Aspetti legali e privacy

Introduzione

Quest'ultima sezione dell'introduzione è destinata a presentare in modo succinto i principali aspetti normativi correlati alla gestione delle infrastrutture all'interno di un istituto scolastico, in particolare la tutela della **privacy** e la **licenza d'uso dei software** (a cura di Giusella Finocchiaro).

A questi sono aggiunti alcune tematiche più tecniche che offrono spunto per la messa in opera di strumenti di salvaguardia di alcuni diritti e, in particolare, la **crittografia**, come meccanismo di protezione della riservatezza dei messaggi e i **criteri di accessibilità dei siti Web per i disabili** (a cura di Paola Salomoni).

Per alcune delle tematiche trattate in questa sezione, sono disponibili approfondimenti:

- sulla **crittografia**;
- sulla **privacy**;
- sulle **licenze d'uso del software**;

In questa breve trattazione introdurremo alcuni degli aspetti tecnici, trattando le principali tecniche e procedure per la prevenzione dei problemi e la loro soluzione. È disponibile un approfondimento sulla **sicurezza come forma di prevenzione**, che tratta in modo più specifico le problematiche relative alla sicurezza delle informazioni.

I diritti di utilizzazione economica del software

Secondo il d. lgs. 518/92 http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64BIS, l'autore o il titolare dei diritti di utilizzazione economica dell'opera ha il diritto esclusivo di effettuare:

1. la riproduzione del software permanente o temporanea, totale o parziale;
2. la traduzione, l'adattamento, la trasformazione e ogni altra modificazione del programma;
3. qualsiasi forma di distribuzione al pubblico.

Il legittimo acquirente, invece, può:

1. riprodurre il programma e tradurre, adattare o trasformare il programma solo se tali attività sono necessarie per l'uso del programma conformemente alla sua destinazione, inclusa la correzione degli errori;
2. effettuare una copia di riserva del programma, qualora tale copia sia necessaria per l'uso;
3. osservare, studiare o sottoporre a prova di funzionamento il programma.

http://www.giustizia.it/cassazione/leggi/l633_41.html#ART64TER

Il contratto di licenza

Il d. lgs. detta soltanto le norme generali. Ampio margine è lasciato alla contrattazione fra l'utilizzatore del software e il soggetto che detiene i diritti di utilizzazione economica del software (l'autore del programma o l'impresa produttrice di software alla quale l'autore ha ceduto i propri diritti). Il contratto che in dettaglio regolamenta i diritti e i doveri dell'acquirente e dell'utilizzatore di software è il contratto di licenza d'uso. Questo contratto è un contratto atipico, cioè non regolamentato dal codice civile, e la definizione del contenuto contrattuale è lasciata all'autonomia delle parti contraenti, le quali possono definire i reciproci diritti e doveri a loro discrezione. Infatti, il mercato offre una grande varietà

di contratti, di tipi di licenze, di prezzi, di obblighi e anche di programmi. Pertanto, non si può dare una definizione unitaria dei programmi per elaboratori esistenti né si possono definire tutti i tipi di programmi esistenti, ma si può soltanto fornire una descrizione delle tipologie più diffuse. Ad esempio, per stabilire se una duplicazione è abusiva o meno occorre far riferimento al contratto. Solitamente i contratti di licenza d'uso (cioè i contratti per "comprare" il programma) limitano l'utilizzo del software ad una sola macchina per volta e talvolta la macchina è espressamente individuata nella documentazione contrattuale. Alcuni contratti di licenza d'uso, tuttavia, consentono la riproduzione del programma su un certo numero di macchine. In genere, i contratti standard di licenza d'uso non consentono l'utilizzazione di un programma da più macchine fra loro collegate in rete. Tuttavia, è possibile stipulare contratti di licenza d'uso che consentano di utilizzare il programma su più macchine o in rete (licenze multiple; a forfait; floating license, cioè licenze per utilizzare i programmi in rete ma da un numero di utenti prefissato) o inserire in contratto clausole ad hoc.

Tipologie particolari di licenza

4.1. Open software

Il titolare dei diritti di utilizzazione economica del software può rinunciare ad essi e mettere a disposizioni del pubblico il programma, compreso il codice sorgente, senza richiedere un compenso. La rinuncia ad un diritto è una particolare modalità di esercizio di quel diritto. Sulla base di questo principio si è diffuso il cosiddetto "open software", che consiste di programmi che sono disponibili sia all'utilizzo che alla modifica da parte di soggetti diversi dall'autore . Il contratto di licenza d'uso per open software più diffuso è costituito dal contratto GNU http://www.gnu.org/licenses/licenses.html

4.2. Licenza a strappo

Un particolare contratto di licenza d'uso è costituito dal c.d. contratto a strappo o contratto di licenza a strappo, shrink-wrap license, nell'originaria formulazione statunitense. In questo caso, il programma è confezionato in un involucro, sul quale sono stampate o attraverso il quale è possibile leggere le condizioni contrattuali. L'apertura dell'involucro costituisce accettazione delle condizioni contrattuali predisposte dal produttore. Le condizioni d'uso del programma sono quelle dei contratti di licenza d'uso più diffusi (uso del programma limitato ad una sola macchina, restrizioni alla possibilità di effettuare copie, garanzia limitata ai soli difetti del supporto materiale, esclusione di altre garanzie e responsabilità). L'acquirente che non intenda accettare il regolamento contrattuale può restituire il prodotto e richiedere la restituzione del prezzo pagato, purché non abbia aperto la confezione. In genere, viene richiesto all'acquirente di compilare e spedire al produttore una cartolina che gli consente di ricevere gli aggiornamenti del software e di usufruire delle limitate prestazioni di garanzia accordate dal contratto. La spedizione della cartolina costituisce espressa accettazione del regolamento contrattuale. Il contratto di licenza a strappo si perfeziona, dunque, con l'atto dell'apertura della confezione. Tale atto vale come accettazione. L'art. 1341 c.c. stabilisce che le condizioni generali di contratto predisposte da una parte sono valide nei confronti dell'altra se conoscibili da questa al momento della conclusione del contratto. Dunque, se il regolamento contrattuale è leggibile al momento della conclusione del contratto le condizioni generali di contratto sono da ritenersi valide. L'effettiva conoscenza di esso non ha alcuna rilevanza per il nostro ordinamento, così come non ha alcuna rilevanza l'effettiva conoscenza delle clausole contrattuali al momento della conclusione di un contratto di trasporto, di banca o di assicurazione, ecc. Il regolamento contrattuale è da ritenersi accettato al momento della conclusione del contratto, sempre che esso fosse conoscibile. Perché si possa considerare conoscibile, è necessario che le condizioni generali di contratto siano inserite nella confezione in modo da essere visibili e leggibili dall'esterno, al momento della conclusione del contratto, come prescrive l'art. 1341 c.c. Non hanno invece alcun effetto le clausole vessatorie presenti nel contratto, che devono essere specificamente approvate per iscritto ai sensi dell'art. 1341, secondo

comma. Quindi quelle clausole, spesso presenti nei contratti standard di licenza d'uso, che stabiliscono limitazioni di responsabilità, restrizioni alla libertà contrattuale nei rapporti con i terzi e deroghe alla competenza dell'autorità giudiziaria devono considerarsi inefficaci.

4.3. Software freeware e shareware

Il software freeware è software distribuito gratuitamente, generalmente in rete, e può essere copiato da chiunque si colleghi con la rete. In genere, reca la scritta "freeware" e il nome dell'autore. Talvolta viene specificato che il programma può essere liberamente copiato, altre volte si invita l'utente ad inviare osservazioni e commenti all'indirizzo specificato. In questo caso, è evidente la rinuncia da parte dell'autore ai propri diritti di utilizzazione economica dell'opera, quindi il software freeware può essere liberamente copiato. Il software shareware presenta molte delle caratteristiche del software freeware: è software distribuito in rete e può essere copiato da chiunque si colleghi con la rete. In genere, reca la scritta "shareware" e il nome dell'autore. A differenza che nel software freeware, nel software shareware si invita l'utente ad inviare un corrispettivo, in genere piuttosto basso, all'indirizzo specificato. Talvolta si precisa che il pagamento del corrispettivo dà diritto agli aggiornamenti del programma. In questo caso, non si può ritenere che l'autore abbia rinunciato ai propri diritti di utilizzazione economica dell'opera: si tratta di un contratto di licenza d'uso di software in cui la distribuzione è effettuata mediante rete e in forme particolari. Pertanto, deve essere corrisposto all'autore il compenso richiesto. Occorre comunque precisare, che per una serie di considerazioni di carattere pratico (in genere si tratta di programmi di modesta rilevanza economica; in genere si tratta di programmi distribuiti dallo stesso autore e non da un'impresa produttrice e in genere l'autore è straniero) non è molto probabile un'azione legale da parte dell'autore.

La cosiddetta "legge sulla privacy"

La più importante legge italiana in materia di "privacy" è la l. 31 dicembre 1996, n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" [http://www.garanteprivacy.it/garante/prewiew/0,1724,2039,00.html?sezione=115&LANG=1]1 , più nota come "legge sulla privacy", la quale attua la direttiva comunitaria 95/46/CE del 24 ottobre 1995 "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati" [http://www.garanteprivacy.it/garante/prewiew/0,1724,380,00.html?sezione=115&LANG=1]2. È bene chiarire subito che la l. 675/96 - come meglio si vedrà esaminando le definizioni di dato personale e di trattamento già richiamate nel titolo - non disciplina soltanto la "privacy", cioè i dati riservati, ma piuttosto il trattamento dei dati personali, cioè la circolazione delle informazioni, siano esse riservate o meno. La l. 675/96 costituisce l'adempimento di altri obblighi internazionali da parte dell'Italia, fra i quali quelli derivanti dall'Accordo di Schengen e quelli derivanti dalla Convenzione del Consiglio d'Europa sulla "Protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale", adottata a Strasburgo il 28 gennaio 1981.

1 Pubblicata nel Supplemento Ordinario alla Gazzetta Ufficiale n. 5 dell'8 gennaio 1997. 2 Pubblicata in G.U.C.E. n. L 281/31 del 23 novembre 1995.

Le disposizioni successive

La l. 675/96 è stata integrata e modificata da molte altre disposizioni normative, cosicché è in corso di predisposizione un Testo unico sulla "privacy". Fra le più importanti disposizioni normative che hanno integrato la l. 675/96, si ricordano: il d. lgs. 9 maggio 1997, n. 123 che ha introdotto la possibilità del consenso in forma orale; il d. lgs. 28 luglio 1997, n. 255 concernente l'esonero e le semplificazioni delle notificazioni; il d. lgs. 11 maggio 1999, n. 135, sulle disposizioni in materia di trattamento di dati

particolari da parte di soggetti pubblici; il d. lgs. 30 luglio 1999, n. 281 sul trattamento dei dati per finalità storiche, statistiche e di ricerca scientifica; il d. lgs. 30 luglio 1999, n. 282, sul trattamento dei dati per garantire la riservatezza in ambito sanitario; il d.p.r. 31 marzo 1998, n. 501, sul funzionamento dell'ufficio del Garante che reca anche norme che disciplinano l'accesso ai dati personali; il d. lgs. 13 maggio 1998, n. 171, recante disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni; il d.p.r. 28 luglio 1999, n. 318, sull'individuazione delle misure minime di sicurezza; il d. lgs. 28 dicembre 2001, n. 467, disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali. A ciò si aggiungano le autorizzazioni generali in materia di trattamento dei dati sensibili. Tutte le norme citate, nonché il testo consolidato della l. 675/96 possono essere reperiti nel sito ufficiale del Garante per il trattamento dei dati personali: http://www.garanteprivacy.it.

Sulla privacy è disponibile un **approfondimento**.

Intercettazione dei messaggi

I messaggi che passano sulla rete sono in realtà facilmente intercettabili. Esempi di attacchi che mirano all'intercettazione dei messaggi sono lo **sniffing** e lo **spoofing** dell'indirizzo IP. Oltre a ciò, l'amministratore di una macchina possiede le credenziali per intercettare tutti i dati che passano attraverso quel nodo e quindi un amministratore in malafede può intercettare facilmente messaggi destinati ad altri utenti.

L'intera **sicurezza** del sistema è fortemente compromessa dalla trasmissione di messaggi in chiaro. Un messaggio in chiaro intercettato può infatti essere letto, violando così la **confidenzialità**. Nel caso si tratti di una **password** o di una qualunque altra credenziale di identificazione, chi ha intercettato il messaggio avrà modo di sostituirsi al mittente, **abusando della sua identità elettronica** e infrangendo così anche l'**autenticazione** e il **non ripudio**. Con questa credenziale, carpita maliziosamente, sarà poi possibile sostituirsi all'utente nella gestione delle sue risorse, esponendo a rischio infine anche l'**integrità** e la **disponibilità** dei dati.

In realtà questo tipo di problema è percepito come critico soprattutto nel settore commerciale. In questo contesto è più che mai importante che i messaggi:

- non subiscano alterazioni (integrità): il contenuto dell'accordo non deve essere cambiato.
- Abbiano un mittente univocamente identificabile (autenticazione e non ripudio): la sottoscrizione di un messaggio è irreversibile e univoca, come una firma.
- Non vengano letti senza autorizzazione (confidenzialità): deve essere possibile inviare un numero di carta di credito o altre informazioni riservate con la garanzia che solo il destinatario le potrà leggere.

Crittografia

Il problema di inviare messaggi riservati attraverso sistemi di distribuzione non affidabili è sentito da secoli in ambito militare e sono innumerevoli le metodologie più o meno complesse messe in atto per spedire informazioni agli alleati, senza che i nemici possano decifrarle.

La **crittografia** è un procedimento di codifica e decodifica dei messaggi basata su funzioni parametriche, la cui computazione dipende da un parametro detto chiave. Un messaggio crittografato non è direttamente leggibile se non si possiede una funzione e una chiave per decriptarlo.

Il modello su cui è basato un sistema crittografico è il seguente:

- Un mittente A vuole inviare un messaggio M a un destinatario B.
- A cripta il messaggio, ovvero applica al messaggio un metodo di cifratura F con chiave di cifratura K.
- Il messaggio così modificato viene poi spedito via rete a B.
- B riceve un messaggio apparentemente illeggibile ma possiede un metodo di decifratura F' e una chiave K' che consentono di riportare il messaggio in chiaro.

Se un intruso dovesse intercettare il messaggio cifrato non sarebbe in grado di leggerlo a meno di possedere F' e K'.

Le chiavi di cifratura e decifratura possono coincidere e in questo caso si parla di **crittografia a chiave simmetrica** (o a **chiave privata**), oppure possono essere diverse e in questo caso si parla di **crittografia a chiave pubblica**.

Chiave pubblica e chiave privata

I metodi utilizzati tradizionalmente per la crittografia classica erano tutti metodi a chiave simmetrica, basati sull'ipotesi che gli alleati condividessero una chiave nota solo a loro (e per questo detta segreta o anche privata). Quando A vuole spedire a B un messaggio cifrato con un metodo a chiave segreta deve, prima di tutto, fare in modo che B conosca la sua stessa chiave di crittografia, K e, poi, criptare il messaggio con F e K. Quando B riceve il messaggio utilizza F' e K per decriptarlo.

La **crittografia a chiave pubblica** è un metodo asimmetrico basato sull'esistenza di due diverse chiavi, una utilizzata per criptare e una utilizzata per decriptare. Ciascun utente deve quindi possedere due chiavi, una privata che conosce solo lui e una pubblica che rende nota a tutti. Ovviamente esiste una relazione matematica tra **chiave pubblica** e **chiave privata** che deve rendere semplice calcolare la chiave pubblica a partire da quella privata e difficilissimo (o meglio computazionalmente impossibile) calcolare la chiave privata a partire da quella pubblica. La sicurezza di un algoritmo asimmetrico risiede proprio nella difficoltà di individuare la chiave privata, quando si è in possesso di quella pubblica.

Se A vuole inviare un messaggio riservato a B deve dunque procurarsi la chiave pubblica di B (che è disponibile a tutti) e utilizzarla per criptare il messaggio. B sarà l'unico a riuscire a decriptare il messaggio poiché è l'unico in possesso della chiave privata.

I meccanismi di crittografia sono alla base delle diverse forme di certificazione a disposizione su Internet e del funzionamento della firma digitale. Sulla crittografia è disponibile un **approfondimento**.

Criteri di accessibilità dei siti Web

Particolare attenzione è stata rivolta recentemente all'accessibilità dei disabili ai siti Web della Pubblica Amministrazione. L'AIPA, attraverso il Gruppo di Lavoro sull'Accessibilità e Tecnologie Informatiche nella Pubblica Amministrazione, ha prodotto una prima bozza di normativa, che va nella direzione di adottare integralmente le raccomandazioni emesse in materia dal World Wide Web Consortium (W3C). In generale i siti progettati attualmente utilizzano stili di presentazione altamente interattivi e a forte contenuto multimediale. Questi siti sono cioè progettati per utenti che non hanno limiti fisici, e dunque sono in grado di interagire attraverso dispositivi che richiedono movimenti manuali fini, né hanno limiti sensoriali, e dunque privilegiano presentazioni di tipo multimediale.

Per valutare il livello di accessibilità di un sito già realizzato possono essere utilizzati appositi strumenti software che consentono di verificare automaticamente il rispetto delle condizioni basilari

dell'accessibilità. Questa attività permette di correggere errori nella progettazione e nello stile di presentazione e riguadagnare a posteriori la piena accessibilità del sito.

I **riferimenti bibliografici** on line consentono di ottenere maggiori informazioni sull'accessibilità dei siti Web e in particolare sulle linee guida per la Pubblica Amministrazione.