ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

Sicurezza informatica e Privacy nella scuola

Antonio Piva, David D'Agostini

1. Introduzione

Accade spesso che fatti di cronaca riportino alla ribalta il tema della privacy nelle scuole ponendo interrogativi sulla liceità di determinate prassi o di certi comportamenti. Si pensi, a titolo esemplificativo, all'affissione dei voti alla fine dell'anno scolastico, oppure alla pubblicazione di dati relativi ad alunni disabili.
Si tratta di problematiche di indubbio impatto sociale e di forte interesse, non solo per gli studiosi della materia, ma soprattutto per le famiglie e i genitori che, sin dall'entrata in vigore della normativa sul trattamento dei dati personali[1] hanno dimostrato una marcata sensibilità per la riservatezza dei propri figli. Ciò non può che sottolineare la necessità di sviluppare una costante attenzione nei confronti della legislazione per evitare possibili infrazioni e per stimolare un atteggiamento consapevole nei confronti di un argomento tanto sentito e attuale.
Esaminiamo, pertanto, alcune ipotesi di applicazione della normativa sulla privacy con specifico riferimento agli istituti scolastici, prendendo spunto anche dai casi più comuni portati in questi anni all'attenzione del Garante, non prima di aver illustrato le principali disposizioni di legge che disciplinano questo ambito.

2. Norme

Come noto, a far data dal 1° gennaio 2004, la principale fonte del diritto in materia di protezione dei dati personali è il d.lgs. 196/03 meglio noto come "*Codice della privacy*"; tale decreto, che ha abrogato e sostituito la precedente legge 675/96, dopo aver dettato le disposizioni generali nella prima parte, nella seconda si occupa di specifici settori tra i quali l'istruzione.
In particolare l'art. 95 riconosce alle finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, il "rilevante interesse pubblico" richiesto ai soggetti pubblici per il trattamento di dati personali sensibili o giudiziari. Si consideri che la quantità di dati sensibili trattati nell'ambito scolastico è davvero notevole: basta pensare ai dati sullo stato di salute, sul credo religioso, sulle origini razziali ed etniche che ogni scuola raccoglie, elabora e conserva.
Vale la pena ricordare, inoltre, che la titolarità del trattamento di dati personali spetta all'istituto scolastico frequentato dall'alunno, stante l'autonomia funzionale, didattica, organizzativa e di ricerca, sperimentazione e sviluppo ad esso riconosciuta (si veda in proposito il d.P.R. 8 marzo 1999, n. 275).

[1] Il 6 maggio 1997 è entrata in vigore la Legge 675/96 che, attuando la direttiva comunitaria 46/95/CE, per la prima volta introduceva nell'ordinamento italiano la disciplina della tutela delle persone rispetto al trattamento dei dati personali. Ampia trattazione a questo tema è stata riservata, in occasione del decimo anniversario della normativa stessa, nel numero 22 del giugno 2007 di Mondo Digitale, al quale si rinvia.

Ruquadro 1

Le schede del regolamento ministeriale

Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro
Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari
Scheda n. 3 – Organismi collegiali e commissioni istituzionali
Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico
Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione
Scheda n. 6 – Scuole non statali (relativamente agli eventuali dati sensibili e giudiziari che emergono nell'attività di vigilanza e controllo effettuata dall'Amministrazione e dai dirigenti scolastici delle scuole primarie incaricati della vigilanza sulle scuole non statali autorizzate)
Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso

In buona sostanza, ogni scuola -al pari di ogni altra Pubblica Amministrazione- può legittimamente trattare tutti i dati comuni (per esempio, i dati anagrafici) necessari per lo svolgimento delle proprie funzioni istituzionali; mentre il trattamento dei dati sensibili e giudiziari degli alunni (in conformità a quanto disposto dagli art. 20 e 21) viene consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici con regolamento adottato in conformità al parere espresso dal Garante per la protezione dei dati personali.
In ottemperanza a tale previsione, il Ministero dell'istruzione, dell'università e della ricerca in data 7 marzo 2006 ha presentato al Garante lo schema di regolamento concernente le tipologie di dati sensibili e giudiziari, nonché delle operazioni eseguibili a cura del Ministero stesso e delle istituzioni scolastiche ed educative pubbliche.
Nel regolamento, successivamente approvato con Decreto ministeriale n. 305 del 7 dicembre 2006[2], viene chiarito, tra l'altro, che i dati sensibili degli studenti possono essere usati solo per specifiche finalità: i dati sulle origini razziali ed etniche possono essere trattati solo per favorire l'integrazione degli alunni con cittadinanza non italiana; i dati relativi alle convinzioni religiose solo per garantire la libertà di credo religioso; i dati sulla salute solo per l'erogazione del sostegno agli alunni disabili, dell'insegnamento domiciliare e per il servizio di refezione; le informazioni sulle convinzioni politiche solo per la costituzione e il funzionamento delle consulte e delle associazioni degli studenti e dei genitori; i dati di carattere giudiziario sono trattati solo per assicurare il diritto allo studio anche a ragazzi sottoposti a regime di detenzione.
Il testo del Regolamento, molto snello ed essenziale, è suddiviso in 3 articoli nei quali si richiama il menzionato d.lgs. 196/03 e si sottolinea l'obbligo di trattare dati sensibili e giudiziari solo previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato (art. 2).
Sono parte integrante del Regolamento 7 schede che individuano tutti i dati sensibili e giudiziari trattati dalle scuole, suddividendoli in ambiti [riquadro 1].
Ogni scheda consente alle scuole di individuare chiaramente i trattamenti consentiti, le finalità di rilevante interesse pubblico perseguite, le fonti normative, i soggetti esterni pubblici e privati a cui è possibile comunicare i dati, i tipi di dati trattati. Inoltre è molto importante non perdere di vista il contesto in cui il trattamento si svolge descritto in maniera riassuntiva dalle schede medesime.
Per esempio per le operazioni propedeutiche di avvio dell'anno scolastico (scheda n.4) non è consentito il trattamento dei dati relativi alle convinzioni filosofiche, che invece è consentito per la gestione del contenzioso e procedimenti disciplinari (scheda n.2).
Agli effetti pratici, le schede risultano estremamente importanti dal punto di vista operativo e costituiscono una "guida" obbligatoria cui le scuole non possono derogare. A titolo esemplificativo, nella gestione del rapporto di lavoro (scheda n. 1), i dati idonei a rilevare l'adesione al sindacato possono essere trattati solo per operare la ritenuta sindacale e per l'esercizio dei diritti sindacali: un trattamento per fini diversi sarebbe illegittimo.
L'adozione del Regolamento da parte del Ministero, pur non richiedendo una successiva adozione da parte delle scuole (obbligate per legge a rispettarlo), ha comportato la necessità di rivedere e modificare alcuni atti già adottati e i procedimenti interni alla scuola seguiti nel trattamento dei dati sensibili e giudiziari.
Risulta, infatti, necessario che:
- nel Documento Programmatico per la Sicurezza la parte relativa all'elenco dei dati personali trattati (punto 19.1 del Disciplinare tecnico contenuto nell'Allegato B al d.lgs. 196/03) sia

[2] Il Decreto risulta pubblicato nella *Gazzetta Ufficiale* n.11 del 15 gennaio 2007.

adeguata alle prescrizioni e indicazioni contenute nelle schede;

- il Titolare del trattamento (vale a dire il dirigente scolastico) adegui la nomina del Responsabile del trattamento richiamando le prescrizioni contenute nel Regolamento e fornendo gli indirizzi per la loro attuazione nei procedimenti amministrativi e nella gestione delle attività;
- il Responsabile del trattamento (per la parte relativa al personale posto alle sue dirette dipendenze) e il Titolare del trattamento (per il personale docente) adeguino le designazioni degli incaricati del trattamento, modificando, se necessario, le autorizzazioni concesse e le linee guida emanate;
- la conoscenza del Regolamento sia oggetto dell'attività di formazione del personale incaricato prevista dal d.lgs.196/03;
- nell'informativa agli interessati si faccia riferimento al rispetto da parte della scuola alle prescrizioni del Regolamento;
- si dia evidenza dell'aggiornamento del Documento Programmatico per la Sicurezza nella relazione al programma annuale.

Il Garante, dal canto suo, ha ribadito recentemente[3] la necessità di delimitare la consultazione diretta di banche dati e le interconnessioni tra sistemi informativi delle scuole, in quanto tali operazioni potrebbero determinare un'ingiustificata circolazione dei dati degli interessati. In particolare l'Autorità ha disposto che i dati vengano trasmessi mediante un diverso tipo di collegamento informatico o telematico che consenta agli altri uffici della Scuola e ad altri soggetti pubblici di consultare i dati solo su richiesta.

A tal proposito, trova applicazione l'art. 96 del Codice della privacy, laddove è previsto che "*al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti*"; possono, inoltre, essere comunicati anche altri dati personali degli alunni, purché non siano sensibili o giudiziari, e abbiano rilevanza in relazione alle predette finalità.

La norma in chiusura richiama espressamente il decreto del Presidente della Repubblica 24 giugno 1998, n. 249 (*Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria*) e la tutela del diritto dello studente alla riservatezza ivi sancita.

3. Casi

In questi anni il Garante si è pronunciato su molteplici ricorsi relativi all'ambito scolastico a volte anche per sfatare alcune convinzioni erronee come il fatto che i voti dovessero rimanere segreti ed essere consegnati in busta chiusa agli studenti. Gli stessi risultati degli scrutini finali -che, peraltro, non sono dati sensibili- devono essere pubblicati anche dopo l'avvento della normativa sulla *privacy*, essendo ciò previsto da una specifica disciplina in materia e rispondendo a principi di trasparenza.

Il 9 febbraio 2004, un'ordinanza del Ministro per l'istruzione ricorda che anche i punteggi attribuiti come crediti scolastici a ciascun alunno sono pubblicati nell'albo degli istituti, unitamente ai voti conseguiti in sede di scrutinio finale. In ciascun albo va anche pubblicato l'esito degli esami, "*con la sola indicazione della dizione non promosso nel caso di esito negativo*"; analoghe soluzioni sono state indicate in passato in varie ordinanze ministeriali del 2001 e del 2003.

Parimenti non esiste alcun provvedimento del Garante che proibisce agli alunni di rendere nota la fede religiosa o che ostacola le soluzioni da tempo in atto per la partecipazione o meno degli alunni all'ora di religione. Il necessario rispetto della volontà di ciascuno di mantenere riservate alcune informazioni sulla propria persona, infatti, non va confuso con la libertà, costituzionalmente protetta, di ognuno di manifestare liberamente le proprie convinzioni, anche di natura religiosa.

Un'importante tematica, alla quale l'Autority ha dedicato un provvedimento[4] *ad hoc*, è il cosiddetto "Portfolio", lo strumento didattico redatto

[3] Parere 7 febbraio 2008 (relatore Giuseppe Fortunato) sullo schema di regolamento per il trattamento di dati sensibili e giudiziari predisposto dalla Scuola superiore della pubblica amministrazione locale - Bollettino del n. 92/febbraio 2008 (doc. web n. 1491594 nel sito www.garanteprivacy.it).

[4] Si tratta della prescrizione del 26 luglio 2005 pubblicata nel Bollettino del n. 63/luglio 2005 (doc. web n. 1155253 nel sito www.garanteprivacy.it).

dall'insegnante per ciascun alunno che, oltre ai progressi formativi ed educativi dello studente, documenta interessi, attitudini, aspirazioni personali che emergono nel corso degli anni scolastici. Il *Portfolio* è compilato e aggiornato (nella scuola d'infanzia) dai docenti di sezione, ovvero (nella scuola primaria e secondaria di primo grado) dal docente *coordinatore-tutor* dell'alunno in collaborazione con altri docenti, alunni e loro genitori, i quali possono apportarvi alcune annotazioni (*allegati A, B*) e *C*) *del citato decreto*).
I genitori di alunni hanno lamentato possibili violazioni della riservatezza derivanti dalle modalità con cui istituti scolastici pubblici e privati trattano dati di carattere personale in relazione al *Portfolio*.
A fronte di tali segnalazioni il Garante è intervenuto precisando che il trattamento di dati personali effettuato mediante il *Portfolio* è consentito solo per raggiungere le finalità individuate direttamente dalla predetta legislazione di riforma (*d.lgs. n. 59/2004*), ovvero per valutare l'apprendimento e il comportamento degli studenti e per certificare le competenze acquisite; non possono, quindi, essere perseguite ulteriori finalità attinenti, per esempio, all'individuazione del profilo psicologico degli alunni o alla raccolta di informazioni sul loro ambiente sociale e culturale di provenienza.
Ciò premesso l'Autorità ha prescritto a tutti gli istituti scolastici di adottare idonee misure volte a favorire il rispetto della riservatezza, dell'identità e della protezione dei dati personali, considerata la quantità, la varietà e la delicatezza delle informazioni che possono essere inserite nel *Portfolio* e l'ingente numero dei minori e familiari interessati [riquadro 2].
Sono, infine, di indubbio interesse le problematiche relative alla tenuta del registro di classe, sia cartaceo che elettronico: considerati i noti principi di pertinenza e non eccedenza e di necessità a cui deve soggiacere ogni trattamento di dati personali, la scuola deve valutare attentamente quali informazioni annotare nel registro.
Il Decreto Ministeriale 5 maggio 1993 e l'Ordinanza Ministeriale n. 236 del 1993 indicano le funzioni che presiedono alla tenuta del registro di classe che, in linea di massima, ha lo scopo di tenere traccia delle notizie più importanti relative alla vita quotidiana della classe (assenze, lezioni, compiti, attività ecc.).
Da ciò consegue che, per la sua natura di documento volto a rendere conoscibili alcune informazioni a beneficio di tutta la classe, non è il caso che il registro contenga dati personali di natura sensibile (né, tanto meno, che venga usato per conservare certificati medici). Per lo stesso motivo, risulta assai difficile pensare che il registro di classe possa essere nascosto agli studenti i quali sono i primi interessati a conoscere molte delle informazioni contenute nel medesimo.
Quanto al registro elettronico appare opportuno ricordare l'obbligo legislativo di adottare le misure minime di sicurezza (codici personali di autenticazione, sistemi di protezione da agenti recanti danno, da intrusioni non autorizzate e sistemi di salvataggio periodico e di ripristino dei dati).

Ruquadro 2

Le misure prescritte per il *Portfolio*

1 - Predisporre un modello di *Portfolio*
2 - Informare gli interessati
3 - Fornire ai docenti istruzioni per la compilazione
4 - Ridurre l'inserimento di dati sensibili degli alunni
5 - Designare gli incaricati che possono accedere
6 - Garantire la sicurezza dei dati
7 - Garantire l'esercizio dei diritti in materia di privacy
8 - Conservare i dati per brevi periodi
9 - Rilasciare il *Portfolio* all'interessato

4. Misure di sicurezza

Gli adempimenti inerenti alla sicurezza dei dati e dei sistemi informatici (art. 31 del *Codice della privacy*) sono finalizzati a ridurre al minimo i rischi di distruzione o perdita dei medesimi, ovvero di accesso non autorizzato, di trattamento non consentito o non conforme alla finalità della raccolta; si prevede inoltre l'adozione di idonee misure di sicurezza in relazione al progresso tecnologico ed alle specifiche caratteristiche del trattamento di dati trattati.
Le prescrizioni sulla sicurezza dei dati e dei sistemi (*art. 34 del Codice, nonché il già citato l'Allegato B - Disciplinare tecnico in materia di misure minime di sicurezza*) comprendono tra le modalità tecniche da adottare in caso di trattamento con l'ausilio di strumenti elettronici, il ricorso a sistemi di autenticazione informatica mediante codice di identificazione personale (*username*) e parola chiave riservata (*pas-*

sword)[5], ovvero tramite dispositivi di autenticazione, per esempio, *token, smart card*, in possesso a uso esclusivo degli incaricati – in ambito scolastico insegnanti, personale tecnico e amministrativo.
Viene introdotto l'utilizzazione di un sistema di profili di autorizzazione, per ciascun utente o per classi omogenee[6], in modo da limitare l'accesso ai solo i dati necessari, che deve essere periodicamente aggiornato verificando la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.
I dati personali, inoltre, devono essere protetti contro il rischio di intrusione (per esempio, mediante *firewall* e programmi denominati *Intrusion Detection System*, IDS) e dall'azione di virus tramite idonei strumenti elettronici da aggiornare costantemente; vengono anche previsti l'aggiornamento periodico dei programmi finalizzati a prevenire la vulnerabilità dei sistemi e a correggerne i difetti (per esempio, *Patch* e nuove versioni) da effettuarsi almeno annualmente ed il salvataggio periodico dei dati (*back-up*) con frequenza almeno settimanale.
Il documento programmatico sulla sicurezza deve contenere l'elenco dei trattamenti, la distribuzione dei compiti e delle responsabilità, l'analisi dei rischi sui dati, le misure di sicurezza da adottare per l'integrità e disponibilità dei dati, la protezione delle aree e dei locali, la modalità di ripristino (si pensi al *disaster recovery*), il piano di formazione del personale incaricato al trattamento[7].
Per quanto concerne l'utilizzo della Videosorveglianza da parte delle Istituzioni Scolastiche ci si riferisce al provvedimento del Garante del 29 aprile 2004[8] e ai Principi di liceità, di necessità e di proporzionalità: l'eventuale installazione di sistemi di videosorveglianza presso istituti scolastici deve garantire "*il diritto dello studente alla riservatezza*" (*art. 2, comma 2, d.P.R. n. 249/1998*) e tenere conto della delicatezza dell'eventuale trattamento di dati relativi a minori. A tal fine, se può risultare ammissibile il loro utilizzo in casi di stretta indispensabilità[9] (per esempio, a causa del protrarsi di atti vandalici), gli stessi devono essere circoscritti alle sole aree interessate ed attivati negli orari di chiusura degli istituti, regolando rigorosamente l'eventuale accesso ai dati. In relazione al principio di necessità, gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili; ciascun sistema informativo e il relativo programma informatico dovrebbero essere configurati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (esempio, programma configurato in modo da consentire solo riprese generali che escludano la possibilità di ingrandire le immagini). Il software va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati[10]; ed anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario - e predeterminato - a raggiungere la finalità perseguita[11].
Il sito scolastico utilizzato per promuovere le proprie attività, se offre agli utenti anche la possibilità di registrarsi tramite appositi moduli (*form*), per consentire poi di comunicare successivi aggiornamenti dell'offerta didattica o delle iniziative collaterali, deve prevedere adeguata e preventiva informativa contenente tutti gli elementi indicati all'art. 13 del Codice della Privacy (modalità di trattamento, finalità, titolare, re-

[5] Parola chiave riservata e conosciuta solamente dall'incaricato, modificata da quest'ultimo al primo utilizzo e successivamente almeno ogni sei mesi; deve essere composta da almeno otto caratteri e non contenere riferimenti agevolmente riconducibili all'incaricato.

[6] Per scuole si pensi agli studenti, personale ATA (in relazione agli specifici incarichi) o corpo docente.

[7] Inoltre, per i dati personali idonei a rilevare lo stato di salute e la vita sessuale, le modalità di cifratura e di separazione dei dati dalle altre informazioni personali dell'interessato.

[8] Si veda anche il Provvedimento a carattere generale - 29 novembre 2000 – denominato Videosorveglianza - Il decalogo delle regole per non violare la privacy.

[9] Gli interessati devono essere preventivamente informati che stanno per accedere o che si trovano in un area video sorvegliata. Si deve perciò utilizzare adeguata informativa contenente, in forma sintetica, gli elementi del'art. 13 del Codice della Privacy (allo scopo può essere utile riferirsi al facsimile di informatica allegato al citato provvedimento emesso da Garante sulla videosorveglianza).

[10] Restano di competenza dell'autorità giudiziaria o di polizia le iniziative intraprese a fini di tutela dell'ordine pubblico o di individuazione di autori di atti criminali (per esempio, spacciatori di stupefacenti, adescatori ecc.).

[11] La conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività.

sponsabile, comunicazione, diritti e modalità di esercizio degli stessi ecc.), chiarendo la natura obbligatoria o facoltativa del conferimento dei dati personali[12]. Il Sito dovrà inoltre, in relazione al d.lgs. 82/2005 (*Codice dell'Amministrazione Digitale*), contenere per esempio anche l'organigramma, l'elenco completo delle caselle di posta elettronica istituzionali, i riferimenti del titolare e dei responsabili del trattamento.

Per quanto riguarda l'utilizzo degli strumenti informatici da parte del personale ed in particolare dei laboratori informatici da parte degli studenti, è opportuno predisporre e divulgare un apposito regolamento vietando per esempio la navigazione in siti contro la morale e/o potenzialmente pericolosi[13], il download di file musicali o programmi per elaboratori senza specifica autorizzazione. Piuttosto che utilizzare un controllo a posteriori, magari analizzando i log contenuti nei sistemi[14], tenendo conto della delicatezza dell'eventuale trattamento di dati relativi a minori è bene considerare l'utilizzo di appositi programmi di *web filtering* al fine di implementare una modalità di controllo preventiva. Infatti le operazioni esercitabili agli utenti dei sistemi possono essere limitate ai siti, alle pagine ed alle operazioni lecite inserendo nelle *black list* dei citati programmi i siti indesiderati, gli indirizzi IP o particolari URL, oppure le parole chiave indesiderate (non consentendo così agli utenti di visualizzare le pagine web con contenuti dubbi).

La mancata ottemperanza alle disposizioni indicate nel codice della privacy comporta conseguenze sotto diversi profili[15]: sanzioni amministrative, risarcimento del danno, illeciti penalmente rilevanti.

I rischi pertanto impongono non una mera e statica adozione delle misure sulla sicurezza ma anche, il costante aggiornamento e controllo delle stesse come per altro previsto dall'art. 34 e all'allegato B del Codice della privacy.

L'identificazione e l'aggiornamento costante dei processi riguardanti il controllo della sicurezza fisica, logica ed organizzativa[16] al fine di garantire la riservatezza, l'analisi dei rischi per l'identificazione delle misure idonee di sicurezza, prevista dal *Documento Programmatico sulla Sicurezza*, la gestione di opportune procedure ed istruzioni operative frequentemente aggiornate[17], il monitoraggio dei processi aziendali anche attraverso costanti verifiche interne tecnico-organizzative e audit, come previsto dalle norme volontarie internazionali ISO 9001, riguardanti la qualità, o più specificatamente dalle norme ISO/IEC 27001, riguardanti i Sistemi di Gestione della Sicurezza delle informazioni, sono utili strumenti per garantire la Sicurezza informatica e Privacy nella Scuola.

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

David D'Agostini avvocato, master in informatica giuridica e diritto delle nuove tecnologie, collabora all'attività di ricerca scientifica dell'Università degli studi di Udine e ha fondato l'associazione "*Centro Innovazione & Diritto*". È componente della Commissione Informatica dei Consigli dell'Ordine del Triveneto, responsabile dell'area "*Diritto & informatica*" della rivista "*Il foro friulano*", membro dell'organo di Audit Interno di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it

[12] Si noti il provvedimento del 31 marzo 2003, con il quale l'Autorità Garante ha sanzionato con una multa il sito web che non aveva informato gli utenti sull'uso dei dati personali raccolti on line.

[13] Si pensi ad armi, sesso, droga, pedofilia ecc.

[14] Se da un lato è un dovere da parte delle Istituzioni scolastiche non consentire (mediante prevenzione) l'utilizzo di materiale illecito e non attinente alle attività scolastiche, dall'altro una mera strategia di controllo a posteriori potrebbe portare, analizzando i log, a violare i Principi di necessità e proporzionalità del Codice della Privacy (mediante operazioni eccedenti rispetto alla finalità); infatti potrebbero portare a conoscere dati personali sensibili (quali per esempio la vita sessuale, stato di saluti, opinioni politiche o convinzioni religione) riguardanti i dipendenti scolastici e gli allievi.

[15] Per una completa trattazione si rinvia al numero 22 del giugno 2007 di Mondo Digitale.

[16] Per il primo aspetto si cita dal controllo dell'accesso ai locali alla custodia dei supporti magnetici; per il secondo protezione delle informazioni e dei sistemi da danni legati a malfunzionamenti tecnologici accidentali o volontari; per il terzo gestione della sicurezza, policy, linee guida e procedure, audit.

[17] Dando corpo alla formazione e sensibilizzazione ricorrente, a tutto il personale ed agli Studenti, sull'uso dei sistemi e sulle problematiche della sicurezza, attuazione di procedure di gestione delle credenziali di autenticazione, sistema di autorizzazione e gestione dell'ambito di trattamento consentito ai singoli incaricati, protezione da accessi non consentiti, procedure per custodia dei backup e ripristino dei sistemi, adozione ed aggiornamento antivirus, predisposizione e controllo di firewall, piano di disaster recovery.