REPUBBLICA ITALIANA **REGIONE SICILIA**

ISTITUTO D' ISTRUZIONE SECONDARIA Statale
"Filippo Re Capriata" LICATA
ITC- **Amministrazione, Finanza e Marketing** – Art. "Sistemi Informativi Aziendali";
IPSAR- **Servizi per l'enogastronomia e l'ospitalità alberghiera**- Art. "Enogastronomia, Servizi di sala e di vendita, Accoglienza Turistica"-
Corso Serale "Progetto Sirio"- **CTP - EDA**
C.F.: 81000810846 telefono (0922) Presidenza 891158 - Fax 891673; Segreteria 891227 – fax 893363
http://www.recapriata.it - E-Mail: agis013006@istruzione.it; Presidenzapresid.itc.licata@tin.it

---

Circ. n.° 89 **Licata lì, 25.01.2012**

A tutto il **Personale scuola**
Albo Scuola

OGGETTO: Sicurezza a scuola, la protezione dei dati personali (privacy). La sicurezza nei laboratori di informatica e la videosorveglianza.

In relazione alla **sicurezza nelle scuole** (Circ. n.° 28, del 06.10.2011, prt.n.° 5578/ C 52), vanno presi in considerazione anche i seguenti due ambiti di attività:

1. quello nel quale vengono trattati **dati personali** di alunni, genitori e personale della scuola. Si pongono, in questo ambito, i **problemi della protezione** di tali dati e della conformità del loro trattamento alla normativa vigente in materia, nonché quelli della **sicurezza e della protezione delle risorse informatiche** utilizzate nel trattamento;
2. quello che comporta l'**utilizzo delle risorse informatiche** delle scuole da parte degli alunni (ma non solo). In tale ambito si pongono i problemi:
   a. della **protezione dei minori da contenuti pedo-pornografici** diffusi attraverso Internet;
   b. della prevenzione di violazioni della normativa sulla **tutela dei diritti di autore**, che si possono verificare nello scambio di dati tra computer o nell'uso di **software** non coperto da licenza d'uso.

La protezione dei dati personali e la sicurezza delle risorse informatiche fanno parte del Contesto normativo:

- **a.** *Codice in materia di protezione dei dati personali* (D.Lgs. 30 giugno 2003, n. 196), di seguito denominato "Codice
- **b.** Disciplinare Tecnico allegato B al D.Lgs. 30 giugno 2003, n. 196;
- **c.** *Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione* (D.M. 305 del 7 dicembre 2006)
- **c. Gazzetta Ufficiale n.° 99 del 29 aprile 2010, il nuovo Provvedimento generale in materia di videosorveglianza del' 8 aprile 2010;** tale provvedimento sostituisce il precedente Provvedimento Generale del 29 aprile 2004. In tale quadro di regole dettate per gli istituti scolastici, il Garante ha precisato che l'eventuale installazione di sistemi di sorveglianza presso Istituti scolastici deve garantire " il diritto dello studente alla riservatezza" (art. 2, c. 2, del DPR n.° 249/ 1998), prevedendo opportune cautele (server registrazione non accessibile, telecamere solo in are esterne o punti particolari interni, ect. In tale situazione, può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle aree interessate (segnalando con la cartellonistica "AREA VIDEOSORVEGLIATA" ed attivando <in particolare>gli impianti negli orari di chiusura.

Buone pratiche suggerite

La normativa in materia definisce molto dettagliatamente le pratiche che devono essere adottate in questa materia, obbligando i soggetti che trattano i dati all'adozione di numerose

"misure"; l'inadempienza di tali obblighi fa scattare sanzioni anche gravi di tipo penale e amministrativo.
Sul **piano relazionale** vanno adottate tutte le **misure atte a informare** sui loro **diritti** i soggetti protetti dal Codice, ovvero le persone fisiche, le persone giuridiche, gli enti o le associazioni cui si riferiscono i dati personali; questi soggetti sono sinteticamente definiti come *"interessati"* (Codice, articoli dal 7 al 10). Ciò si deve concretizzare nella stesura e nella consegna di opportuni documenti di ***"informativa agli interessati"*** (Codice, art. 13). Ricordiamo che, all'interno delle scuole, la nozione di *"interessato"* definita dal Codice all'art. 4 comprende gli alunni, i componenti delle loro famiglie che hanno relazione con la scuola, il personale scolastico e tutti i soggetti che a qualsiasi titolo intrattengono rapporti con la scuola stessa (ad esempio, per la fornitura di beni e di servizi, per progetti di collaborazione attraverso convenzioni, ecc.).
I diritti degli *"interessati"* sono di notevolissima ampiezza e profondità e sono particolarmente tutelati dalla normativa: oltre alle finalità del trattamento e agli estremi identificativi di chi lo esegue, l'interessato ha diritto a conoscere la struttura della base dati all'interno della quale i dati stessi sono conservati; egli può richiedere, senza particolari formalità, la modifica o l'integrazione dei dati che lo riguardano e può opporsi, per motivi legittimi, al trattamento. Può, inoltre, opporsi al trattamento per fini commerciali dei propri dati, senza dover motivare la sua volontà. **L'interessato non ha bisogno di particolari formalità per esercitare i suoi diritti: basta anche la semplice richiesta verbale**, alla quale deve essere dato *"idoneo riscontro senza ritardo"* (Codice, art. 8).
Sul **piano gestionale**, vanno adottate tutte le **misure di sicurezza** volte alla riduzione dei *"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."* (Codice, art. 31). L'adozione delle misure di sicurezza è importante anche ai fini della difesa in caso di eventuali danni cagionati per effetto del trattamento dei dati personali. Il Codice, infatti (art. 15), equipara il trattamento dei dati all'esercizio delle *"attività pericolose"* previste dall'art. 2050 del Codice Civile. Ciò comporta che il soggetto ritenuto responsabile è tenuto al risarcimento, nella misura che sarà prevista caso per caso dal giudice, a meno che non provi di "*avere adottato tutte le misure idonee a evitare il danno".*
In ogni caso, vanno messe in opera le **misure minime di sicurezza** previste dal Codice **per chi tratta dati personali con l'ausilio di computer** (articoli dal 33 al 36 e Disciplinare Tecnico allegato B), Prot. 247/ C 52 del 18.01.2012. Tale obbligo – la cui inosservanza è sanzionata penalmente (Codice, art. 169) - riguarda praticamente la totalità dei soggetti che trattano dati e, quindi, tutte le scuole. Si tratta di un complesso di misure raggruppabili, in linea di massima, in due categorie:

- misure di carattere **organizzativo**; consistono sostanzialmente nella stesura e nell'aggiornamento periodico (entro il **31 marzo di ogni anno**) del cosiddetto "*Documento programmatico sulla sicurezza"* (DPS). Alla stesura di tale documento si perviene attraverso:
  - la **ricognizione sui tipi di dati trattati** e delle operazioni eseguibili su di essi, con particolare attenzione a quelli oggetto del Regolamento dati sensibili;
  - la **definizione dei ruoli interni** rispetto al trattamento dei dati personali (individuazione del *"titolare"*, del *"responsabile"*, degli *"incaricati"*);
  - l'**analisi dei rischi** che incombono sui dati e, in relazione a questi, l'individuazione degli **opportuni provvedimenti per prevenirli**.
- misure di carattere **tecnico**, che permettano non solo di evitare accessi non autorizzati ai dati, ma anche di garantire la loro integrità e quella degli strumenti adoperati per trattarli, ovvero i computer e le reti interne. Sono descritte dettagliatamente nel Disciplinare Tecnico. In sintesi riguardano:
  - la **protezione degli accessi** ai computer, attraverso procedure di autenticazione informatica;
  - la **protezione dei computer** rispetto a trattamenti illeciti (ad esempio la diffusione di dati protetti), che possono verificarsi anche a seguito dell'uso consapevole o inconsapevole di **programmi informatici dannosi**. Da un punto di vista pratico, ci si dovrà dotare di adeguati software che proteggano i computer e le reti interne alla scuola in modo automatico e continuativo (*antivirus, antispyware, antidialer, firewall*). Questi software normalmente dispongono di archivi interni contenenti i "nomi" e le

caratteristiche tecniche dei software dannosi, archivi che possono essere aggiornati in modo automatico per far fronte alle nuove "minacce" che quotidianamente vengono immesse sulle reti di comunicazione dati. Vanno inoltre aggiornati in continuazione i sistemi operativi presenti sulle macchine (o sui server di Rete);

- la custodia dei dati, le copie di sicurezza, il **ripristino dei dati e dei sistemi** in caso di loro perdita parziale o totale.

Una misura di "buon senso", particolarmente consigliabile per le scuole e la nostra, è inoltre quella di progettare l'architettura del proprio sistema informatico (cosa che si sta facendo) prevedendo la **distribuzione delle risorse informatiche** tramite **due reti**, fra loro fisicamente separate:

- la rete **didattica**, che raggruppa l'insieme dei computer presenti nel laboratorio (o nei laboratori) della scuola;
- la rete **amministrativa**, che raggruppa i computer destinati a tutte le altre attività (gestione archivi anagrafici, contabilità e finanza, protocollo corrispondenza, ecc.).

Le norme citate prevedono l'**obbligo di interventi formativi specifici per le persone incaricate del trattamento** (praticamente tutto il personale scolastico). La formazione deve riguardare sia gli aspetti generali (profili più rilevanti della normativa, responsabilità, ecc.) che le misure concretamente messe in atto nella struttura. Ma poiché i computer sono usati da tutti - alunni, docenti, personale, famiglie - crediamo che le misure di sicurezza avranno tanta maggiore efficacia quanto più esse saranno accompagnate da **interventi di formazione adeguati alla tipologia e all'età dei destinatari**.

La protezione dei minori da contenuti pedo-pornografici

Contesto normativo:

- *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet.* (Legge 6 febbraio 2006, n. 38, nel seguito indicata come "legge 38"). Il testo è reperibile in Rete all'indirizzo http://www.giustizia.it/cassazione/leggi/l38_06.html#TESTO
- *Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare al fine di impedire l'accesso ai siti segnalati dal Centro nazionale per il contrasto della pedopornografia* (Decreto Interministeriale 29 gennaio 2007, nel seguito indicato come "Decreto Interministeriale"). Il testo è reperibile all'indirizzo http://www.comunicazioni.it/it/index.php?IdPag=1177

Licata lì, **25.01.2012**

Il Dirigente Scolastico
Prof. Arch. **Sergio Coniglio**