Privacy a scuola

Prof. Pietro Prosperi

Presupposti normativi e riferimenti

- Codice delle Privacy
- Vademecum: la scuola a prova di privacy (2016)
- Cloud Computing - Proteggere i dati per non cadere dalle nuvole (2012)
- La trasparenza nei siti della PA - linee guida (2014)
- Norme Accessibilità, Siti web, Trasparenza, Usabilità
- Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione

Codice della Privacy

(Decreto Legislativo 30 giugno 2003 n. 196)

Finalità (art. 2 - Codice della Privacy)

Garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Definizioni (dal Codice della Privacy)

- **TRATTAMENTO**: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
- **DATO PERSONALE:** qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
- **DATI SENSIBILI:** i dati personali 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 o sindacale**, nonché i dati personali idonei a rivelare lo **stato di salute e la vita sessuale**.

Definizioni (dal Codice della Privacy)

- **TITOLARE**: la persona fisica, la persona giuridica ... cui competono ... le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; nelle scuole il Dirigente Scolastico quale legale rappresentante;
- **RESPONSABILE**: la persona fisica, la persona giuridica ... preposti dal titolare al trattamento di dati personali; figura delegata dal DS in genere il DSGA o un impiegato amministrativo;
- **INCARICATO**: le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;
- **INTERESSATO**: persona fisica cui si riferiscono i dati personali.

Diritti dell'interessato (art. 7 - Codice della Privacy)

- Conoscere l'origine, le finalità e le modalità di trattamento;
- Conoscere il titolare, i responsabili e gli incaricati al trattamento;
- Ottenere l'aggiornamento, la rettifica, l'integrazione e la cancellazione;
- Opporsi al trattamento, anche se pertinenti allo scopo della raccolta.

I diritti sono esercitati con richiesta, senza formalità, rivolta al titolare o al responsabile, anche per il tramite di un incaricato. La richiesta può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica.

Informativa (art. 13 - Codice della Privacy)

L’interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

- le finalità e le modalità del trattamento;
- la natura obbligatoria o facoltativa del conferimento;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati;
- i suoi diritti;
- gli estremi identificativi del titolare e dei responsabili.

L’informativa non si applica quando i dati sono trattati in base a un obbligo di legge o nel caso di ricezione di curricula spontaneamente trasmessi dagli interessati.

Regole per i soggetti pubblici (artt. 18 - 22 Codice della Privacy)

- Il trattamento di dati personali è consentito soltanto per lo svolgimento delle funzioni istituzionali;
- Il trattamento dei dati, diversi da quelli sensibili e giudiziari, è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente;
- Il trattamento dei dati sensibili è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite;
- Nel fornire l'informativa fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

Consenso (art. 23 - Codice della Privacy)

Il consenso espresso dell'interessato è previsto per il trattamento di dati personali da parte di privati o di enti pubblici economici.

Deve essere manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Il consenso non è richiesto quando il trattamento è necessario per un obbligo di legge, per obblighi contrattuali, per i dati provenienti da pubblici registri o per la salvaguardia della vita e dell'incolumità fisica di un terzo.

Misure minime (art. 31 - Codice della Privacy)

Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31:

> *"I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da* ***ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta****."* (art. 31. Obblighi di sicurezza)

Parametri di sicurezza

- **INTEGRITA'**: i dati non devono essere alterati (cancellati o modificati) da terzi non autorizzati o a causa di eventi accidentali o naturali
- **RISERVATEZZA**: ridurre il rischio di accesso improprio e all'utilizzazione da parte di soggetti non autorizzati; occorre prevedere meccanismi di autenticazione
- **DISPONIBILITA'**: ridurre il rischio di impedimento agli utenti autorizzati di fruire del sistema o di accedere alle informazioni

Misure minime da utilizzare nel caso di trattamenti con strumenti elettronici (art. 34 - Codice della Privacy)

- **autenticazione** informatica;
- adozione di procedure di **gestione delle credenziali** di autenticazione;
- utilizzazione di un **sistema di autorizzazione** (diversi profili di autorizz. per gli incaricati);
- **aggiornamento periodico** dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- **protezione degli strumenti elettronici** e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la **custodia di copie di sicurezza**, il ripristino della disponibilità dei dati e dei sistemi;
- **adozione di tecniche di cifratura** o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Misure minime (art. 34 - Codice della Privacy)

IN SINTESI:

- Prevedere un sistema di autenticazione e autorizzazione che permetta di risalire in caso di controversie legali e di utilizzo non conforme al responsabile delle azioni dannose;
- Il sistema dovrà essere mantenuto aggiornato sia per quanto riguarda l'hardware che il software;
- Predisporre un sistema per il ripristino dei dati persi (Disaster Recovery Plan).

Autenticazione

- Accesso tramite username e password o budge pass ecc.
- Robustezza della password
- Scadenza password ogni 6 mesi (3 mesi per i dati sensibili)
- Istruzioni agli incaricati per non lasciare incustoditi gli strumenti elettronici quando si allontanano dalle loro postazioni e per assicurare la diligente segretezza delle credenziali di accesso o la custodia dei dispositivi

La scuola a prova di privacy

(Vademecum del Garante per la protezione dei dati personali)

Informativa

Tutte le scuole hanno l'obbligo di far conoscere agli interessati (studenti, famiglie, professori, etc.) como vengono trattati i loro dati.

Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali o quelli previsti dalla normativa.

Per tali trattamenti, non sono tenute a chiedere il consenso degli studenti.

I dati sensibili e giudiziari devono essere trattate con estrema cautela, nel rispetto di specifiche norme di legge.

Esempi di uso dei dati sensibili

- I dati sulle **origini razziali ed etniche** possono essere trattati per favorire l'integrazione degli alunni stranieri.
- I dati sulle **convinzioni religiose** possono essere utilizzati per la fruizione dell'insegnamento della religione cattolica o delle attività alternative.
- I dati sullo **stato di salute** possono essere trattati per l'adozione di specifiche misure di sostegno per gli alunni disabili o DSA, per gestire le assenze per malattia per partecipare alle attività sportive.
- Le **opinioni politiche** possono essere trattate per garantire la costituzione e il funzionamento degli organismi di rappresentanza.
- I **dati di carattere giudiziario** possono essere utilizzati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione.

Violazione della privacy

In caso di violazione della privacy, l'interessato può presentare:

- al Garante un'apposita **segnalazione** (gratuita) o un **reclamo** (atto circostanziato con pagamento dei diritti di segreteria) ;
- **ricorso** al Garante o in alternativa può rivolgersi all'autorità giudiziaria ordinaria, quando il titolare del trattamento non abbia dato adeguato riscontro alla richiesta dell'interessato di esercitare i propri diritti.

Vita dello studente

- I **moduli di iscrizione** non possono includere la richiesta di informazioni personali eccedenti e non rilevanti per il perseguimento di tale finalità
- Non lede la privacy l'insegnante che assegna ai propri alunni le svolgimento di **temi in classe** riguardanti il loro mondo personale e familiare.
- Gli **esiti degli scrutini e degli esami di Stato** sono pubblici. Il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap o con DSA non va inserito nei tabelloni.
- Evitare di inserire, nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari, **dati personali che rendano identificabili gli alunni** coinvolti in casi di bullismo o in altre vicende particolarmente delicate.

Vita dello studente

- Fare attenzione a chi ha accesso ai **nominativi degli allievi con DSA** limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa.
- Su esplicita richiesta degli studenti interessati, le scuole secondarie possono **comunicare o diffondere i dati relativi ai loro risultati scolastici** utili a agevolare l'orientamento, la formazione e l'inserimento professionale.

Vita dello studente

la nota n. 10719 del 21 marzo 2017 del Garante per la protezione dei dati personali, in merito al "**documento del 15 maggio**" da redigere per le classi quinte afferma:

"Non si ha alcuna ragionevole evidenza della necessità di fornire alla commissione esaminatrice dati personali riferiti agli studenti in un documento finalizzato ad orientare tale commissione nella redazione del testo della terza prova che sia il più adeguato possibile agli studenti esaminandi".

Uso delle nuove tecnologie

- E’ estremamente importante prestare attenzione in caso si notino comportamenti anomali e fastidiosi su un social network, su sistemi di messaggistica istantanea o su siti che garantiscono comunicazioni anonime (**Cyberbullismo**).
- **L’utilizzo di telefoni cellulari**, di apparecchi per la registrazione di suoni e immagini è in genere consentito per fini personali e nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte.
- Le istituzioni scolastiche hanno la possibilità di regolare o di **inibire l’utilizzo di registratori, smartphone, tablet** e altri dispositivi elettronici all’interno delle aule o nelle scuole stesse.
- Gli studenti non possono diffondere o comunicare i dati di altre persone senza averle prima informate adeguatamente e averne ottenuto l’esplicito consenso.

Uso delle nuove tecnologie

- Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le **recite, le gite e i saggi scolastici**, se raccolte per fini personali.
- Se pubblicate in internet o sui social network occorre ottenere il consenso informato delle persone interessate.
- E' possibile **registrare la lezione** esclusivamente per scopi personali. Per la diffusione su internet occorre il consenso esplicito.
- Gli istituti possono decidere di **regolamentare diversamente o anche di inibire l'utilizzo** di apparecchi in grado di registrare. Deve comunque essere garantito il diritto agli studenti DSA di avvalersi di strumenti compensativi.

Pubblicazioni on line

Per facilitare la corretta applicazione della normativa sono state pubblicate

“Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati”

Graduatorie del personale supplente

- Gli istituti scolastici possono pubblicare sui propri siti internet le graduatorie di docenti e personale amministrativo tecnico e ausiliario (ATA) per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio;
- Devono però contenere solo i dati strettamente necessari all'individuazione del candidato (nome, cognome, punteggio e posizione in graduatoria);
- I dati personali non possono rimanere pubblicati on line per un periodo superiore a quello previsto;
- E' illecita la pubblicazione dei numeri di telefono e degli indirizzi privati dei candidati.

Pubblicazioni on line

- Gli **elenchi messi on line** devono avere carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale.
- Non possono essere pubblicati il nome degli studenti i cui genitori sono in ritardo con il **pagamento della retta o del servizio mensa**.
- Non si possono pubblicare on line, in forma accessibile a chiunque, gli elenchi dei bambini che usufruiscono dei **servizi di scuolabus**, indicando tra l'altro le rispettive fermate di salita-discesa o altre informazioni sul servizio.

Videosorveglianza

- E’ possibile installare un sistema di videosorveglianza negli istituti scolastici se indispensabile per tutelare l’edificio e i beni scolastici;
- le **telecamere che inquadrano l’interno** degli istituti possono essere attivate solo negli orari di chiusura;
- le **aree perimetrali esterne**, al pari di ogni altro edificio pubblico o privato, possono invece essere oggetto di ripresa, per finalità di sicurezza, anche durante l’orario di apertura dell’istituto;
- la presenza di telecamere deve sempre essere **segnalata da appositi cartelli**.

Raccolta di informazioni

Nel caso di raccolta di informazione per attività di ricerca effettuate da soggetti legittimati attraverso questionari, i ragazzi o i genitori nel caso di minori, devono essere preventivamente informati sulle modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate.

Non è possibile utilizzare i dati presenti nell'albo - anche on line - degli istituti scolastici per inviare materiale pubblicitario a casa degli studenti

Cloud computing

proteggere i dati per non cadere dalle nuvole

(Vademecum del Garante per la protezione dei dati personali)

Cos’è il cloud computing

Con il termine cloud computing si intende un insieme di tecnologie che, grazie all’uso di risorse hardware e software distribuite nella rete, permettono di usufruire di servizi di archiviazione ed elaborazione dati.

Modelli di servizi cloud

- **Cloud Infrastructure as a Service - IaaS**: il fornitore del servizio cloud offre gli strumenti hardware e software di base (spazi di memoria, sistemi operativi, programmi di virtualizzazione…) cioè server virtuali remoti che l'utente finale può utilizzare.
- **Cloud Software as a Service - SaaS**: Il fornitore eroga via Internet una serie di servizi applicativi ponendoli a disposizione degli utenti finali (ad esempio fogli di calcolo, elaboratori di testi, gestione protocollo).
- **Cloud Platform as a Service - PaaS**: Il fornitore offre soluzioni evolute di sviluppo software che rispondono alle specifiche esigenze del cliente (ad esempio applicativi per la gestione finanziaria, della contabilità o della logistica).

Quadro giuridico

Manca ancora un quadro normativo aggiornato – in tema di privacy, ma anche in ambito civile e penale - che tenga conto di tutte le novità introdotte dal cloud computing e sia in grado di offrire adeguate tutele nei riguardi delle fattispecie giuridiche connesse all'adozione di servizi distribuiti di elaborazione e di conservazione dati.

Responsabile del trattamento

- La pubblica amministrazione o l'azienda, che trasferisce in tutto o in parte il trattamento sul cloud deve procedere a **designare il fornitore dei servizi cloud "responsabile del trattamento"**.
- Il cliente dovrà sempre prestare molta attenzione a come saranno utilizzati e conservati i dati personali caricati sulla "nuvola": in caso di violazioni commesse dal fornitore, **anche il titolare sarà chiamato a rispondere dell'eventuale illecito**.
- Il Codice della privacy prevede che il titolare eserciti un **potere di controllo nei confronti del responsabile del trattamento** (in questo caso il cloud provider), verificando la corretta esecuzione delle istruzioni impartite in relazione ai dati personali trattati.
- Il titolare del trattamento dovrà quindi **tenere in debito conto anche il luogo dove vengono conservati i dati** e quali sono i trattamenti previsti all'estero, nel caso di trasferimento dei dati fuori dall'Unione Europea.

Fattori da valutare nella scelta del cloud

- Quali sono le misure di sicurezza adottate dal fornitore per proteggere i dati?
- In caso di problemi al collegamento Internet, è comunque possibile continuare a usufruire dei servizi senza l'accesso al cloud? In quanto tempo può essere ripristinato il sistema? Esistono piani di emergenza per i servizi essenziali?
- È possibile che i dati sul cloud possano essere persi o distrutti?
- In quale Stato sono conservati i dati caricati sulla "nuvola"? È possibile scegliere di usufruire di server collocati solo in territorio nazionale o in Paesi dell'Unione europea?
- La tecnologia utilizzata dal fornitore di cloud è di tipo "proprietario"? I dati possono essere esportati facilmente?
- Nel caso in cui si accerti una violazione o la perdita dei dati, il fornitore garantisce un pronto risarcimento del danno?

Linee di indirizzo ed indicazioni in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica

(Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione)

Aspetti legali

(Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione)

La circolare prescrive che chi effettua fotografie o registrazioni e intende divulgarle deve:

- informare la persona interessata (privacy)
- acquisire il consenso espresso (se dati sensibili consenso in forma scritta)

Per l'inosservanza sono previste sanzioni amministrative che vanno da 3.000 a 18.000 euro (per i dati sensibili da 5.000 a 30.000 euro)

Aspetti legali

(Circolare 30 Novembre 2007, Ministero della Pubblica Istruzione)

- I seguenti casi vanno segnalati all'Autorità Giudiziaria (illeciti penali):
- Indebita raccolta, rivelazione e diffusione di immagini attinenti alla vita privata che si svolgono in abitazioni altrui o in altri luoghi di privata dimora (art. 615 bis c.p.)
- il possibile reato di ingiurie, in caso di particolari messaggi inviati per offendere l'onore o il decoro del destinatario (art. 594 c.p.)
- le pubblicazioni oscene (art. 528 c.p.)
- la tutela dei minori riguardo al materiale pornografico (art. 600-ter c.p.; l. 3/8/98, n. 269)

Aspetti legali

Autore del reato minorenne: la competenza è del **Tribunale per i minorenni** e procede la Procura della Repubblica presso tale Tribunale

Autore del reato maggiorenne: la competenza è del **Tribunale ordinario** e procede la Procura della Repubblica presso tale Tribunale

Ruolo degli insegnanti

- PREVENZIONE: fornire educazione e informazione per sensibilizzare i ragazzi:
  - i ragazzi potrebbero ritenere scherzi dei veri e propri reati
  - spesso le vittime del cyberbullismo non si rendono conto delle conseguenze e tendono a minimizzare, “normalizzare” i comportamenti
- l’apparente distacco, creato dal mezzo informatico, lascia meno tempo alla riflessione; il bullo non vede le conseguenze del proprio comportamento
  - gli studenti potrebbero non denunciare il cyberbullismo anche in conseguenza delle sanzioni (requisizione dello smartphone) o per non vedersi ridicolizzati
- Aiutare i ragazzi che si trovano in difficoltà
- Intervenire con chi utilizza le rete impropriamente

Policy di sicurezza

Policy di sicurezza

Documento nel quale sono contenute tutte le disposizioni, i comportamenti e le misure organizzative richieste ai dipendenti e ai collaboratori aziendali (nelle scuole: personale ata, docenti e alunni) per contrastare i rischi informatici

Caratteristiche

- **AGGIORNATE**: sia per riflettere i cambiamenti della rete che del suo uso (sempre più dispositivi mobili)
- **COMPRENDERE TUTTI GLI ASPETTI**: dall'accesso ai locali all'uso della rete
- **BILANCIARE SICUREZZA E PRODUTTIVITA'**: le policy troppo severe ostacolano il lavoro
- **CHIARE**: scritte in modo chiaro, tali da essere facilmente comprese, utilizzare pochi termini tecnici
- **CONOSCIUTE**: se nessuno le conosce sono inutili; informare dei rischi piuttosto che esporre semplicemente le regole
- **ATTUATE**: prevedere controlli a vari livelli e sanzioni per le infrazioni

Alcuni punti da sviluppare

- Utilizzo del Personal Computer e dei dispositivi mobili
- Utilizzo della rete interna
- Gestione delle Password
- Uso della posta elettronica
- Uso della rete Internet e dei relativi servizi
- Protezione antivirus
- Osservanza delle disposizioni in materia di Privacy
- Sanzioni
- Aggiornamento e revisione

Alcuni esempi trovati in rete

AZIENDE

- Esempio di regolamento aziendale (napolifirewall.com)
- Policy strumentazioni informatiche (daycoeurope.com)
- Regolamento informatico (assoprivacy.net)

SCUOLE

- icviatrionfale.gov.it
- icsocrate.it
- iiscremona.gov.it
- comprensivocassino1.gov.it