all'interno di istituti scolastici o che seguono percorsi di studio connotati da una particolare specializzazione.
Tornando invece al dato giuridico, l'aspetto rilevante è che tutti i modelli indicati di offerta di servizi cloud si prestano, di per se stessi, nel loro normale utilizzo, al trattamento di dati personali.

Il concetto di dato personale

Può sembrare superfluo chiarire il concetto di dato personale, tuttavia così non è. Nell'esperienza degli scriventi, la percezione del dato personale diffusa in contesti non giuridici coincide sostanzialmente con quella di dato identificativo e inoltre molto spesso "dati personali" e "dati sensibili" sono usati come espressioni intercambiabili.

A questa approssimativa percezione corrente si sommano le complessità che il concetto espone invece al giurista, complessità che lo stesso Gruppo di lavoro cd. "ex art. 29" composto dai Garanti europei ha ritenuto necessario affrontare attraverso una serie di precisazioni concettuali nell'**opinione n. 4/2007**.

Ovviamente non è questa la sede per affrontare *funditus* il tema, tuttavia una qualche minima apertura sul significato giuridico da attribuire al concetto di "dato personale" è assolutamente necessaria, posto che stabile se un'informazione possa o non possa rientrare nella nozione è **dirimente** ai fini dell'applicabilità o no della disciplina di settore: mere informazioni dissociate da una componente personale o dati anonimi sono infatti fuori della portata applicativa della disciplina del Codice privacy.

Orbene, si intende per "dato personale" qualsiasi informazione associabile a una persona fisica anche soltanto identificabile (e dunque non necessariamente identificata), definizione nella quale gli elementi fondamentali sono due:

- il riferimento alla **persona fisica** (dunque non a una persona giuridica, a un ente a una pubblica amministrazione, ecc.)
- l'esistenza di **un elemento connettivo** tra informazione e persona fisica.

Anche chiarita in questi termini, la nozione ha oggettivamente una portata assai ampia. Ad esempio, è stata riconosciuta la natura di dato personale a informazioni che sono associabili a una persona identificata solo attraverso **l'incrocio** con altre informazioni **detenute da terzi soggetti** e tali dunque da permettere la potenziale individuazione a costoro del soggetto a cui i dati si riferiscono. Ha per esempio precisato il Garante che *"è... necessario... evitare di inserire nelle comunicazioni scolastiche elementi che consentano di* ***risalire****, anche* ***indirettamente****, all'identità di minori coinvolti in vicende particolarmente delicate"*[4]. Ugualmente, sono state considerate dati personali informazioni rese sì anonime attraverso una dissociazione dell'elemento connettivo dal riferimento a una persona fisica, ma in virtù di un processo non irreversibile.

Diversamente, invece, dati di calcolo utilizzati in un progetto, ossia tipologie di dato che potrebbero essere verosimilmente conferite in un cloud anche in ambito didattico, non sono di per sé dati personali.
Ugualmente non sono, di regola, dati personali voci numeriche di bilancio riferite a una società di capitali. Anche in questo caso, si tratta di informazioni che potrebbero verosimilmente essere gestite in servizio cloud, ad esempio in ambito ragionieristico.

Allo stesso modo, informazioni statistiche aggregate che non possano più essere associate ai singoli soggetti che le hanno generate costituiscono informazioni non qualificabili come dati personali.
Ancora, informazioni di carattere storico e informazioni su persone non più viventi, sia pure in quest'ultimo caso con particolari cautele che in questa sede non è possibile approfondire[5], non vanno considerati dati personali.

4 Esempio tratto dall'opuscolo cit. *"La privacy tra i libri di scuola"*.
5 Si tratta di implicazioni connesse con la dignità della persona, da osservare anche nei confronti dei deceduti.

Invece, **tutte le volte** in cui si ravvisi la possibilità di istituire una connessione qualsivoglia tra un'informazione (di qualsiasi tipo: non solo uno scritto ma anche un'immagine, si pensi a una ripresa video o a una foto, o una registrazione audio) e una persona fisica vivente occorre, **a livello prudenziale**, ritenere che si sia in presenza di un dato personale. La persona fisica a cui l'informazione si riferisce viene qualificata, nei termini del Codice privacy, come "interessato".

È opportuno notare che l'elemento connettivo tra informazione e persona fisica può istituire (e non è infrequente) anche **relazioni multiple**, ossia collegare più interessati a uno stesso gruppo di informazioni: quelle informazioni saranno necessariamente allora dati personali per ciascuno degli interessati. Ad esempio, l'alunno che registri il video di una lezione con uno smart phone può porre in essere attività di trattamento che coinvolge contemporaneamente soggetti diversi, tutti interessati ai sensi del Codice privacy, quali il docente e altri studenti.
Lo stesso gruppo di informazioni contiene cioè, contemporaneamente, dati personali riferibili a persone fisiche diverse, tutte interessate di trattamento. Proprio in riferimento a questa tipologia di situazioni il Garante ha ad esempio chiarito, nel già citato opuscolo dal titolo *"La privacy tra i banchi di scuola"*, che *"è possibile registrare la lezione esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente* ***le*** *persone coinvolte nella registrazione (professori, studenti…), e ottenere il loro esplicito consenso*", ossia ottenere il consenso da una pluralità di interessati tutti collegati alla medesima informazione.

Tipologie di dati personali

Non tutti i dati personali appartengono alla medesima tipologia. Come si indicherà più avanti, elemento essenziale nella decisione di conferire in maniera eventualmente selettiva i dati nel cloud è la **capacità di identificare la tipologia dei dati personali** che vengono di volta in volta trattati. In particolare, il Codice privacy individua due speciali tipologie di dati personali all'interno del *genus* dei dati personali "comuni", e presidiate da una disciplina più stringente, determinata dalla particolare incidenza nella sfera personale delle relative informazioni e dall'elevato rischio di discriminazione o di esclusione sociale che la loro circolazione può comportare. Si tratta dei:

- dati sensibili;
- dati giudiziari.

La prima categoria è costituita dai dati idonei a rivelare:

- l'origine razziale ed etnica
- le convinzioni religiose, filosofiche o di altro genere
- le opinioni politiche,
- l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico
- lo stato di salute
- la vita sessuale

Questi ultimi due sottogruppi (dati idonei a rivelare lo stato di salute e dati idonei a rivelare la vita sessuale) si trovano talvolta indicati nella prassi come dati "supersensibili" in quanto sono oggetto di protezioni ulteriormente rafforzate nel Codice privacy rispetto alle altre tipologie di dati sensibili.

I dati giudiziari sono dati personali idonei a rivelare:

- i provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti;
- la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

In altre parole, i dati giudiziari connettono una persona fisica con informazioni relative al suo coinvolgimento in procedimenti penali. Non sono dati giudiziari quelli che informano invece di procedimenti civili o amministrativi.

Nel settore dell'educazione, il trattamento di quest'ultima tipologia di dati sembra del tutto marginale e confinata a ipotesi specifiche quali ad esempio esperienze didattiche condotte in luoghi di detenzione o la partecipazione a specifici progetti educativi. Nella generalità delle altre ipotesi, l'eventuale trattamento di dati giudiziari potrebbe intervenire in via puramente occasionale e non intenzionale.

Approfondimento sui dati sensibili

Quanto ai dati sensibili, ipotesi tipiche di trattamento di questa tipologia di dati sembrano ricorrere non tanto nello svolgimento dell'attività didattica in sé, quanto piuttosto nella fase amministrativa e gestionale della struttura scolastica. Si pensi per questo a trattamenti di dati per finalità contabile-amministrativa rispetto ad assenze e permessi per malattia, all'adesione a sindacati, alla gestione di agevolazioni/benefici/misure per disabilità, a scelte di programmazione relative della fruizione di attività di sostegno, all'indicazione di intolleranze alimentari la cui conoscenza è necessaria per l'erogazione del servizio di mensa scolastica, alla scelta dell'ora di religione, ecc.

Il trattamento di tali dati è reso possibile da espresse disposizioni di legge, dunque in sé non pone problemi ai sensi del Codice privacy, tuttavia il trasferimento delle attività di trattamento su cloud computing richiede un'analisi attenta dell'ambito di circolazione dei dati e in particolare volta a determinare la presenza di strumenti giuridici idonei a rendere leciti i trasferimenti, oltre che delle misure di sicurezza predisposte, incluso soprattutto il profilo della continuità operativa e del *disaster recovery*

I punti sopra accennati, e gli altri che si indicheranno in seguito (ved. più avanti sezione “come”) si rendono del resto necessari anche in caso di trasferimento sul cloud di dati “comuni”. Tuttavia, il trattamento di dati sensibili aggiunge una serie di altri adempimenti che il titolare del trattamento (ved. oltre) è tenuto a rispettare e che, di conseguenza, il responsabile del trattamento da questi nominato (nella specie il fornitore del servizio cloud) è tenuto ad applicare direttamente o comunque rendendo possibile l’autonomo adempimento al titolare del trattamento. Ad esempio, nel caso di soggetti pubblici vige l'obbligo di separare i dati idonei a rivelare lo stato di salute dagli altri dati personali trattati per finalità che non richiedono il loro utilizzo (art. 22, co. 7 Codice privacy). Si richiede inoltre l'impiego, per tutti i dati sensibili, di tecniche di cifratura o di procedure tali da rendere i dati temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità (art. 22, co. 6 Codice privacy). E’ allora importante che il servizio cloud consenta al titolare – per esempio una scuola – di applicare autonomamente misure minime di sicurezza, come la cifratura di dati o la creazione di profili di autorizzazione diversi per i singoli incaricati del trattamento.

In linea di massima, il suggerimento è quello di affidare a sistemi esterni di cloud computing il trattamento di dati personali “comuni” e di osservare maggiore prudenza nel caso di dati sensibili, ovvero di accertarsi che il servizio cloud messo a disposizione consenta l’applicazione delle misure di sicurezza previste dall’art. 22 del Codice privacy.

Quanto allo svolgimento dell'attività didattica vera e propria, essa può comportare il trattamento di dati sensibili in via più indiretta, occasionale e in definitiva atipica. In particolare, deve considerarsi plausibile che orientamenti più o meno definiti in materia di convinzioni politiche, filosofiche, religiose o sessuali possano emergere dalle opinioni espresse dall'alunno, specie se si tiene conto del fatto che il percorso didattico, in alcune materie in particolare, è volto anche a stimolare l'elaborazione critica e la formulazione di posizioni personali, tuttavia non appare possibile individuare o prevedere casi o ipotesi tipiche di emersione di orientamenti riconducibili alla nozione di dato sensibile ed è piuttosto vero, semmai, che tali orientamenti, se emergono, maturano durante un lungo percorso di relazione didattica e spesso anche per iniziativa estemporanea degli stessi alunni.

Non appare fuori luogo ritenere perciò che il trattamento di dati sensibili, nella normalità dei casi, va considerato puramente eventuale nel corso dell'attività propriamente didattica.

CHI

L'allocazione della titolarità del trattamento

Va chiarito a questo punto se e in quale modo, nella scelta di servizi cloud, docenti e dirigenti scolastici siano riguardati dalla normativa in materia di protezione dei dati personali e se ciò comporti responsabilità sul piano giuridico. Il Codice privacy prevede che chiunque tratta dati personali deve invariabilmente rientrare in una delle tre seguenti categorie di soggetti:

- titolare del trattamento;
- responsabile del trattamento;
- incaricato di trattamento.

Le suindicate categorie, alle quali ci si può per comodità riferire come ai "ruoli attivi" di trattamento, per distinguerle dal ruolo "passivo" che è proprio dell'interessato, non hanno una valenza astrattamente classificatoria, ma sono direttamente collegate a conseguenze giuridiche. In particolare, si tratta di conseguenze in materia di responsabilità civile, responsabilità per illeciti amministrativi, responsabilità penale. Non le approfondiremo, per via dei limiti intrinseci di questa pubblicazione.

Tali conseguenze si concentrano nell'imputazione di effetti giuridici **sulla figura del titolare**, ossia su colui a cui spettano decisioni autonome e apicali in materia di trattamento. La *ratio* è chiara: chi decide autonomamente un'attività di trattamento ne sopporta le conseguenze giuridiche.

La normativa di settore (Codice privacy) ravvisa **tre caratteristiche essenziali** nella figura del titolare del trattamento. Il titolare è cioè il soggetto che:

- decide le finalità del trattamento;
- decide le modalità e gli strumenti di trattamento utilizzati;
- decide il profilo della sicurezza (la decisione può essere anche nel senso di "esternalizzare" verso terzi il profilo della sicurezza, concordandone il livello garantito e riservandosi poteri di verifica)

Semplificando alquanto, l'individuazione del titolare del trattamento avviene ad esito di un apprezzamento che non può prescindere da considerazioni **di fatto**: ossia, è titolare il soggetto che nei fatti opera come tale, anche indipendentemente da diverse indicazioni contrattuali (quelle nella specie del contratto collettivo) o da diverse investiture formali (come l'attribuzione di specifici incarichi didattici). Questo non vuol dire, occorre precisare, che indicazioni contrattuali e investiture formali non abbiano rilevanza, tutt'altro: esse permettono di comprendere quale ripartizione dei ruoli le parti coinvolte abbiano concordato e come vadano intese e contestualizzate le operazioni di trattamento dei dati personali; tuttavia dati meramente formali non possono prevalere su situazioni fattuali da cui emergano evidenze diverse.

Normalmente, **il singolo istituto scolastico potrà essere considerato quale "titolare del trattamento"**, ma vi potranno anche essere eccezioni.

Le scelte autonome del docente

Tale precisazione ha una rilevanza specifica nel settore in esame, posto che il ruolo ricoperto dal **docente** è per sua natura connotato da una sfera di autonomia più o meno ampia (anche a seconda delle determinazioni assunte dall'organo collegiale della scuola) ed esercita una certa libertà critica nelle scelte del percorso formativo degli allievi. Il docente può in definitiva trovarsi **nei fatti** a compiere **scelte autonome** circa gli strumenti didattici informatici da utilizzare. È qui d'obbligo una precisazione: mentre la finalità educativa e formativa non appare in sé rimessa al docente, questi infatti piuttosto la esegue quale prestazione contrattuale, possono invece essere, a seconda dei casi, rimesse al docente alcune concrete modalità di effettuazione della finalità didattica. Che la scelta di modalità e strumenti didattici sia oggetto di determinazione autonomo e diverso rispetto alla scelta della finalità più generale di insegnamento traspare già chiaramente, giusto per proporre uno dei tanti possibili esempi, da un provvedimento del Garante risalente alla fase di prima applicazione della normativa di settore (vigente ancora la legge 675/96). In data 4 marzo 1999, doc. web n. 39093 l'autorità ha avuto infatti modo di chiarire che *"l'assegnazione da parte degli insegnanti di temi in classe, anche se attinenti alla sfera personale o familiare degli alunni, è del tutto lecita e rispondente alle **funzioni** attribuite all'**istituzione scolastica**"*. In definitiva, tutto ciò che rientra nelle finalità didattiche non confligge di per sé con esigenze di protezione dei dati personali. Ha tuttavia precisato già in quell'occasione il Garante: *"Restano peraltro fermi gli obblighi di*

riservatezza già previsti per il corpo docente, a livello di segreto d'ufficio e professionale, dalle disposizioni vigenti in materia di istruzione scolastica ed ora rafforzati dai principi sanciti dalla legge n. 675/1996 nonché, in particolare, quelli relativi alla ***conservazione*** *dei dati personali eventualmente contenuti nei temi predisposti dagli alunni (v. art. 9 della legge stessa)"*. La precisazione riguarda appunto il profilo delle modalità del trattamento, che includono le modalità di conservazione dei dati personali.
A seconda dei casi, può essere rimessa al docente anche la scelta del profilo della sicurezza dei dati: affidarsi a un determinato strumento informatico può infatti implicare anche un'accettazione delle misure di sicurezza predisposte dal fornitore dello stesso.

Poste queste premesse, **il docente che scelga autonomamente di conferire dati personali dei suoi alunni in soluzioni cloud (es. applicazioni didattiche online) agisce, ad avviso degli scriventi, come titolare di trattamento**.

Naturalmente, questa valutazione dipende dai casi specifici. Per uscire dal piano astratto ed esemplificare, l'eventuale scelta del docente di utilizzare nell'attività didattica un'applicazione online di terzi potrebbe, a seconda dei casi, configurarsi come scelta assolutamente autonoma di un titolare del trattamento oppure come applicazione di decisioni prese a livello gerarchicamente superiore dal dirigente d'istituto, che abbia individuato in quell'applicazione un utile strumento didattico o anche come applicazione di una decisione dell'organo collegiale dell'istituto. **In tali casi potrebbero essere questi soggetti individuati come titolare del trattamento, o potrebbe verificarsi una situazione di contitolarità**.

Sotto altro profilo, del tutto incidentale in questa rapida ricostruzione divulgativa, va segnalato al lettore che la questione dell'**allocazione dei ruoli privacy**, ossia delle nomine a "responsabile di trattamento" e "incaricato di trattamento" (ruoli sui quali non c'è qui spazio di approfondimento), nel settore scuola non va sottovalutata e presenta intrinseche complessità sulle quali sarebbe probabilmente auspicabile una riflessione chiarificatrice del Garante.

La corretta individuazione dei ruoli attivi di trattamento, con le connesse responsabilità, può infatti rappresentare attività dagli esiti tutt'altro che scontati. Nel caso di strutture complesse o di strutture

nelle quali esistono oggettivi margini di scelta decisionale indipendente possono ravvisarsi sottolivelli di titolarità autonoma (o di contitolarità). Già in una delle sue primissime decisioni il Garante osservava: *"... Poss(o)no essere considerate 'titolari' - o contitolari - dei trattamenti complesse unità organizzative (quali direzioni generali o aree), interne alla complessiva struttura, ove queste esercitino un potere decisionale reale e del tutto autonomo sulle finalità e sulle modalità dei trattamenti effettuati nel proprio ambito"*[6].

6 Garante prot. d.p., 9 dicembre 1997, doc. web n. 30915.

PERCHE'

Le ragioni del cloud computing

Perché questo manualetto sul cloud? Perché il cloud è un'occasione e una risorsa. In particolare, è un potente strumento di contenimento dei costi e di massimizzare dei risultati e riduce tutta una serie di operazioni di dotazione informatica, manutenzione, ammortamento, aggiornamento, rinnovo di strumenti hardware e software. In definitiva semplifica l'esigenza di approvvigionamento informatico trasformandola in una sorta di utenza a consumo.

Lo stesso **codice dell'amministrazione digitale** (d.lgs. 7 marzo 2005, n. 82), all'art. 68, co. 1, rubricato *"Analisi comparativa delle soluzioni"*, indica **espressamente** il cloud tra le scelte di software che la pubblica amministrazione è tenuta a valutare. Peraltro, tra i criteri che la pubblica amministrazione deve seguire c'è appunto quello della *"conformità alla normativa in materia di protezione dei dati personali"* (comma secondo). Un cloud conforme, questo è uno dei temi centrali del presente manualetto, **è assolutamente possibile allo stato della normativa** (si tornerà sul punto nella parte relativa al "come").

Del resto, la tecnologia in questione è ormai di ampia e comune applicazione nell'Unione Europea, ed è considerata assolutamente strategica, il che evidentemente ne attesta non solo il successo attuale ma ne indica le prevedibili linee di un'ulteriore affermazione nel prossimo futuro. In altre parole, lo scenario che si va tratteggiando è quello di una presenza sempre più pervasiva della tecnologia cloud.

Sembra opportuno, in questa parte dedicata ai "perché" del cloud, proporre una rapidissima panoramica delle più recenti aperture europee sull'argomento:

- nella seconda metà del 2012 la Commissione europea ha diffuso la comunicazione dal titolo *"Unleashing the Potential of Cloud Computing in Europe"*[7], Bruxelles 27.9.2012, COM(2012) 529 final, volta a individuare le linee per uno sviluppo sempre più integrato del cloud computing in Europa;

7 "Liberare il potere del cloud computing in Europa" (trad. d. a.).

- è operativa una *"European Cloud Strategy"*, ossia un'iniziativa della Commissione europea, seguita alla già detta comunicazione, e volta a promuovere i servizi cloud;
- si è dato vita a uno *European Cloud Partnership* (ECP) e al relativo *Steering Board.* Quest'ultimo, riunitosi per la prima volta il 19 novembre 2012, ha recentemente prodotto (inizio 2014) un rapporto dal titolo *"Establishing a Trusted Cloud Europe"*, di ampia circolazione, che propone idee e indica azioni programmatiche per migliorare il funzionamento dei servizi cloud nel mercato europeo. Per dare un'idea di massima del fenomeno di cui stiamo parlando, a pag. 8 del rapporto viene indicato che *"(g)li effetti economici complessivamente attesi dal cloud computing tra il 2010 e il 2015 nelle cinque maggiori economie europee è stimato da solo in circa 763 miliardi di euro. L'economia del cloud sta crescendo a un ritmo superiore al 20% e potrebbe generare circa mille miliardi di prodotto interno lordo e 4 milioni di posti di lavoro per il 2020 in Europa, con il supporto del giusto framework di politiche"* (trad. d.a.)[8];
- di recente Neelie Kroes, vice-presidente della Commissione europea responsabile per l'Agenda digitale, è tornata a pronunciarsi sul cloud computing. Ne ha ricordato le opportunità a livello europeo in un discorso, *"A cloud for Europe"*, tenuto il 14 novembre 2013 alla conferenza omonima a Berlino; le ha ancora ribadite il 10 marzo 2014 al Cebit di Hannover (*"Securing our digital economy"*) e il 18 marzo 2014 (*"Want to build tomorrow's Internet?"*) ad Atene nel contesto della Future Internet Assembly.

Sintetica panoramica delle caratteristiche del cloud

È utile completare questo brevissimo *excursus* sulle ragioni del cloud evidenziando alcuni dei tratti salienti della tecnologia, tratti legati anche al suo oggettivo successo:

- scalabilità del servizio, ossia possibilità di espandere o contrarre l'approvvigionamento di servizi informatici a seconda delle esigenze. Nel caso il fruitore del cloud sia un'azienda può trattarsi della fluttuazione di esigenze di produzione, per cui in periodi di crescita è desiderabile avere una maggiore disponibilità di risorse informatiche, in modo da sostenere adeguatamente l'espansione delle attività, mentre in periodi di riduzione della produzione è desiderabile non trovarsi con risorse sovradimensionate, ossia in definitiva non sopportare

8 . *"The expected cumulative economic effects of cloud computing between 2010 and 2015 in the five largest European economies alone is around € 763 Bn. The cloud economy is growing by more than 20% and could generate nearly € 1 trillion in GDP and 4 million jobs by 2020 in Europe, with the support of the right policy framework"*.

costi non necessari. Per un istituto scolastico o universitario si può trattare di fluttuazioni della richiesta informatica dovute a variazioni nel numero di iscritti o delle attività di formazione sviluppate;

- **abbattimento dei costi fissi**, ad esempio quelli necessari per l'acquisto di hardware o di licenze software, costi di manutenzione, aggiornamento, sicurezza. In definitiva, tutto ciò che è necessario alle esigenze di elaborazione e memorizzazione di informazioni elettroniche viene fornito dal cloud provider contro il pagamento di un canone. Ciò permette semplificazioni nella programmazione e, a seconda dei casi, risparmi economici. Un fattore da considerare per gli istituti scolastici può ad esempio essere quello dell'obsolescenza e della manutenzione degli elaboratori in dotazione, come anche quello dell'acquisto e del rinnovo di licenze per programmi applicativi (a parte naturalmente il caso dell'utilizzo di programmi gratuiti o concessi con formule contrattuali diverse dalla tradizionale licenza). Una migrazione al cloud, a seconda delle caratteristiche del servizio scelto, può abbattere significativamente sul lato software esigenze di acquisto e rinnovo di licenze e può avere significativi benefici anche in termini di dotazioni strumentali, nel senso che l'allocazione sul cloud provider di una serie di servizi di elaborazione consente alla struttura scolastica di dotarsi solo del minimo di terminali necessari al collegamento con il cloud provider. In parte potrebbe trattarsi anche dei dispositivi portatili degli stessi utenti finali, studenti o personale docente;
- **sicurezza informatica**. Altre considerazioni di rilievo riguardano l'aspetto della sicurezza delle informazioni, se si considera che la massa critica economica e organizzativa di cloud provider può garantire livelli molto elevati in tal senso, sia sul piano tecnico sia su quello organizzativo. Sotto altro profilo, la sicurezza va concepita anche in termini di effettiva capacità di controllo e verifica da parte del titolare del trattamento dei dati sulle misure di sicurezza implementate. Si tornerà sul punto, a proposito dell'esame dei profili contrattuali;
- **ubiquità del servizio e neutralità del dispositivo d'accesso**. Un vantaggio (certo non esclusivo) della tecnologia cloud è quello di non essere strettamente legata a un determinato punto fisico di accesso, nel senso che di regola ci si può collegare a una rete cloud da qualsiasi terminale connesso in Internet. Questo consente una grande indipendenza da vincoli di luogo fisico e la possibilità di lavorare in situazioni di ufficio virtuale. Una siffatta funzionalità può rivelarsi utile anche per finalità didattiche o per la creazione di gruppi di

ricerca virtuali. L'ubiquità è peraltro potenziata dal fatto che la fruizione dei servizi cloud è in gran parte indipendente dal dispositivo (anche mobile) e dal sistema operativo dell'utente;

- **sincronizzazione dei dati**. Anche in questo caso non si tratta di una caratteristica esclusiva dei servizi cloud. La sincronizzazione può avere un ruolo strategico indispensabile nella corretta organizzazione delle informazioni.

COME

Come affrontare scelte in materia di cloud computing che rispondano a esigenze di rispetto della normativa e riflettano un approccio consapevole del titolare del trattamento?

Verifica dell'esistenza delle condizioni per un trasferimento lecito dei dati extra UE/SEE

Sarebbe semplicistico ridurre l'analisi delle tematiche in materia di trattamento dei dati personali relative al cloud al solo profilo del trasferimento di dati extra UE/SEE. La tematica tuttavia è certamente una delle più rilevanti e ricorrenti.

Ebbene, innanzitutto va sfatato un luogo comune: non è affatto impossibile avvalersi dei servizi di un cloud computing provider extra-europeo. Basta verificare alcuni elementi che rendono questa attività lecita, anche in ambito scolastico.

Il trasferimento di dati personali in area extra UE/SEE è considerato lecito se ricorrere una delle seguenti ipotesi:

- **Consenso dell'interessato –** la prestazione del consenso da parte dell'interessato, ossia del soggetto al quale i dati personali si riferiscono, o la ricorrenza di uno dei casi tipizzati di esonero dal consenso ed elencati dalle lettere b) a g) dell'art. 45, co. 1 Codice privacy (non se ne parlerà, per via dei limiti di questo manualetto) rendono lecito il trasferimento, sempre che il consenso sia espresso e abbia i requisiti di libertà, specificità e preventiva informazione previsti dal codice privacy.

Va avvertito che nel caso di conferimento di dati degli studenti in applicazioni cloud per la didattica, gli scriventi esprimono forti perplessità sulla validità di un eventuale consenso di questi ultimi, per un doppio ordine di ragioni:

- i minori infradiciottenni (ove sia questo il caso) non hanno, per regola generale civilistica (art. 2 cod. civ.), la capacità di agire e come tale, a parte in casi in cui leggi speciali stabiliscano diversamente, di esprimere un valido consenso in merito al trattamento dei propri dati personali. Potrebbe supplire naturalmente il consenso dei genitori;

- in generale, un consenso prestato da un soggetto sottoposto all'autorità morale del docente difficilmente (salvo specifiche eccezioni) può essere considerato "libero" e soddisfare i requisiti di cui all'art. 23 Codice privacy. Anche in questo caso tuttavia si potrebbe ovviare con l'espressione di uno specifico consenso da parte dei genitori.

- **Binding corporate rules –** Con l'espressione si allude all'utilizzo da parte del fornitore del servizio di cloud computing delle cd. *"binding corporate rules"* o *BCRs*, vale a dire codici di regole in materia di protezione dei dati personali auto-adottati da società multinazionali e osservati dall'intera struttura del gruppo. Le *BCRs* sono approvate attraverso una specifica procedura, non priva di complessità, da tutte le autorità garanti dei paesi membri UE da cui hanno origine i trasferimenti di dati personali, attraverso un meccanismo facilitato da un sistema di mutuo riconoscimento che fa perno su un'autorità garante capofila ("*lead authority*");

- **Model clauses –** Sono cd. "clausole contrattuali standard", approntante dalla Commissione europea, note anche come "*model clauses*". Forniscono schemi contrattuali tipici, non modificabili, già predeterminati dalla Commissione e che quindi non necessitano ulteriori procedure di verifica, se non quella relativa alla loro effettiva trasposizione integrale. Si tratta ad avviso degli scriventi di uno degli strumenti più efficaci, sia per l'immediatezza e la sicurezza del controllo dell'articolato contrattuale sia per la linearità e praticità nell'applicazione (le clausole standard relative al rapporto titolare-responsabile sono reperibili qui, devono essere compilate ma non modificate nel testo che è predefinito: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1767001);

- **Contratto ad hoc –** Un'ulteriore soluzione per il trasferimento di dati può essere la stipulazione di contratti *ad hoc* tra il fornitore di servizi cloud e i soggetti destinatari del flusso dei dati personali. Questa costituisce peraltro, tra tutte, l'ipotesi più giuridicamente impervia e importa una serie di difficoltà che in questa sede non è possibile affrontare;

- **Safe Harbor –** Per i titolari di trattamento stabiliti negli Stati Uniti è possibile aderire al programma "Safe Harbor" del Dipartimento del commercio statunitense, approvato dalla

Commissione con la decisione 520/2000/CE del 26 luglio 2000. Tale programma prevede il rispetto di un nucleo essenziale (e assai limitato) di principi privacy da parte degli aderenti. Tuttavia, da un lato l'adesione al **Safe Harbor** è puramente volontaria e si risolve in un'autocertificazione, dall'altro il programma è considerato ormai datato e sostanzialmente disallineato con standard di protezione altrimenti garantiti attraverso il ricorso ad altri strumenti, come appunto le *model clauses*[9].

Punti specifici da esaminare nella scelta di un cloud

La verifica della presenza delle condizioni che rendono lecito il trasferimento extra UE/SEE non esaurisce naturalmente la serie di verifiche che una scelta di servizi cloud impone.

Per comodità di approccio, si ritiene utile proporre un'elencazione di punti specifici sui quali si richiama l'attenzione del titolare del trattamento (docente o dirigente scolastico, nel taglio seguito in questo manualetto) nella scelta di soluzioni cloud, con l'avvertenza che naturalmente la rilevanza e l'incidenza dei punti qui di seguito elencati dipende anche specificamente dalla tipologia di dati che si intende trattare, dal loro significato più o meno strategico per il funzionamento delle struttura scolastica, dalla quantità e dalla complessità dei trattamenti che si vogliono affidare a soluzioni cloud.

1. **Esame di eventuali finalità ulteriori del cloud provider –** Occorre controllare, nei documenti contrattuali, se lo strumento cloud utilizzato si limiti alla fornitura di un mero servizio strumentale o se il fornitore dello stesso non si riservi possibilità di utilizzo dei dati per proprie finalità ulteriori (ad es. promozionali). In tal caso si segnala che il fornitore del servizio sarebbe a sua volta qualificabile come titolare autonomo di trattamento e che il conferimento dei dati personali da parte del docente o del dirigente scolastico andrebbe definito come "comunicazione di dati a soggetto privato", con una serie di conseguenze a

9 Può essere utile segnalare che nell'opinione 5/2012 il Gruppo di lavoro dei Garanti europei osservava, p. 17: *"[...I]n the view of the Working Party, sole self-certification with Safe Harbor may not be deemed sufficient in the absence of robust enforcement of data protection principles in the cloud environment"* (trad. d. a.: *"Ad avviso del Gruppo di lavoro, la semplice autocertificazione prevista dal Safe Harbor può non essere sufficiente in assenza di una solida attuazione dei principi di protezione dei dati personali in ambiente cloud*"). Ugualmente, *ivi*, p. 18: *"Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC"* (trad. d. a.: *"Da ultimo, il Gruppo di lavoro ritiene che i principi Safe Harbor di per se stessi non garantiscano i mezzi necessari ad assicurare l'applicazione di idonee misure di sicurezza da parte del fornitore di servizi cloud negli Stati Uniti, secondo quanto potrebbe essere invece richiesta dalle normative nazionali basate sulla Direttiva 95/46/CE")*.

cascata in ambito privacy, che potrebbero esporre il soggetto comunicante/cedente, in caso di illecito, anche a responsabilità penali (da 6 a 24 mesi di reclusione, art. 167 c. 1 D.Lgs. 196/2003);

2. **Valutazione della tipologia di dati che si intende conferire –** Non vi è alcuna ragione di conferire in blocco dati personali, senza previa scrematura per tipologie o senza l'adozione di cautele, quali potrebbero essere per esempio la sostituzione degli identificativi degli interessati con pseudonimi (si tratterebbe in definitiva dell'applicazione di *"privacy enhancing technology"* o *"P.E.T."*);

3. **Comprensione dell'ambito di circolazione dei dati –** Occorre fare riferimento ai documenti contrattuali e verificare, nel caso non sia garantita la circolazione intra UE/SEE o in paesi con livello di protezione adeguato, che siano presenti schemi che garantiscono efficacemente la liceità del trasferimento dei dati, come le *model clauses*;

4. **Garanzie in materia di misure di sicurezza –** Essendo qualificabile il fornitore di servizi cloud come un responsabile esterno del trattamento, occorre che il titolare stabilito in Italia, ossia nel caso in esame il docente o il dirigente scolastico, attuino le misure di sicurezza idonee e minime previste dal Codice privacy e dall'allegato B al medesimo e facciano attuare le stesse misure anche al responsabile del trattamento. Va notato che, in linea di massima e per il valore che può avere una semplice considerazione di esperienza, i maggiori fornitori internazionali di servizi cloud assicurano un livello di sicurezza dei dati assolutamente superiore agli standard normativi. Tuttavia, specifiche previsioni in materia di dati sensibili potrebbero non essere allineate con le pur considerevoli misure di sicurezza poste in essere dal fornitore di servizi cloud. Inoltre, sul versante delle misure idonee, potrebbero non essere stati implementati servizi compatibili con le richieste del Garante in materia di amministratori di sistema. Pertanto, l'altro elemento cruciale da tenere presente sta nella effettiva possibilità tecnologica, per il cliente-titolare, di applicare autonomamente ulteriori misure di sicurezza utilizzando il servizio cloud (ad esempio, utilizzando file in forma cifrata, o potendo creare nuovi profili di autorizzazione per il trattamento di dati personali): ciò è spesso possibile;

5. **Garanzie in termini di continuità operativa e disaster recovery –** In generale, ma soprattutto per conferimenti di grandi quantità di dati personali che impattano sulla fornitura del servizio pubblico offerto dalla scuola (nel caso di istituti scolastici pubblici), è essenziale verificare le garanzie in termini di continuità operativa e ripristino dei dati nel caso di compromissione;

6. **Nomina a responsabile di trattamento –** Se sono conferiti nel cloud dati personali di terzi è necessario che il cloud sia nominato "responsabile del trattamento" ai sensi dell'art. 29 del Codice privacy. Diversamente esso potrebbe agire in qualità di titolare del trattamento, ma con le conseguenze già notate in precedenza sub n. 1;

7. **Garanzia di effettiva possibilità di controllo sul fornitore di servizi cloud –** Il titolare del trattamento, nel caso che ci occupa docenti e dirigenti scolastici o istituti nel loro complesso, deve, conformemente al proprio ruolo, essere in condizione di esercitare un effettivo potere di verifica sui trattamenti posti in essere dal fornitore di servizi cloud, con il limite dei diritti di proprietà industriale e intellettuale di costui, della protezione del *know how*, dei segreti industriali o di diritti privacy altrui. Il fornitore di servizi cloud mette normalmente a disposizione dell'utente un pannello di controllo per verificare una serie di elementi, tra i quali il luogo dove in un dato momento si trovano i dati personali;

8. **Verifica di giurisdizione e legge applicabile al contratto con il fornitore del servizio cloud –** Non sono possibili in questa sede approfondimenti sulle conseguenze giuridiche di tali pattuizioni contrattuali, si raccomanda in ogni caso di curare che la giurisdizione sia quella italiana, come anche la legge applicabile. Bisogna, tuttavia, dire che la legge privacy applicabile ad un titolare del trattamento di dati italiano è senz'altro quella italiana, ex art. 5 D.lgs. 196/2003); non solo, quanto al foro competente quando parte in causa sia un ramo dell'amministrazione dello Stato (e non un ente pubblico a sé stante) varrà – a prescindere da quanto scritto nel contratto – il foro erariale italiano, previsto dall'art. 25 c.p.c..

9. **Certezza della cancellazione al termine del trattamento dei dati conferiti –** Il titolare deve assicurarsi che al termine del contratto di cloud computing non permangano nella disponibilità del fornitore del servizio cloud dati conferiti al medesimo;

10. **Portabilità dei dati personali –** Elemento importante è quello della presenza o no di vincoli che non consentano al titolare del trattamento la migrazione verso altri servizi cloud. Questo requisito è ovviamente tanto più rilevante quanto più ampio è il volume di dati conferiti nel cloud e va posto anche in relazione con il significato e l'importanza di quei dati. Deve aggiungersi che la portabilità ideale prevede che sia rispettata, nella riconsegna dei dati, l'architettura di cartelle e file, come anche le codifiche applicate ai dati e sia possibile la scelta di un formato aperto oppure di un formato proprietario che sia pienamente e gratuitamente compatibile con formati aperti;

11. **Interoperabilità –** Si tratta di un requisito da valutare in base all'utilizzo che si intende fare dei dati conferiti nel cloud, utilizzo eventualmente integrato con altri sistemi informatici e telematici. L'interoperabilità postula l'adesione del fornitore del servizio cloud a standard e specifiche particolari, che rendono appunto possibile la comunicazione tra sistemi diversi. Si tornerà specificamente sul punto con alcuni esempi al termine di questo manualetto;

12. **Formalizzazione della responsabilità del fornitore cloud –** È desiderabile che le parti disciplinino espressamente la fase cd. "patologica" del contratto, formalizzando le ipotesi di responsabilità del fornitore cloud. È chiaro che un simile assetto contrattuale è ipotizzabile solo nel caso di importanti migrazioni di dati su servizi di cloud computing;

13. **Durata del contratto ed eventuale termine per la disdetta –** Si consiglia di porre attenzione a questo passaggio contrattuale e valutare i vincoli che pone e la libertà di modificare il fornitore di servizi cloud in maniera relativamente agevole;

14. **Parametri SLA e PLA –** Ossia i parametri numerici che definiscono i tempi di risposta e i livelli di servizio garantito in generale ("Service Level Agreement") o in particolare con riferimento alla privacy ("Privacy Level Agreement"). Tali parametri hanno ovviamente un

senso particolare nel caso in cui siano conferiti nel cloud grandi volumi di dati personali o gruppi di dati che hanno valore strategico, mentre rivestono un'importanza più contenuta nel caso di trattamenti minori e di mero ausilio all'erogazione dei servizi didattici.

15. **Diversificare i dati e valutare soluzioni cloud ibride –** Nel caso si intendano usare soluzioni cloud che coinvolgono un cospicuo numero di dati, rispondenti a tipologie diverse, possono essere consigliabili strategie di diversificazione, con l'adozione ad esempio di soluzioni cloud ibride (cloud privato + cloud pubblico). Occorre anche valutare se la dipendenza da un unico fornitore cloud possa essere un vantaggio (perché semplifica procedure e controlli) oppure un limite;

16. **Certificazioni –** Può essere utile orientarsi nella scelta del fornitore di servizi cloud anche in base alle certificazioni che questo può fornire. Naturalmente, come detto in precedenza, la rilevanza di questo aspetto dipende molto dalla tipologia, dalla qualità e dalla quantità dei dati conferiti nel cloud. La certificazione comporta di regola la sottoposizione del fornitore di servizi cloud ad *audit* periodici effettuati da terze parti.

Come già notato, ma vale la pena ribadirlo, i criteri di orientamento appena esposti vanno interpretati con ragionevolezza: essi potrebbero essere eccessivi e sovrabbondanti qualora l'utilizzo del cloud fosse limitato alla fruizione marginale di applicazioni di sussidio alla didattica, mentre potrebbe essere appena sufficiente quando il trasferimento sul cloud interessi completi settori di attività dell'istituto scolastico, rendendo quest'ultimo oggettivamente dipendente dal fornitore del servizio.

Valutare le effettive esigenze

Vanno da ultimo tenute presenti, in una valutazione complessiva in merito all'adozione di servizi cloud, le caratteristiche intrinseche di questa tecnologia rispetto a soluzioni informatiche più tradizionali, caratteristiche per le quali si rimanda alla rapida elencazione più sopra proposta (scalabilità, abbattimento dei costi fissi, sicurezza informatica, ubiquità del servizio e neutralità del dispositivo d'accesso, sincronizzazione dei dati). Occorre in definitiva chiedersi se tali caratteristiche siano rilevanti rispetto al servizio che si intende sottoscrivere e quali siano le

concrete esigenze di servizi informatici di cui si ha bisogno. La risposta evidentemente non potrà essere sempre omogenea ma dipende in maniera determinante dall'ampiezza del bacino di utenza al quale un certo istituto scolastico fa riferimento, dalle reali esigenze di disponibilità di servizi informatici, dalle capacità computazionali o dai programmi specifici richiesti, dalla possibilità di creare condivisioni utili con altri istituti che condividono le medesime esigenze, dal settore specifico dell'offerta didattica.

Limiti da tenere presenti

Da ultimo, occorre tenere presenti eventuali specifici obblighi di adozione di strumenti e procedure telematiche imposti da norme di legge, come ad esempio in materia di anagrafi regionali e anagrafe nazionale degli studenti. L'assolvimento di tali obblighi potrebbe essere valutato anche attraverso il ricorso a tecnologia cloud, tuttavia si impongono verifiche sulla reale compatibilità delle soluzioni rispetto a reti già esistenti di interscambio di informazioni nelle quali si entra a far parte.

Sono numerosi i progetti informatici di integrazione in ambito scolastico che vedono impegnato il MIUR e coinvolti a vario titolo gli istituti scolastici. Per citarne solo alcuni:

- la già accennata anagrafe nazionale degli studenti;
- il plico telematico;
- il sistema nazionale di valutazione delle scuole pubbliche e delle istituzioni formative accreditate dalle Regioni
- il Sistema Informativo Integrato delle Scuole

Esula dal perimetro di questo lavoro un'analisi specifica di questi progetti e sistemi informatici di condivisione ed elaborazione delle informazioni. Ciò che preme rilevare è comunque che un fattore di cui tenere dovuto conto è che molti di questi progetti prevedono già tendenzialmente contratti ministeriali con fornitori di servizi informatici. Nel caso in cui ci si debba inserire nel loro contesto, l'avvertenza è quella di verificare preliminarmente, caso per caso, se la migrazione di servizi e di dati su cloud di terze parti sia compatibile con la logica e la struttura dei progetti già avviati. Su un piano leggermente diverso, occorre poi comprendere e valutare se l'adozione di proprie soluzioni cloud che si pongano accanto a progetti già avviati non possa determinare ingiustificate duplicazioni di dati.

CONCLUSIONI

Il cloud computing rappresenta la tecnologia del momento. La strategia per una più facile integrazione di soluzioni cloud è attivamente perseguita in ambito comunitario. Sono molte le ragioni di questa affermazione, ma possono riassumersi tutte nella combinazione tra facilità di utilizzo (per via di una spiccata virtualizzazione del servizio e la possibilità di un'erogazione "su misura" all'utente) e contenimento dei costi.

Naturale perciò che soluzioni cloud siano adottate anche nel settore della scuola. Le caratteristiche della tecnologia, peraltro, che si basa una potenza computazionale ragguardevole, su una concentrazione delle informazioni presso pochi fornitori del servizio a livello globale, e sull'elevata mobilità dei dati, impongono un approccio consapevole e informato.
In definitiva, il cloud non deve spaventare ma va colto piuttosto come un'opportunità di cui giovarsi.

È chiaro che la consapevolezza implica uno sforzo, attivo, di identificazione dei dati personali da parte del titolare del trattamento, che a seconda dei casi (nel limitato approccio scelto per questo manualetto) sarà il docente o il dirigente scolastico.

Nel testo è stata fornita una serie di indicazioni pratiche, che, lungi dall'essere esaustive, possono fornire un primo orientamento pratico. Soprattutto si vuole raccomandare un approccio basato su una costante contestualizzazione delle esigenze reali di approvvigionamento di servizi informatici rispetto alle necessità avvertite, un confronto con soluzioni tradizionali, una valutazione della compatibilità dei servizi che vengono acquisiti con protocolli, specifiche e progetti integrati di collaborazione e scambio di informazioni già in essere.

Al termine di questo manualetto proponiamo due schede riassuntive, speculari, del tipo "checklist", l'una pensata come strumento per il titolare del trattamento, l'altra come strumento per il fornitore di servizi cloud che potrebbero essere utilizzate come promemoria pratico di valutazione delle soluzione cloud che si intende sottoscrivere.

Checklist n. 1

La presente checklist vuole essere uno strumento pratico-riepilogativo di massima per il titolare del trattamento nel valutare la scelta di soluzioni cloud

Punto da esaminare	Sì	No	Note
I trasferimenti extra UE/SEE sono effettuati nel rispetto del Codice privacy (per esempio tramite Model Clauses)?			
Emergono finalità ulteriori del cloud provider nel trattamento dei dati?			
È stata valutata la tipologia dei dati da conferire?			
Si è compreso l'ambito di circolazione dei dati?			
Si sono garanzie in materia di misure di sicurezza?			
Continuità operativa e disaster recovery sono garantire?			
Nomina del cloud provider a responsabile di trattamento è prevista?			
Ci sono strumenti di controllo sull'operato del cloud provider?			
Giurisdizione e legge applicabile sono chiarite nei testi contrattuali, con particolare riferimento alla protezione dei dati personali?			
I dati conferiti sono effettivamente cancellati al termine del contratto?			
È assicurata la portabilità dei dati, anche con uso di formati aperti?			
È assicurata l'interoperabilità rispetto a progetti in essere?			
Il fornitore cloud è sufficientemente affidabile sul piano della solidità economica e organizzativa?			
È soddisfacente la durata del contratto e l'eventuale termine per la disdetta?			
Si sono esaminate con attenzione le SLA e le PLA?			
Si sono valutate soluzioni cloud ibride (cloud pubblico + cloud privato o di comunità)?			
Sono presenti certificazioni e audit di terze parti?			
Le caratteristiche della soluzione cloud proposta sono in linea con le esigenze del titolare?			
Si sono valutate comparativamente anche soluzioni tradizionali?			
Si sono verificate eventuali incompatibilità rispetto ai progetti informatici istituzionali di cui si è parte?			

CHECKLIST n. 2

Questa checklist finale è pensata, in via speculare, come uno strumento riepilogativo ad uso del fornitore di servizi cloud. Potrebbe esserne richiesta la compilazione da parte del titolare che intende sottoscrivere una soluzione cloud oppure potrebbe proattivamente essere proposta, compilata, dallo stesso fornitore cloud al titolare, per evidenziare i punti di forza del servizio.

Punto da esaminare	Sì	No	SaaS	PaaS	IaaS
I trasferimenti extra UE/SEE sono effettuati nel rispetto del Codice privacy (ad esempio tramite Model Clauses)?					
Emergono finalità ulteriori del cloud provider nel trattamento di dati?					
È fornito un servizio diverso a seconda della tipologia dei dati da trattare?					
Si è specificato l'ambito territoriale e soggettivo di circolazione dei dati?					
Si sono previste garanzie in materia di misure di sicurezza e il cliente può applicare autonomamente ulteriori misure di sicurezza?					
Continuità operativa e disaster recovery sono previste?					
La nomina a responsabile di trattamento è accettata dal fornitore?					
Ci sono strumenti di controllo del cloud provider, come pannelli o altri tool di monitoraggio?					
Giurisdizione e legge applicabile in materia di protezione dei dati personali sono quelle italiane?					
I dati conferiti sono effettivamente cancellati al termine del contratto?					
È assicurata la portabilità dei dati, anche con formati aperti?					
È assicurata l'interoperabilità rispetto a progetti in essere?					
Il fornitore cloud è sufficientemente affidabile sul piano economico e organizzativo?					
Sono previsti chiaramente la durata del contratto e l'eventuale termine per la disdetta?					
Sono disponibili le SLA e le PLA?					
Sono disponibili soluzioni cloud ibride (cloud pubblico, privato o di comunità)?					
Sono presenti certificazioni e audit di terze parti?					
Il cliente-titolare è in grado di applicare autonomamente misure minime di sicurezza?					

Luca Bolognini – Presidente dell'Istituto Italiano per la Privacy. Laureato in giurisprudenza all'Università di Bologna, avvocato dell'Ordine di Roma, socio fondatore dello Studio ICT Legal Consulting Balboni Bolognini & Partners con sedi a Milano, Roma, Bologna, Amsterdam e corrispondenti in 18 Paesi esteri, svolge su tutto il territorio nazionale l'attività professionale, in particolare occupandosi di privacy/protezione dei dati personali, diritto delle comunicazioni e dei media, diritto del marketing, responsabilità amministrativa d'impresa e procedimenti innanzi ad autorità indipendenti. E' componente di Organismi di Vigilanza 231. Cura inoltre libri, documenti e analisi di diritto delle nuove tecnologie e delle comunicazioni. Ha svolto docenze per numerosi enti (tra cui Scuola Superiore della PA, Alma Graduate School, IED, TUV et al.) ed è incaricato, dal 2010, dell'insegnamento di diritto della privacy alla Scuola di Specializzazione per le Professioni Legali dell'Università di Teramo. E' docente dell'Istituto Jemolo partire dall'annata 2013/14. E' componente del Comitato dei Saggi dell'Associazione Nazionale Operatori e Responsabili della Conservazione Digitale (ANORC). Ha scritto in questi anni articoli, saggi ed editoriali per numerosi volumi, riviste scientifiche, quotidiani e periodici nazionali e internazionali (tra cui Corriere della Sera, Il Sole 24 Ore, Il Mondo, Affari Italiani, The Wall Street Journal, European Voice). Ha scritto e curato con Diego Fulco il primo commentario italiano al codice di Deontologia Privacy per avvocati e investigatori privati, edito da Giuffrè. E' stato co-autore e curatore con Paganini e Fulco del volume "Next Privacy, il futuro dei nostri dati nell'era digitale" (RCS Etas). Sito web: www.lucabolognini.it. Contatti: lucabolognini@istitutoitalianoprivacy.it

Enrico Pelino - Iscritto all'ordine degli Avvocati di Bologna, è specializzato in protezione dei dati personali, tutela della privacy e diritto dell'informatica, materie oggetto di numerose collaborazioni professionali e di approfondimenti e pubblicazioni scientifiche. In queste materie ha conseguito nel 2005 un dottorato di ricerca dell'Università di Bologna, occupandosi del tema della privacy e del potere di controllo riconosciuto alla persona sulle proprie informazioni. Successivamente è stato membro scientifico di progetti di ricerca interuniversitari, tra cui il Progetto di Ricerca di Interesse Nazionale (PRIN) 2007. È stato altresì assegnista di ricerca dell'Università di Bologna fino al 2009 su temi legati alla protezione dei dati personali nelle comunicazioni elettroniche. È relatore in convegni sul tema della protezione dei dati personali ed è stato docente in master e corsi universitari, oltreché collaboratore della cattedra di diritto di Internet presso l'Università di Bologna (Prof.ssa G. Finocchiaro). Si occupa altresì di diritto commerciale e di più generali profili di diritto civile, in ambito sia contenzioso sia stragiudiziale. Profili: Linkedin: www.linkedin.com/pub/enrico-pelino/1b/16b/a26. TED: www.ted.com/profiles/view/id/240689.

www.istitutoitalianoprivacy.it