



Gianni 56x52 cm.

# LA SICUREZZA DEI DATI

Franca Fabrizio

Il rispetto della privacy comporta delle grandi responsabilità per il personale scolastico e l'obbligo di educare alla riservatezza

*composent. Les magistrats sont les exécuteurs*

L'articolo 2 della nostra Costituzione afferma che "la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo" anticipando l'affermazione del principio del diritto alla riservatezza e precludendo alla definizione dei criteri fondamentali da osservare nel trattamento di quei dati personali e/o sensibili che riguardano i soggetti che hanno rapporti, a vario titolo, con aziende private e con le pubbliche amministrazioni. Una direttiva comunitaria del 1995 e il D.Lgs n. 675/1996 con le successive integrazioni, che l'hanno recepita, disciplinano la materia del trattamento dei dati personali nel nostro Paese fino all'emanazione del D.Lgs n. 196/2003 che ha reso famoso, a livello di massa, il termine inglese di *privacy*.

Il D.Lgs n. 196/2003 (*Codice in materia di protezione dei dati personali*) assume una rilevanza enorme nel panorama legislativo e democratico attuale e delle stesse istituzioni, in quanto impone un'attenzione particolare e l'attivazione di una serie di procedure e accorgimenti nella raccolta, conservazione e trattamento dei dati personali acquisiti.

In base alle disposizioni impartite da questo *Codice*, al fine di assicurare **adeguate misure di sicurezza delle informazioni acquisite**, ogni istituzione e/o ente deve predisporre e/o aggiornare, entro il 31 marzo di ogni anno, il *Documento programmatico per la sicurezza* che contiene:

- l'elenco dei trattamenti di dati (personali, sensibili e giudiziari);

- le figure che svolgono compiti in questo ambito all'interno dell'istituzione/ente con le relative mansioni e responsabilità;
- l'analisi dei rischi cui possono essere esposti i dati;
- le procedure e le misure da attuare per garantire un corretto trattamento degli stessi e la loro adeguata conservazione negli ambienti di lavoro al fine di impedire l'accesso a persone non autorizzate;
- la definizione dei criteri e delle modalità per il ripristino dei dati in caso di danneggiamenti;
- le misure adottate per evitare eventi dannosi;
- l'individuazione dei criteri da adottare, da parte del responsabile, per separare e conservare dati sensibili e giudiziari da dati personali dei soggetti, anche mediante l'uso di armadi con chiusura a chiave.

**I principi fondamentali** definiti agli artt. 1 e 2 del codice della *privacy* sono i seguenti:

- chiunque ha diritto alla protezione dei dati personali che lo riguardano;
- il trattamento dei dati si deve effettuare assicurando la tutela del diritto alla riservatezza, all'identità personale e alla protezione dei dati personali, nel rispetto dei diritti, delle libertà e della dignità della persona.

L'art. 3 precisa che i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione dei **dati identificativi e personali**, così

da escludere il loro trattamento quando le finalità da perseguire possono essere soddisfatte mediante dati anonimi o con modalità tali che permettano l'identificazione dell'interessato solo in caso di necessità.

Ne deriva che occorre trattare i dati solo per fini consentiti, solo se necessario, raccogliendo e conservando il minimo dei dati utili al raggiungimento degli obiettivi definiti.

**Gli obblighi** previsti dalla legge sulla *privacy* scattano quando si devono trattare:

- *dati personali* (ad esempio, quelli anagrafici);
- *dati sensibili* (quelli che rivelano stato di salute e vita sessuale, origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni, organizzazioni di carattere religioso, politico, sindacale);
- *dati giudiziari* (quelli idonei a rivelare informazioni/provedimenti in materia di casellario giudiziale, di sanzioni amministrative dipendenti da reati penali e di relativi carichi pendenti, provvedimenti di condanna, ecc.).

Il soggetto **titolare** del trattamento è, nella scuola, il dirigente che ne ha la legale rappresentanza. Poiché tale figura non tratta direttamente i dati personali, è sua facoltà individuare tra il proprio personale un **responsabile** che, per esperienza, capacità e affidabilità, possa fornire garanzia del pieno rispetto delle disposizioni vigenti in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Oltre al responsabile, che sovrintende e controlla la corretta gestione e conservazione dei dati, il dirigente di un ente deve nominare anche degli **incaricati**, ovvero delle persone fisiche che operano sotto la diretta autorità del titolare o del responsabile e che attuano le operazioni di trattamento dei dati attenendosi alle istruzioni impartite.

L'uso, inoltre, nelle strutture lavorative (uffici, scuole, aziende, ecc.) di **strumenti informatici ed elettronici** comporta ulteriori impegni da parte di titolare, responsabile ed incaricati.

È necessario che vengano eseguite sistematicamente procedure minime quali:

- l'autenticazione informatica;
- l'adozione di procedure di gestione delle credenziali di autenticazione;
- la protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti, ad accessi non consentiti e all'utilizzo di determinati programmi informatici;
- l'adozione di procedure per la custodia delle copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- l'adozione di tecniche di cifratura o di codici identificativi per particolari trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale di un soggetto quali quelli effettuati da organismi sanitari.

La normativa stabilisce, inoltre, in quali casi è obbligatorio acquisire il **consenso** dell'interessato al trattamento dei dati e in quali casi, invece, esso non è richiesto. Per gli enti pubblici, tra cui vi sono le istituzioni scolastiche, il consenso non deve essere richiesto, in quanto i dati servono per lo svolgimento di attività previste dalla norma.

L'art. 13 fornisce chiarimenti sull'**informativa** da dare, oralmente o per iscritto, al soggetto di cui si raccolgono dati personali, precisando le finalità e le modalità del trattamento cui sono destinati i dati, la natura obbligatoria o facoltativa del conferimento dati con le relative conseguenze di un eventuale rifiuto di rispondere, i soggetti cui i dati potrebbero essere comunicati, i diritti dell'interessato (art. 7), gli estremi identificativi del titolare.

Nelle scuole, l'informativa è fornita ai genitori al momento dell'iscrizione e agli insegnanti nella fase della loro assunzione. Prima delle prove INVALSI i genitori ricevono un'altra informativa, il cui titolare è il MIUR, in quanto vengono trattati dati, anche se in codice, di alunni che potrebbero essere identificati tramite la scuola di appartenenza.

La normativa prevede delle **sanzioni** a carico del titolare se non sono state attuate le misure di sicurezza e protezione dei dati prescritte dal *Codice*. L'art. 15 recita, infatti, che "*Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile*".

Il riferimento all'art. 2050 del codice civile implica che il soggetto che abbia cagionato un danno deve "*dimostrare concretamente di avere messo in atto ogni misura di sicurezza (accorgimenti, procedure, ecc.) idonea ad evitarlo*" in maniera da escludere il nesso tra il trattamento dei dati, il danno causato e il danneggiato il quale, da parte sua, deve provare di avere riportato un danno.

Il mancato rispetto della norma e l'omissione delle misure di sicurezza comportano l'arresto fino a 2 anni e un'ammenda da 10.000 a 50.000 euro.

Pertanto, viene richiesta la massima attenzione a tutti, titolari, responsabili ed incaricati, indipendentemente dalla categoria lavorativa di appartenenza, nell'acquisizione, trattamento e conservazione dei dati acquisiti, che non devono eccedere quelli necessari per la realizzazione della finalità stabilita dalla legge o per quella specifica per la quale si richiede il consenso.

La D.M. 104/2007, emanata dal MIUR e inviata a tutte le scuole, disciplina anche gli aspetti legati all'acquisizione, utilizzo improprio e/o alla diffusione di **immagini e filmati relativi a persone**.

Nello Statuto delle studentesse e degli studenti (D.P.R. 249/98), all'art. 2, comma 2, si sancisce il diritto alla riservatezza degli studenti e si impegnano le scuole a educare gli alunni sull'importanza della protezione dei dati personali, prevedendo anche le sanzioni disciplinari e le multe (da 3 a 18 mila euro) in caso di divulga-



zione senza consenso di immagini e filmati attinenti la vita privata (*Abuso dell'immagine altrui*).

La materia è molto complessa e delicata e richiede sinergici interventi educativi e riflessioni congiunte da parte degli operatori scolastici e delle famiglie degli allievi che, spesso, molto leggermente abusano nell'uso di dispositivi elettronici (cellulari, computer) venendo meno alle regole e alle disposizioni di legge.

Sostenere i ragazzi nella conoscenza dei principali diritti di rilevanza costituzionale, tra cui il diritto alla riser-

vatezza dei dati personali, è uno dei compiti delle istituzioni educative, famiglia e scuola insieme, per educare alla legalità e formare cittadini rispettosi degli altri e delle norme vigenti.

Franca Fabrizio - Dirigente dell'Istituzione Scolastica *Eugenia Martinet* di Aosta.