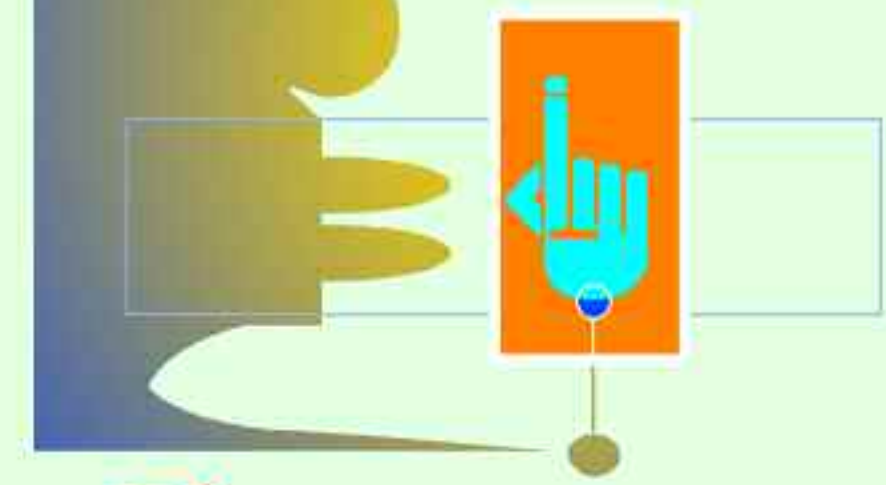
Provincia Autonoma di Trento
Assessorato all'istruzione e alle Politiche Giovanili

*Il trattamento dei dati personali nelle Istituzioni scolastiche*




# GUIDA ALLA RISERVATEZZA

# GUIDA ALLA RISERVATEZZA

## IL TRATTAMENTO DEI DATI PERSONALI NELLE ISTITUZIONI SCOLASTICHE

L'Autore del testo è:

*Anna Simonati*, Ricercatrice di Diritto amministrativo
Facoltà Giurisprudenza - Università degli studi di Trento

Copertina:
*Maurizio Corradi*

Impaginazione e stampa:
*Grafiche Futura - Mattarello (TN)*

Finito di stampare *Settembre 2005*

*La presente pubblicazione è consultabile e scaricabile dal Portale della scuola Trentina* **www.vivoscuola.it**

# INDICE

## I PRINCIPALI PROBLEMI IN AMBITO SCOLASTICO

# PRESENTAZIONE

Il decreto legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali", d'ora in avanti semplicemente Codice) razionalizza e, in parte, modifica la preesistente disciplina relativa alla gestione dei dati personali[1].

Non si tratta di una normativa generale sul diritto alla riservatezza, bensì di un insieme ordinato di disposizioni, atte ad indicare le modalità dello svolgimento di attività coinvolgenti dati personali di terzi. La nozione di riservatezza non viene definita nel Codice né in altre disposizioni vigenti; essa rappresenta il prodotto di una lunga e graduale elaborazione dottrinale e giurisprudenziale e va attentamente chiarita perché costituisce il "prerequisito" fondamentale per la corretta applicazione delle norme.

Questa pubblicazione vorrebbe essere una guida operativa al trattamento dei dati personali da parte degli istituti scolastici a carattere statale della P.A.T. A questo tema il Codice del 2003 dedica poche e scarne disposizioni specifiche. Sarà indispensabile, dunque, tenere conto dei principi generali emergenti dal contesto complessivo della disciplina vigente, oltre che delle regole di dettaglio.

La Guida consta di varie parti.

In primo luogo, è predisposto un Glossario, in cui sono non solo definiti, ma anche sinteticamente illustrati i concetti fondamentali utilizzati più frequentemente dal legislatore.

Successivamente, sono riassunti i principi e le regole basilari in materia di protezione della riservatezza. Sono esaminate le previsioni costituzionali, che, proprio perché si pongono al livello normativo supremo, devono sempre essere tenute presenti dagli operatori. Inoltre, sono descritti i principi emergenti dal decreto legislativo del 2003. È riservata particolare attenzione alla disciplina del trattamento di dati personali da parte della pubblica amministrazione e non si trascura di specificare le disposizioni applicabili agli istituti scolastici.

Un altro aspetto esaminato è quello della responsabilità in cui possono incorrere gli operatori, a seconda del ruolo rispettivamente ricoperto nella struttura di appartenenza.

Ancora, si evidenziano i profili maggiormente significativi del rapporto fra la normativa relativa al trattamento di dati personali e quella inerente all'esercizio da parte dei privati del diritto di accesso ai documenti amministrativi. Si tiene conto, in proposito, della recentissima riforma (non ancora del tutto vigente al momento della redazione di questa Guida) cui è stata

sottoposta la legge n. 241 del 1990, ove l'istituto dell'accesso trova la sua disciplina generale. Non si trascura, poi, di segnalare i sommi capi della normativa settoriale in materia di accesso contenuta nel regolamento ministeriale del 1996.

L'ultima parte della Guida, infine, vuole fungere da sintetico "manuale di comportamento" per gli operatori della scuola, additando le soluzioni maggiormente accreditate ai problemi correlati con l'attività di gestione dei dati in ambito scolastico.

Alla redazione della Guida hanno collaborato i Dirigenti dell'Assessorato all'Istruzione e alle Politiche Giovanili Roberto Ceccato, Aldo Gabbi e Paolo Renna, cui desidero esprimere la mia gratitudine. Inoltre, un particolare ringraziamento va a Marco Acquisti per il costante e puntuale sostegno.

*Anna Simonati*

[1] In grassetto sono evidenziati i termini definiti nel **Glossario**.

# PREMESSA

## CHE COS'È IL DIRITTO ALLA RISERVATEZZA?

Il diritto alla riservatezza è il diritto soggettivo riconducibile sia all'esigenza di segretezza rispetto a taluni aspetti della "sfera intima", sia alla possibilità del **titolare** dei dati di mantenere piena consapevolezza in merito alla loro circolazione.

Non è un istituto legislativamente definito.

La L. n. 675/1996 rappresenta la prima tappa realmente significativa del processo di "codificazione giuridica" del diritto alla riservatezza nell'ordinamento italiano, nonché il punto di partenza dal quale il vigente Codice ha tratto la maggior parte dei suoi contenuti. È necessario precisare, preliminarmente, che a torto essa è stata definita, nel linguaggio comune, come "legge sulla riservatezza". Infatti, con questa disciplina il legislatore ha assunto una prospettiva piuttosto circoscritta. Era rintracciabile soltanto un nucleo di indicazioni di portata prevalentemente operativa, preordinate a stabilire, da un lato, le modalità con cui era ammesso il **trattamento** delle informazioni personali mediante la predisposizione di **banche di dati** e, dall'altro lato, le caratteristiche fondamentali degli strumenti di difesa posti a disposizione del singolo in vista dell'indebita o dell'illegittima utilizzazione delle informazioni medesime. Invece, non vi si poteva ravvisare alcuna indicazione attinente al problema della definizione, quanto meno per sommi capi, della natura sostanziale della riservatezza e della sua collocazione sistematica nel contesto dei diritti inviolabili dell'uomo.

Su questo fronte, nulla è mutato con la riforma del 2003.

Pertanto, il problema della definizione della riservatezza, del suo inserimento nel contesto dei diritti fondamentali della persona e della predisposizione di adeguati strumenti di tutela è stato affrontato esclusivamente a livello dottrinale e giurisprudenziale.

Probabilmente, è nel giusto chi ha ritenuto che la riservatezza consti di varie sfaccettature, tanto che pare opportuno considerarla come una «*costellazione di diritti*» (in dottrina, MODUGNO). Non sarebbe del tutto corretto ridurla all'esigenza di segretezza rispetto a taluni aspetti della "sfera intima" individuale. Al contrario, come già si è accennato, è preferibile riconoscere l'esistenza di una posizione giuridica complessa, che consente al singolo di verificare le modalità della circolazione dei dati che lo riguardano.

Questa concezione è accolta dalla Corte Costituzionale già a partire dagli anni settanta del XX secolo. Nello stesso periodo, anche la Corte di

Cassazione ravvisa un diritto «*alla autonoma determinazione della vita di relazione*» e riconosce la necessità di proteggere «*una certa sfera della vita individuale e famigliare, [...]l'illesa intimità personale in certe manifestazioni della vita di relazione, [...] tutte quelle vicende, cioè, il cui carattere intimo è dato dal fatto che esse si svolgono in un domicilio ideale, non materialmente legato ai tradizionali rifugi*». In conclusione, la Corte chiarisce che la tutela del diritto alla riservatezza comporta la protezione di «*quelle situazioni e vicende strettamente personali e familiari, le quali anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze, che, compiute sia pure con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione e il decoro, non siano giustificate da interessi pubblici preminenti*».

La nozione di riservatezza fin qui sinteticamente indicata è stata implicitamente accolta nel Codice.

Sulla sua ampiezza evidentemente incide anche il potenziamento dei meccanismi che consentono la raccolta, l'elaborazione e la circolazione delle informazioni, determinato, negli ultimi decenni, dal progresso tecnologico. Mentre in passato il diritto alla riservatezza si poneva come libertà essenzialmente negativa (cioè come spazio di "non interferenza" da parte del potere pubblico), oggi risulta strettamente correlato ad un'esigenza di autodeterminazione, cioè al diritto di effettuare le proprie scelte senza dover subire alcun condizionamento da parte di terzi. Attualmente, dunque, esso ricomprende aspetti di "libertà positiva", comportando la possibilità dei singoli di rifiutarsi di fornire informazioni sul proprio conto, nonché la possibilità di verificare la correttezza dei dati già raccolti, chiedendone eventualmente la rettifica.

Inoltre, dalla variazione dei possibili mezzi di offesa del diritto è conseguito un graduale approfondimento dell'intensità della tutela. A fronte del potenziamento delle tecniche di raccolta, elaborazione e interconnessione dei dati, anche il trattamento di notizie apparentemente "neutre" inerenti alla sfera personale dei singoli è suscettibile di tramutarsi in un pericoloso strumento di controllo (ed eventuale compressione) delle libertà.

## LA RISERVATEZZA... A SCUOLA

La tutela del diritto alla riservatezza in vista del **trattamento** di dati in ambito scolastico presenta varie sfaccettature, che si possono rispecchiare in un'ampia e diversificata casistica.

Gli ambiti problematici possono riguardare essenzialmente due distinti settori.

In primo luogo, è necessario gestire tutte le informazioni relative agli studenti. Si tratta di dati che giungono in possesso degli istituti scolastici non solo "in via amministrativa", ma anche in seguito allo svolgimento della normale attività didattica ed educativa. Questa consistente quantità di dati va utilizzata con particolare cautela, poiché, nella maggior parte dei casi, essa concerne soggetti minorenni, che, in quanto tali, l'ordinamento ritiene meritevoli di peculiare tutela (v. *infra*, I principi fondamentali). Inoltre, l'art. 2 del D.P.R. 24 giugno 1998, n. 249 (regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria) annovera la riservatezza fra i diritti che la comunità scolastica è tenuta a proteggere in capo agli alunni.

In secondo luogo, gli istituti scolastici, al pari delle altre pubbliche amministrazioni, devono conservare e utilizzare i dati relativi al personale, docente e non. Ovviamente, anche da questa materia possono emergere profili problematici. Essi, tuttavia, non presentano peculiarità rispetto alle questioni corrispondenti sollevate in altri settori dell'attività pubblica. In questa sede, pertanto, ci si limiterà a precisare, sul punto, che, proprio alla luce della particolare attenzione che richiede il trattamento di dati relativi a minori, sembra opportuno che le informazioni attinenti agli studenti e quelle attinenti ai dipendenti dell'istituto scolastico siano trattate separatamente. Di conseguenza, sarebbe opportuno altresì (quanto meno, nelle strutture di maggiori dimensioni) provvedere alla nomina di persone diverse quali responsabili (v. *infra*, Glossario, voce *Responsabile*) dei due distinti trattamenti.

# GLOSSARIO

## AUTENTICAZIONE INFORMATICA

È l'insieme degli **strumenti elettronici** e delle procedure per la verifica (anche indiretta) dell'identità del soggetto cui è consentito l'accesso alla **banca di dati** informatica;

## BANCA DI DATI

È qualsiasi complesso organizzato di **dati personali**. La banca di dati può essere realizzata su supporto cartaceo o di altra natura (per esempio, informatico) e può essere ripartita in più unità, anche dislocate in siti diversi;

## CREDENZIALI DI AUTENTICAZIONE

Sono i dati e i dispositivi, in possesso esclusivo ed univoco di una persona autorizzata all'accesso a una **banca di dati** informatica, utilizzati per l'**autenticazione informatica**;

## DATI ANONIMI

Sono i dati che, in origine o a seguito di **trattamento**, non possono essere associati ad un **interessato** identificato o identificabile.

Il trattamento di dati in forma anonima è l'unico che sicuramente non mette a repentaglio il diritto alla riservatezza dei titolari delle informazioni; pertanto, se possibile, esso deve essere effettuato in via preferenziale rispetto ad altre soluzioni;

## DATI IDENTIFICATIVI

Sono i **dati personali** che permettono l'identificazione diretta del soggetto cui si riferiscono (*in primis*, ovviamente, rientrano in questa categoria di dati le generalità della persona);

## DATI PERSONALI

Sono le informazioni relative a persone fisiche, persone giuridiche, enti o associazioni, identificati o identificabili anche indirettamente, cioè mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

I dati personali rientrano nel campo di applicazione del Codice indipendentemente dal supporto (grafico-cartaceo, informatico, fotografico, sonoro, ecc.) tramite il quale essi sono stati elaborati. Non necessariamente si tratta di informazioni riservate;

## DATI SENSIBILI

Sono 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.

Questa nozione è della massima importanza, poiché il **trattamento** di dati sensibili richiede la predisposizione di particolari cautele. L'elencazione è tassativa, ma il concetto di "dato sensibile" va interpretato e applicato in modo assai attento, poiché non implica necessariamente che il dato riguardi *direttamente* la sfera intima della persona; al contrario, è sufficiente che l'informazione trattata sia "idonea", anche in via indiretta, a consentire la ricostruzione della sfera intima individuale;

## DOCUMENTO PROGRAMMATICO SULLA SICUREZZA (D.P.S.) -

Deve essere predisposto periodicamente da parte del **titolare** di **trattamento** di **dati personali** effettuato mediante **strumenti elettronici**, il quale può incaricare per la redazione il **responsabile**, se designato.

Il D.P.S. relativo a trattamenti coinvolgenti **dati sensibili** deve contenere:

- l'elenco dei trattamenti di dati personali in atto;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati trattati, in particolare in termini di sicurezza;
- l'indicazione delle **misure di sicurezza** da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree in cui essi sono conservati, ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati che abbiano subito distruzione o danneggiamento;
- la previsione di interventi formativi degli **incaricati** del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili normativi più rilevanti in rapporto alle specifiche competenze, delle responsabilità in caso di violazione dei precetti, delle modalità per aggiornarsi sulle **misure minime** adottate dal titolare;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al Codice, all'esterno della struttura del titolare;

## GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

È l'autorità preposta a vigilare sulla legittimità del **trattamento**. Deve assicurare il rispetto della disciplina vigente e promuoverne la conoscenza, anche assicurandone la corretta interpretazione; inoltre, è chiamato a garantire la repressione degli illeciti commessi in violazione delle disposizioni del Codice e commina le sanzioni amministrative.

Il Garante ha predisposto un sito internet (www.garanteprivacy.it), ove è possibile reperire, oltre alla normativa vigente, tutti i provvedimenti e le comunicazioni emesse, la risposta ai quesiti maggiormente frequenti in materia di protezione del diritto alla riservatezza, nonché i *fac simile* della modulistica di uso comune;

## INCARICATO

È la persona fisica autorizzata, dal **titolare** o (se nominato) dal **responsabile**, a compiere le operazioni correlate al **trattamento**. Ovviamente, non può mai trattarsi di una persona giuridica, né di un intero ufficio.

> Negli istituti scolastici, sono sicuramente incaricati del trattamento, ciascuno nell'ambito delle proprie funzioni, non solo gli addetti agli uffici di segreteria, ma anche i docenti. Inoltre, solo per lo svolgimento di determinate attività di portata strettamente materiale (per esempio, lo spostamento di documentazione da un luogo all'altro), possono essere nominati quali incaricati del trattamento i bidelli.

La designazione dell'incaricato e la determinazione dei suoi compiti vanno effettuate analiticamente per iscritto; comunque, è sufficiente la documentata preposizione di un individuo ad una unità organizzativa, previa chiara delimitazione in forma scritta dell'ambito del trattamento di competenza di quella unità. L'incaricato, nel caso di violazione delle disposizioni in materia di trattamento dei **dati personali**, può incorrere in responsabilità civile, penale e amministrativa in relazione ai compiti specifici che gli sono stati assegnati (v. *infra*, **La responsabilità per la violazione delle regole sul trattamento dei dati personali**);

## INTERESSATO

È il soggetto (persona fisica, persona giuridica, ente o associazione) cui si riferiscono i **dati personali** sottoposti a **trattamento**; si tratta, pertanto, del titolare potenziale del diritto alla riservatezza.

È destinatario della notifica, con cui il **titolare** lo informa dell'esistenza, delle modalità e delle finalità del trattamento.

Di conseguenza, egli può esercitare una serie di diritti e precisamente:

- ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano (anche se non ancora registrati) e la loro comunicazione in forma intelligibile;
- ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di **strumenti elettronici**, degli estremi identificativi del titolare e dei **responsabili**, nonché dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o **incaricati** (qualora il titolare del trattamento solo in un secondo momento acquisisca consapevolezza in merito alla trasmissione a terzi dei dati trattati, effettuerà un'integrazione dell'informativa);
- ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge; tali adempimenti possono essere chiesti e ottenuti anche qualora alcune delle informazioni conservate risultino sovrabbondanti rispetto alle finalità del trattamento (v. *infra*, **I principi fondamentali**);
- in caso di rettifica o modifica dei dati trattati, ottenere l'attestazione che tali operazioni sono state portate a conoscenza dei soggetti cui i dati sono stati dal titolare comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto alla rilevanza del diritto tutelato;
- opporsi, in tutto o in parte, per motivi legittimi, al trattamento dei dati personali che lo riguardano.

I diritti dell'interessato possono essere esercitati, qualora costui sia defunto, da chiunque vi abbia un interesse proprio, nonché da chi agisca a tutela della persona deceduta oppure per ragioni familiari meritevoli di protezione. Di regola, si ritiene che siano legittimati non solo e non tanto i suoi aventi causa (es. gli eredi), quanto i suoi prossimi congiunti;

## MISURE MINIME

È il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione dei **dati personali** oggetto di **trattamento**. Questi devono essere 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 i rischi di distruzione o perdita anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il Codice richiede la predisposizione di misure di sicurezza distinte, a seconda che il trattamento sia svolto o meno con l'ausilio di **strumenti elettronici**.

Il trattamento di dati personali effettuato *senza l'ausilio di strumenti elettronici* è consentito solo se sono adottate le seguenti misure minime:

- ☞ aggiornamento periodico (con cadenza almeno annuale) dell'individuazione dell'ambito del trattamento consentito ai singoli **incaricati** o alle unità organizzative, ove l'elencazione degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;
- ☞ previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti, con trasmissione agli incaricati stessi di istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali;
- ☞ previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati, per cui le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate e quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

Per quanto riguarda le misure minime di sicurezza richieste per il trattamento svolto con l'ausilio di mezzi informatici, v. *infra*, **Il trattamento informatico**;

## PAROLA CHIAVE

È la componente più importante della **credenziale di autenticazione**. Si tratta di una sequenza di caratteri o altri dati in forma elettronica, associata ad una persona e nota esclusivamente a questa;

## RESPONSABILE

È la persona fisica o giuridica (compresi la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) che il **titolare** del **trattamento** può, se lo ritiene opportuno, nominare quale soggetto preposto al

trattamento di **dati personali**. Può trattarsi di più soggetti, anche con compiti suddivisi.

Nell'ambito degli istituti scolastici, di regola si tratta del segretario amministrativo.

In ogni caso, la determinazione dei compiti va effettuata dal titolare in modo analitico e per iscritto.

Se designato, il responsabile non svolge un ruolo meramente esecutivo delle istruzioni impartitegli dal titolare; al contrario, nell'ambito dei compiti analiticamente attribuitigli per iscritto dal titolare, egli collabora con costui nella scelta delle modalità di effettuazione del trattamento (e, ove previsto dal titolare, effettua la nomina degli **incaricati** del trattamento). Pertanto, in caso di violazione della normativa vigente, egli di regola condivide con il titolare la relativa responsabilità civile, penale e amministrativa (v. *infra*, **La responsabilità per la violazione delle regole sul trattamento dei dati personali**). Di conseguenza, il titolare lo deve individuare tenendo conto delle sue qualità personali in termini di esperienza, capacità e affidabilità;

## Strumenti elettronici

Si tratta degli elaboratori, dei programmi per elaboratori e di qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il **trattamento**.

La nozione rileva, poiché per i trattamenti svolti mediante l'ausilio di strumenti elettronici è richiesta l'assunzione di **misure minime** di sicurezza particolarmente rigorose;

## Titolare

Si tratta della persona fisica o giuridica (compresi la pubblica amministrazione e qualsiasi altro ente, associazione od organismo) cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità e alle modalità del **trattamento** di **dati personali**, nonché relativamente agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Negli istituti scolastici, titolare del trattamento è il dirigente.

Il titolare assume la responsabilità complessiva dell'operazione ed è chiamato a svolgere le scelte "strategiche". In particolare, è delicato il momento della designazione degli altri soggetti "attivi" del trattamento

(**responsabile** e **incaricato**), che deve essere effettuata per iscritto, attribuendo loro poteri giuridici e mezzi materiali di intervento tali da garantire lo svolgimento efficace ed efficiente del trattamento. Inoltre, al titolare spetta tenere i rapporti con il **Garante** ove previsto.

Il titolare, nel caso di violazione delle disposizioni in materia di trattamento dei dati personali, può incorrere in responsabilità civile, penale e amministrativa (v. *infra*, **La responsabilità per la violazione delle regole sul trattamento dei dati personali**);

## TRATTAMENTO

È qualunque operazione o complesso di operazioni, 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**.

Pertanto, anche la sola ricezione e conservazione presso i propri archivi delle informazioni configura un trattamento e risulta in generale sottoposta alle norme del Codice.

# PRINCIPI E REGOLE

# I PRINCIPI FONDAMENTALI

## I PRINCIPI COSTITUZIONALI

Si è detto che la nozione di riservatezza non è definita dal legislatore, né essa trova espressamente spazio nelle previsioni costituzionali.

Ciò nonostante, dottrina e giurisprudenza sono ormai concordi nel ritenere che il diritto alla riservatezza sia indirettamente protetto a livello costituzionale negli artt. 13 (sulla libertà personale, che comporta il diritto di ciascuno all'autodeterminazione), 14 (sulla tutela del domicilio), 21 (sulla libertà di non rendere noto il proprio pensiero e di comunicazione privata) e 15 (sulla libertà e segretezza della corrispondenza), nonché negli artt. 2 (che sancisce la protezione dei diritti inviolabili dell'uomo) e 3 (sul principio di uguaglianza).

Inoltre, non va sottovalutato il fatto che una frazione significativa dei dati sottoposti a **trattamento** in ambito scolastico riguarda gli studenti e cioè, nella maggior parte dei casi, persone minorenni.

Il Codice non differenzia la disciplina applicabile ai trattamenti di dati relativi a questi soggetti. L'unica disposizione (invero, assai scarna) in tal senso rilevante è quella dell'art. 50, ove si precisa che è vietato pubblicare o diffondere notizie e immagini idonee a consentire l'identificazione di minori coinvolti a qualunque titolo in un procedimento giudiziario.

Tuttavia, indubbiamente i minorenni, in ragione della situazione di intrinseca vulnerabilità in cui si trovano, meritano una tutela particolarmente intensa. Non bisogna dimenticare, poi, che i fanciulli e i ragazzi ricevono una protezione giuridica qualificata dal combinato disposto degli artt. 30 e 31 della Costituzione (in particolare, nell'art. 31, c. 2, ove è stabilito che la Repubblica "*protegge […] l'infanzia e la gioventù, favorendo gli istituti necessari a tale scopo*").

Queste previsioni pongono i principi fondamentali con cui deve essere armonizzata qualsiasi operazione correlata al trattamento di **dati personali** in ambito scolastico.

# IL "CODICE DELLA PRIVACY"

## I PRINCIPI GENERALI

In primo luogo, il Codice garantisce 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 concernenti la sua persona (art. 2, c. 1).

In sintesi, il diritto all'identità personale comporta che, in linea di principio, solo eccezionalmente i **dati identificativi** possano essere utilizzati da soggetti diversi da quelli cui si riferiscono. Il diritto alla protezione dei dati personali consente all'individuo di esercitare una vigilanza costante sulla circolazione delle informazioni che lo riguardano. Pertanto, entrambi i diritti rappresentano estrinsecazione del diritto alla riservatezza latamente inteso.

Inoltre, poiché il Codice prevede che la disciplina del trattamento dei dati personali debba assicurare un elevato livello di tutela di tutte le libertà individuali (non solo della riservatezza), è attribuita particolare importanza al principio di semplificazione, per cui i procedimenti non devono essere inutilmente "aggravati", complicando eccessivamente la posizione del privato (art. 2, c. 2).

È stabilito, poi, che le regole relative, da un lato, all'esercizio dei diritti da parte degli interessati e, dall'altro lato, allo svolgimento dei compiti di chi è preposto al trattamento siano reciprocamente compatibili (principio di armonizzazione) e risultino complessivamente idonee ad assicurare il buon funzionamento del sistema (principio di efficacia) (art. 2, c. 2).

È fondamentale il principio di necessità del trattamento dei dati, in base al quale i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, **dati anonimi** od opportune modalità che permettano di risalire all'interessato solo in caso di necessità (art. 3).

## LE ALTRE REGOLE

Ancora, il trattamento deve essere improntato al rispetto di altre basilari regole di portata generale:

- liceità (art. 11, c. 1, lett. *a)*): il trattamento deve svolgersi in armonia con la disciplina vigente (sia di rango legislativo che regolamentare) e con i principi di ordine pubblico. Laddove **titolare** del trattamento sia un sog-

getto pubblico, la liceità deve intendersi quale legittimità: ciò significa che non solo è vietato operare in contrasto con l'ordinamento vigente, ma anche è necessario che le operazioni svolte dalla p.a. trovino fondamento nell'intento di espletare compiti che ad essa sono istituzionalmente deferiti dal legislatore o comunque attività strettamente correlate all'espletamento di tali compiti;

- correttezza (art. 11, c. 1, lett. *a)*): il trattamento deve svolgersi in applicazione dei parametri di lealtà e trasparenza, in particolare per quanto riguarda i doveri di informazione e aggiornamento nei confronti dell'interessato. Ciò determina una serie di conseguenze. Precisamente, è stabilito che i dati possano essere raccolti esclusivamente per scopi determinati, espliciti e legittimi. Pertanto, la finalità cui punta il trattamento deve essere individuata e resa nota fin dall'inizio; l'utilizzo dei dati raccolti in operazioni diverse da quelle originariamente preventivate è ammissibile solo se compatibile con l'obbiettivo complessivo del trattamento. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono distrutti o ceduti ad altro titolare, purché destinati ad un trattamento compatibile con gli scopi per i quali i dati sono stati originariamente raccolti;
- esattezza (art. 11, c. 1, lett. *c)*) e completezza (art. 11, c. 1, lett. *d)*) dei dati trattati: l'onere di verificare questi parametri incombe di regola sul titolare del trattamento, ma anche l'interessato può chiedere la rettifica dei dati inesatti o incompleti (v. *supra*, Glossario, voce *Interessato*). È interessante sottolineare che il dato parziale è ritenuto pericoloso, poiché non è idoneo a rappresentare adeguatamente la realtà

L'applicazione dei principi di esattezza e completezza dei dati trattati richiede agli istituti scolastici la massima attenzione qualora, durante il trattamento di dati personali relativi ad alunni minorenni, intervengano vicende di separazione o divorzio fra i loro genitori. Tale circostanza potrebbe determinare variazioni, anche significative, nella gestione del patrimonio informativo dello studente. D'altra parte, appare eccessivamente "esigente" (e, paradossalmente, potrebbe dare luogo a comportamenti potenzialmente lesivi della riservatezza delle persone coinvolte) accollare alla scuola l'onere di verificare periodicamente presso le famiglie la permanenza della situazione originariamente descritta. Pertanto, potrebbe forse rappresentare una buona prassi l'inserimento, nell'informativa resa dal titolare all'inizio del trattamento, della richiesta all'interessato di comunicare (esercitando, di fatto, un suo diritto) eventuali modificazioni dei dati a suo tempo raccolti qualora ciò possa in qualche modo influenzare le modalità del trattamento;

- pertinenza e non eccedenza rispetto alle finalità del trattamento (art. 11, c. 1, lett. *d)*): i dati devono presentare un legame contenutistico con l'obbiettivo del trattamento, ma non possono risultare sovrabbondanti rispetto a questo; possono dunque essere sottoposti a trattamento solo nella misura strettamente necessaria alla realizzazione dello scopo. La necessità del trattamento si estrinseca anche (sul piano "cronologico") nella regola per cui la conservazione dei dati può consentire l'identificazione dell'interessato soltanto per il lasso di tempo strettamente necessario (art. 11, c. 1, lett. *e)*).

  I dati trattati in violazione dei principi ora indicati e delle regole più specifiche che ne rappresentano applicazione non possono essere utilizzati (art. 11, c. 2).

# LE REGOLE PER IL TRATTAMENTO DEI DATI DA PARTE DELLE PUBBLICHE AMMINISTRAZIONI

## LE DISPOSIZIONI GENERALI

Il **trattamento** di **dati personali** da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali e nel rispetto dei precetti contenuti nel Codice, ma non è richiesto il consenso dell'**interessato** (art. 18, c. 4). D'altra parte, l'ottenimento di tale consenso non sana l'eventuale illegittimità derivante dalla violazione delle disposizioni vigenti.

Invece, i soggetti pubblici sono equiparati a quelli privati rispetto all'obbligo di comunicare preventivamente all'interessato (o, in alternativa, alla persona presso la quale sono raccolti i dati) una serie di informazioni (art. 13).

In primo luogo, è necessario segnalare le finalità e le modalità del trattamento cui sono destinati i dati.

Inoltre, vanno indicati gli estremi identificativi del **titolare** e del **responsabile** del trattamento; quando il titolare ha designato più responsabili, ne è indicato almeno uno. Devono essere chiarite, altresì, le modalità attraverso le quali è conoscibile, in modo agevole, l'elenco aggiornato dei responsabili. Non è meno importante la regola per cui bisogna menzionare i soggetti o le categorie di soggetti ai quali i **dati personali** potranno essere comunicati nel corso del trattamento, o che potranno venirne a conoscenza in qualità di responsabili o **incaricati**, delimitando il prevedibile ambito di diffusione.

L'interessato deve essere reso consapevole, poi, della gamma dei diritti che gli sono riconosciuti (v. *supra*, **Glossario,** voce *Interessato*).

Una regola di primario rilievo è quella che impone di chiarire, nell'informativa all'interessato, se la comunicazione dei dati da parte di costui a seguito di richiesta del titolare del trattamento abbia natura obbligatoria o facoltativa, precisando anche quali conseguenze derivino dall'eventuale rifiuto di rispondere. Questa previsione consente al singolo, cui sia stato domandato di fornire alcune informazioni che lo riguardano, di maturare piena consapevolezza in merito alla possibilità (e all'opportunità) di non trasmettere i pro-

pri dati e appare particolarmente utile quando titolare del trattamento sia una pubblica amministrazione. In questo caso, infatti, il privato potrebbe essere indotto a dedurre dalla posizione di intrinseca "superiorità" del suo interlocutore l'inesistenza di fatto di margini valutativi in ordine alla comunicazione delle informazioni. Laddove questa non sia indispensabile (ma soltanto utile) per l'espletamento dei compiti istituzionali connessi con lo svolgimento del trattamento, dunque, è doveroso che ciò sia adeguatamente evidenziato.

In generale, l'informativa può essere effettuata in forma scritta oppure orale. Tuttavia, quando titolare del trattamento è una pubblica amministrazione, è quanto mai opportuno (e forse addirittura necessario, in base ai principi di efficienza ed efficacia dell'attività amministrativa, che derivano da quello di buon andamento, di cui all'art. 97 della Costituzione) che essa avvenga per iscritto. È sufficiente, comunque, la predisposizione di appositi moduli prestampati, adattabili alle varie situazioni.

Per quanto riguarda l'obbligo di notificare in via preventiva al **Garante** l'intenzione di procedere al trattamento, esso di regola non opera a carico degli istituti scolastici. Il Codice, infatti, ha ridotto sensibilmente i casi in cui tale adempimento è necessario (art. 37) e nessuna delle fattispecie previste coinvolge, neanche indirettamente, compiti educativi o di istruzione; peraltro, il Garante, mediante l'emanazione di appositi provvedimenti, ha via via escluso l'obbligo della previa notificazione con riferimento a numerose tipologie di trattamento poste in essere dall'amministrazione. L'unica eccezione è prevista nell'art. 39, c. 1, lett. *a)*, del Codice, ove è stabilito che la notificazione al Garante debba avvenire laddove si verifichi la comunicazione di dati personali, non prevista da una norma di legge o di regolamento ed effettuata in qualunque forma, da parte di un soggetto pubblico ad altro soggetto pubblico.

La notificazione è inviata utilizzando il modello predisposto e reso disponibile dal Garante e gli viene trasmessa per via telematica, oppure mediante telefax o lettera raccomandata.

Quelle fin qui tratteggiate sono le regole che devono essere applicate in vista di qualsiasi trattamento. Ad esse si affiancano altri precetti, che pongono in capo all'amministrazione oneri in parte distinti, a seconda che il trattamento riguardi **dati sensibili** o comuni.

## IL TRATTAMENTO DEI DATI COMUNI

Il trattamento di dati non sensibili è consentito anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente, purché esso risulti funzionale allo svolgimento dei compiti istituzionali del soggetto pubblico titolare del trattamento stesso (art. 19, c. 1).

Per quanto concerne la comunicazione a terzi dei dati trattati, essa è consentita a condizioni diverse a seconda che il destinatario della comunicazione sia pubblico o privato. Precisamente, la comunicazione a soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento o è comunque necessaria per lo svolgimento di funzioni istituzionali (art. 19, c. 2). Invece, la comunicazione a privati (cui è equiparata la diffusione a una pluralità indifferenziata di soggetti) è ammessa unicamente quando è prevista da una norma di legge o di regolamento (art. 19, c. 3).

## IL TRATTAMENTO DEI DATI SENSIBILI

Il trattamento di dati sensibili è consentito esclusivamente se risulta autorizzato da espressa disposizione di legge, nella quale devono essere specificati le categorie di informazioni che possono essere trattate, i tipi di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. La disciplina di riferimento deve essere espressamente indicata anche nell'informativa resa all'interessato all'inizio del trattamento (art. 20).

Il legislatore ribadisce e rafforza (all'art. 22) alcuni criteri che rispecchiano principi generali (v. *supra*, I principi fondamentali). Si precisa, infatti, che il trattamento deve essere svolto secondo modalità idonee a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato. Inoltre, i dati eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Infine, con preciso riferimento ai soggetti pubblici si chiarisce che essi hanno il dovere di verificare periodicamente l'esattezza e l'aggiornamento dei dati sensibili, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento alle informazioni che l'interessato abbia eventualmente fornito di propria iniziativa.

I dati sensibili non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato.

Quelli idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo.

Nel caso di trattamento svolto mediante l'ausilio di mezzi elettronici, la **parola chiave** personale dell'incaricato deve essere modificata almeno ogni tre mesi.

## IL TRATTAMENTO DA PARTE DEGLI ISTITUTI SCOLASTICI

In generale, in base all'art. 95 del Codice, si considerano di rilevante interesse pubblico le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte in forma integrata.

Per quanto riguarda l'attività degli istituti scolastici, va chiarito che certamente rientrano fra le menzionate finalità di rilevante interesse pubblico, per esempio, gli interventi di sostegno psico-sociale e di formazione in favore di giovani, la gestione di asili nido e di mense scolastiche, la fornitura di sussidi, contributi e materiale didattico.

Nell'informativa all'interessato, il titolare pubblico del trattamento deve fare esplicito riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento.

Una disposizione del tutto particolare è quella contenuta nell'art. 96 del Codice, relativo al trattamento di dati relativi agli studenti. Vi si prevede 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 e altri pertinenti dati personali, diversi da quelli sensibili o giudiziari. L'indicazione dei dati in tal senso comunicati deve essere contenuta nell'informativa resa all'interessato. Qualora ciò si verifichi, i dati possono essere successivamente trattati esclusivamente per le finalità precedentemente esplicitate.

Un'ultima notazione riguarda il trattamento di dati sensibili. Il Garante, in proposito, ha recentemente escluso che gli istituti scolastici debbano o possano dotarsi di un autonomo regolamento sul punto, risultando sufficientemente dettagliate le disposizioni contenute nel Codice. L'unico intervento di normazione attuativa ammissibile è costituito dalla prossima emanazione di un regolamento ministeriale, il quale dovrà risultare conforme al parere espresso dal Garante stesso.

# LA RESPONSABILITÀ PER LA VIOLAZIONE DELLE REGOLE SUL TRATTAMENTO DEI DATI PERSONALI

## LA RESPONSABILITÀ AMMINISTRATIVA

In generale, la mancata assunzione delle misure di sicurezza e la violazione della disciplina contenuta nel Codice determina la comminazione di sanzioni amministrative di natura pecuniaria (artt. 161-166 del Codice).

Per quanto riguarda il comportamento degli istituti scolastici pubblici, le principali infrazioni rientranti fra gli illeciti amministrativi si configurano in relazione alla violazione totale o parziale dell'obbligo di informativa all'**interessato** al momento dell'avvio del **trattamento** e all'indebita cessione a terzi dei dati trattati. Altri casi rilevanti concernono la mancata collaborazione con il **Garante**.

I controlli, cui può conseguire la comminazione della sanzione amministrativa, sono effettuati principalmente dal Garante o dalla Guardia di Finanza. Essi si svolgono sulla documentazione presente *in loco* e sulla conformità a quanto dichiarato nel **documento programmatico sulla sicurezza**.

## LA RESPONSABILITÀ PENALE

Nei casi più gravi, scatta la responsabilità penale in capo al **titolare** del trattamento ed eventualmente al **responsabile** e all'**incaricato** (artt. 167-172 del Codice).

In primo luogo, è prevista la pena detentiva per chi viola i principi applicabili al trattamento (v. *supra*, **I principi fondamentali** e **Le regole per il trattamento dei dati da parte delle pubbliche amministrazioni**). Affinché la sanzione possa essere comminata, però, devono ricorrere due importanti presupposti: che l'agente perseguisse l'intento di procurare a sé o ad altri un profitto o di arrecare un danno a terzi e che dalla condotta sia effettivamen-

te derivato un pregiudizio. Inoltre, se il fatto costituisce un reato più grave di quello punito nel Codice, resta salva l'applicazione della sanzione più severa prevista in altra sede normativa.

La pena detentiva è prevista, salvo che il fatto costituisca più grave reato, anche per chi comunica false informazioni o produce documenti falsi al Garante.

Analoga sanzione opera in capo a chi non abbia rispettato il provvedimento con cui il Garante, dopo essere stato adito mediante ricorso per la supposta violazione dei diritti dell'interessato, abbia disposto, in via cautelare, il blocco temporaneo o la sospensione di alcune operazioni del trattamento oppure abbia ordinato, in seguito all'accertamento dell'illegittimità del trattamento stesso, la cessazione della condotta dannosa.

Infine, sono previste congiuntamente sanzioni pecuniarie e detentive in capo al soggetto che, essendo tenuto ad assumerle, ometta di adottare le misure di sicurezza minime. In questo caso, però, il Garante ha la facoltà di dettare prescrizioni ai fini della regolarizzazione dell'attività, fissando per l'adempimento un termine non superiore a sei mesi (prorogabile solo nelle fattispecie contraddistinte da peculiare complessità). Se l'autore del reato si adegua, la pena è convertita nella corresponsione di una somma di denaro e, a seguito del pagamento, il reato è estinto.

In caso di sospetta commissione di reati, i controlli possono essere svolti anche dalla Polizia giudiziaria.

## LA RESPONSABILITÀ CIVILE

Nell'immediato, la norma forse maggiormente significativa in tema di responsabilità per violazione delle norme del Codice è quella di cui all'art. 15, in cui si precisa che chiunque cagiona pregiudizio ad altri per effetto del trattamento di **dati personali** è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile, che concerne la responsabilità civile per i danni prodotti nell'esercizio di attività pericolose. Dato il rischio intrinsecamente correlato all'assunzione di iniziative operative in taluni settori, il legislatore dispone che, laddove l'agente abbia provocato una lesione in capo a terzi, ai fini della costituzione dell'obbligo risarcitorio si produca l'inversione dell'onere della prova.

Poiché anche il trattamento di dati personali è considerato attività pericolosa, ne consegue che, in caso di produzione di danno a un terzo, quest'ultimo, in vista del risarcimento del pregiudizio subito, dovrà dimostrare esclu-

sivamente di avere patito una lesione (danno) a seguito dell'operato del titolare del trattamento (nesso di causalità). Invece, egli non sarà tenuto a dimostrare l'esistenza della colpa in capo alla controparte: spetterà al titolare del trattamento (e, in quanto anch'essi chiamati in causa, al responsabile e all'incaricato) dimostrare di avere assunto tutte le precauzioni idonee ad evitare il pregiudizio.

È importante sottolineare che è risarcibile anche il danno non patrimoniale.

# LA TUTELA DELLA RISERVATEZZA IN CASO DI ACCESSO AI DOCUMENTI AMMINISTRATIVI

## LA DISCIPLINA LEGISLATIVA

### LE NOZIONI FONDAMENTALI

Il diritto di accesso è il diritto dei soggetti privati, titolari di un interesse diretto, concreto e attuale corrispondente a una situazione giuridicamente protetta (quale, per esempio, l'intento di impugnare, in sede amministrativa o giurisdizionale, un provvedimento sfavorevole) collegata a un determinato documento amministrativo, di prendere visione o estrarre copia del documento medesimo.

La nozione di "documento amministrativo" è ampia e comprende ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi a uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse.

Queste definizioni sono attualmente contenute nell'art. 22 della legge n. 241 del 1990, recentemente modificata dalla legge n. 15 del 2005. La maggior parte delle modifiche introdotte dalla normativa del 2005 è destinata ad entrare in vigore dopo l'emanazione di un regolamento. Molto spesso, però, il legislatore si è limitato a prendere atto, recependolo, dell'orientamento interpretativo, relativo alla previgente versione della legge n. 241, espresso dalla giurisprudenza. Pertanto, è utile tenere conto fin d'ora della "nuova" formulazione delle previsioni.

# I CRITERI DI ARMONIZZAZIONE FRA ACCESSO E RISERVATEZZA

Della possibilità che sia esperita una richiesta di accesso ai documenti amministrativi contenenti dati riservati di terzi si occupano espressamente gli artt. 59 e 60 del Codice.

La prima delle due disposizioni si limita a rinviare, per la disciplina della materia, alla legge n. 241 del 1990 e ai regolamenti attuativi. L'unica precisazione interessante è quella per cui le attività correlata all'esecuzione di tale normativa – che sicuramente configura un **trattamento** di informazioni, data l'ampiezza di questa nozione – si considerano di rilevante interesse pubblico. Ciò concorre a legittimarne lo svolgimento anche in presenza del coinvolgimento di **dati sensibili**.

L'art. 60 è più specifico e concerne il trattamento di dati sensibili idonei a rivelare lo stato di salute o la vita sessuale dell'**interessato**. In quel caso, l'accesso è consentito se la situazione giuridicamente rilevante che l'aspirante accedente intende tutelare è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto fondamentale. Ai fini dell'accertamento del rilievo costituzionale degli interessi coinvolti nel caso concreto, sarà necessario, dunque, verificare quale sia l'interesse che l'istante intende proteggere mediante l'accesso, da un lato, e quale sia l'interesse connesso alla tutela della riservatezza del titolare del dato, dall'altro lato.

Nella "nuova" formulazione dell'art. 24, c. 7, della legge n. 241 del 1990 è contenuto un rinvio espresso all'art. 60 del Codice.

Nella stessa disposizione, poi, è menzionato, quale criterio generale di armonizzazione fra accesso e riservatezza, quello della stretta indispensabilità dell'apprendimento dei dati sensibili contenuti nella documentazione, in vista della predisposizione di adeguata tutela del proprio patrimonio giuridico.

Nonostante la legge non lo prospetti espressamente, uno strumento che in concreto può essere utile è l'accesso parziale. Precisamente, per garantire la tutela della riservatezza del titolare dei dati contenuti nell'atto, è possibile limitare l'accesso ad alcuni brani del documento oppure criptare le generalità dei soggetti ivi menzionati. È chiaro, però, che tale meccanismo non rappresenta una valida soluzione allorché il titolare delle informazioni sia comunque riconoscibile, nonostante l'eliminazione dei riferimenti alle sue generalità.

Invece, non pare realmente efficace lo strumento, talora valorizzato in

dottrina e applicato da una parte della giurisprudenza, della limitazione dell'accesso alla sola visione del documento, con esclusione dell'estrazione di copia. Infatti, nel momento in cui l'atto è stato mostrato all'istante, i dati che esso contiene gli sono stati resi noti, cessando di essere segreti. La mera visione dell'atto, dunque, costituisce già una lesione della riservatezza del titolare dei dati.

A volte, può essere utile differire l'accesso a un momento certo e determinato, ma successivo a quello della richiesta. Ciò di regola si verifica quando gli atti cui l'istante intende accedere fanno parte di una procedura complessa che non si è ancora conclusa (es. atti di un concorso o di una procedura selettiva).

## IL REGOLAMENTO MINISTERIALE PER IL SETTORE DELLA SCUOLA

Nel regolamento del Ministero della pubblica istruzione n. 60 del 10 gennaio 1996 (in vigore dal 3 marzo dello stesso anno) è indicata una serie di documenti, rispetto ai quali l'accesso è (tendenzialmente) escluso.

Una prima gamma di ipotesi riguarda gli atti contenenti dati sanitari: naturalmente, vi sono compresi non solo i certificati medici relativi alle assenze degli alunni (v. *infra*, I principali problemi in ambito scolastico), ma anche quelli prodotti dai dipendenti della scuola e ogni altro documento idoneo ad attestare le condizioni psico-fisiche delle persone (es. documenti prodotti dai lavoratori per ottenere dispense dal servizio, visite fiscali di controllo, ecc.). D'altra parte, in giurisprudenza si è ammesso l'accesso di un terzo alla documentazione sanitaria presentata da un dipendente scolastico al fine di ottenere l'esclusione dalla graduatoria del personale soprannumerario in ragione del proprio handicap; nel caso di specie, il terzo era un soggetto inserito nella menzionata graduatoria, che voleva verificare la regolarità dell'esclusione del collega.

Sono tendenzialmente sottratte all'accesso anche le schede contenenti informazioni personali di natura psico-attitudinale; al contrario, devono essere resi pubblici i criteri generali della medesima natura individuati dall'amministrazione in vista dell'effettuazione di procedure selettive.

Per quanto concerne i documenti relativi al rapporto di lavoro esistente fra l'istituto scolastico e i suoi dipendenti, questi entrano a far parte del fascicolo personale di costoro; pertanto, normalmente l'accesso è consentito esclusivamente all'**interessato**. Questa regola si applica alle relazioni informative che il dirigente scolastico è tenuto a redigere in varie occasioni (es. a conclusione del periodo di prova, oppure in vista di un trasferimento, o ancora nel corso di procedimenti disciplinari), nonché ai rapporti conclusivi di indagini ispettive sull'operato di singoli docenti.

Sono per lo più coperti da riserbo anche gli atti con cui il dirigente scolastico sia entrato in contatto con l'autorità giudiziaria, sia penale che amministrativo-contabile, per i giudizi di responsabilità (es. istanze o relazioni prodotte o richieste dal giudice penale o dalla Corte dei Conti e rientranti nel fascicolo personale del dipendente).

# I PRINCIPALI PROBLEMI IN AMBITO SCOLASTICO

# LA PUBBLICAZIONE DEI VOTI E DEGLI ESITI DEGLI SCRUTINI

In primo luogo, va chiarito che questa tipologia di atti non contiene **dati sensibili** degli studenti.

Inoltre, non si ravvisa nemmeno un problema di tutela della riservatezza in senso stretto. Anzi, le informazioni contenute negli atti che costituiscono l'esito degli scrutini sono pubbliche per legge.

Ciò è stato ripetutamente chiarito in varie comunicazioni dal **Garante**, il quale ha anche escluso che sia necessario consegnare tale documentazione in busta chiusa al solo **interessato**.

Nella medesima prospettiva si pone il Ministero per l'istruzione, che, in numerose ordinanze, ha precisato 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". Risulterebbero, dunque, eccessivamente garantistiche le soluzioni talora proposte, per cui ci si potrebbe limitare ad esporre la lista degli studenti promossi, omettendo qualsiasi indicazione relativamente a quelli respinti. In questo contesto, risulta interessante per la settorialità del suo contenuto, l'ordinanza n. 35 del 4 aprile 2003, in cui il Ministro ha sollecitato l'attenzione e la sensibilità dei dirigenti scolastici affinché sia evitata la pubblicazione, congiuntamente con le valutazioni sul profitto scolastico, di indicazioni lesive della riservatezza degli alunni disabili.

Qualche problema potrebbe sorgere dall'esigenza di proteggere le riservatezza degli alunni rispetto alle loro opinioni religiose. In proposito, il Garante ha sottolineato che mai sono stati emanati provvedimenti atti a proibire agli alunni di rendere nota la fede religiosa, asserendo che il necessario rispetto della volontà di ciascuno di mantenere riservate alcune informazioni sulla propria persona non va confuso con la libertà, costituzionalmente protetta, di manifestare liberamente le proprie convinzioni, anche di natura religiosa. Si tratta, però, di una posizione un po' "ambigua", che dà per scontato che, a monte della pubblicazione dei dati relativi alle opinioni religiose del ragazzo, vi sia una sua libera scelta. Ciò, tuttavia, non si verifica nel caso della pubblicazione degli esiti degli scrutini. Pertanto, una parte della dottrina, pur riconoscendo che il **trattamento** di questa categoria di dati da parte

delle scuole è autorizzata da una disposizione di legge, precisa che essi non possono essere ulteriormente divulgati a soggetti pubblici e privati (se non, in casi del tutto particolari, ai servizi sociali a fini di protezione del preminente interesse dello studente minorenne). Se ne desume che nei tabelloni degli esiti degli scrutini, che vengono esposti al pubblico, non potrebbe comparire alcun riferimento alla frequenza dell'insegnamento di religione (con la relativa valutazione o la scritta "*non si avvale*"). Taluno ritiene che questo orientamento trovi conferma nel fatto che la valutazione del profitto relativo all'insegnamento di religione non è contenuta, come quella relativa al profitto nelle altre materie, nella pagella, bensì in una scheda a sé stante. Tuttavia, la tesi espressa dal Ministero dell'Istruzione è di segno opposto: si sostiene che la votazione relativa all'insegnamento della religione cattolica debba essere pubblicato insieme all'esito degli scrutini, poiché tale pubblicazione non è suscettibile di rivelare l'intimo convincimento dello studente, ma solo il suo interesse per l'apprendimento della disciplina.

## I DATI TRATTATI A FINI DIDATTICI

Naturalmente, non si può escludere che emergano **dati personali**, a volte addirittura sensibili, negli elaborati prodotti dagli alunni. In questo caso, è assolutamente necessario che le informazioni raccolte non siano ulteriormente e indiscriminatamente divulgate, fatta salva l'eventuale comunicazione a soggetti pubblici (es. servizi sociali) nell'esclusivo interesse dei minori coinvolti. Questa regola corrisponde, prima ancora che alla normativa in materia di trattamento dei dati, a principi deontologici e di sensibilità sociale. Comunque, può essere opportuno cercare di delimitare molto attentamente i casi in cui si richieda agli studenti di descrivere aspetti intimi della loro vita personale o famigliare.

In questo contesto, è, ovviamente, particolarmente "delicata" la posizione degli insegnanti di sostegno, che, in ragione delle mansioni che sono chiamati a svolgere, inevitabilmente vengono a conoscenza di dati sensibili degli alunni loro affidati. Essi sono evidentemente tenuti, sul piano deontologico e giuridico, a mantenere il segreto sulle informazioni apprese. La scuola dovrebbe provvedere alla loro nomina quali **incaricati** del trattamento, evidenziando la peculiarità del loro ruolo rispetto a quello degli altri docenti.

Per quanto concerne il trasferimento delle informazioni da parte della scuola che le ha originariamente sottoposte a trattamento ad altri istituti scolastici, esso è consentito, in base alle regole generali (v. *supra*, **Le regole per il trattamento dei dati da parte delle pubbliche amministrazioni**). È necessario, dunque, che l'operazione sia funzionale allo svolgimento dei compiti istituzionali di entrambi i soggetti coinvolti e, qualora si tratti di dati sensibili, deve essere legislativamente autorizzata.

## IL PORTFOLIO

Il D. Lgs. n. 59/2004 prevede che per ciascun alunno sia redatto un *Portfolio*, cioè una cartella delle competenze individuali, costantemente aggiornata, idonea ad illustrare i progressi compiuti nell'ambito del percorso scolastico.

Esso può contenere vari tipi di documenti: dagli elaborati via via prodotti dallo studente alla documentazione medica che lo riguarda e certifica la presenza di stati patologici (per esempio, allergie), dalle dichiarazioni relative a eventuali stati di adozione o allontanamento dal Paese d'origine o comunque a esperienze svoltesi nel periodo della prima infanzia e idonee a incidere sulla crescita psico-fisica del minore alla descrizione di suoi disagi o paure, dalle notizie sulla religione professata a quelle sull'ambiente famigliare in cui è inserito. Può trattarsi, dunque, di dati anche sensibili.

Peraltro, le categorie di informazioni suscettibili di inserimento nel *Portfolio* molto difficilmente sono individuabili *a priori*, poiché manca un modello unitario a livello nazionale e ciascun istituto è dotato di ampia autonomia. Ne deriva la necessità di adottare la massima cautela nel trattamento dei dati e di attenersi rigorosamente ai principi contenuti nel Codice.

In proposito, il Ministero ha precisato che è legittimo inserire dati personali nel *Portfolio* soltanto se essi sono pertinenti e non eccedenti rispetto alla finalità complessiva del trattamento; i dati sensibili possono essere indicati esclusivamente se sono indispensabili alla valutazione e all'orientamento dell'alunno.

Inoltre, per garantire l'uniformità di trattamento fra gli studenti, ogni Istituto dovrà predisporre un modello di *Portfolio*, tenendo conto che si tratta essenzialmente di uno strumento didattico, in cui le informa-

zioni riservate possono essere inserite solo in via eccezionale e qualora strettamente indispensabile. La scuola, titolare del trattamento, deve impartire istruzioni in tal senso agli insegnanti che predispongono la cartella (che dovranno essere designati sicuramente quali incaricati e, ove dotati di poteri decisionali, anche quali responsabili del relativo trattamento).

I genitori o i soggetti esercenti la potestà sui minori interessati devono essere informati dello svolgimento del trattamento e possono chiedere sia l'aggiunta di dati ritenuti rilevanti, sia l'eliminazione di quelli indebitamente inseriti, secondo le regole generali.

Alla fine del corso di studi, il *Portfolio* deve essere consegnato allo studente, affinché costui lo depositi, ove ciò sia previsto, presso l'Istituto scolastico di grado successivo.

## I DATI RELATIVI ALLO STATO DI SALUTE DEGLI ALUNNI CONTENUTI NEI CERTIFICATI MEDICI

Come è noto, per le assenze protratte per un lasso di tempo sufficientemente lungo (attualmente, per più di 5 giorni) l'alunno interessato deve produrre il relativo certificato medico. È evidente che tale documento contiene dati sensibili; pertanto vanno rigorosamente applicate, ai fini della sua conservazione agli atti, le regole previste nel Codice per il trattamento di questo tipo di informazioni.

Precisamente, è necessario che del trattamento sia incaricato un soggetto determinato, che dovrà essere nominato dal dirigente scolastico quale **responsabile** del trattamento (v. *supra*, **Glossario,** alla voce corrispondente). Le generalità di costui devono essere comunicate a studenti e/o genitori.

Invece, non è in alcun caso ammessa la conservazione dei certificati medici all'interno del registro di classe.

## LA COLLABORAZIONE CON I SERVIZI SOCIALI

A volte, l'istituto scolastico è chiamato a collaborare con altri soggetti pubblici e ciò può comportare la trasmissione di dati, anche sen-

sibili, degli alunni.

Il caso più frequente è quello in cui la scuola sia contattata dai servizi sociali, che desiderano apprendere informazioni sulle condizioni psicofisiche di un alunno minorenne per verificare eventuali situazioni di degrado o maltrattamento. In questa eventualità, ove risulti l'intento esclusivo di salvaguardare l'integrità personale del ragazzo nell'ambito delle funzioni istituzionali dell'ufficio, i dati dovranno essere comunicati. È chiaro che tutti i soggetti a vario titolo coinvolti nella vicenda sono vincolati al segreto da regole giuridiche e deontologiche.

Le medesime considerazioni valgono qualora sia il dirigente dell'istituto scolastico, d'accordo con i docenti, ad attivare i servizi sociali segnalando condizioni di difficoltà degli studenti.

## LA COMUNICAZIONE A TERZI DEI DATI RELATIVI AL PROFITTO DEGLI STUDENTI

Un'altra fattispecie rilevante sul piano applicativo concerne la richiesta dei nominativi e dei recapiti degli studenti diplomati (talora, con l'indicazione della votazione conseguita) da parte di imprese o enti, operanti nel corrispondente settore professionale. In questa eventualità, si applica la disposizione contenuta nell'art. 96 del Codice (su cui v. *supra*, Il trattamento da parte degli istituti scolastici). Non è escluso, però, che quella previsione possa essere interpretata "estensivamente", al fine di consentire l'adozione di soluzioni "flessibili". Infatti, la comunicazione delle informazioni di cui all'art. 96 del Codice avviene nell'interesse degli studenti, che aspirano a un celere e conveniente inserimento nel mondo del lavoro a conclusione del loro ciclo di studi; tuttavia, non sempre essi sono pienamente consapevoli *a priori* della possibilità che le imprese si rivolgano direttamente alla scuola per ottenere i nominativi di eventuali futuri dipendenti. Pertanto, pare ragionevole (e conforme alla *ratio* della norma) consentire che sia l'istituto scolastico ad assumere l'iniziativa, chiedendo per iscritto agli studenti interessati l'autorizzazione alla trasmissione delle informazioni che li riguardano esclusivamente agli operatori del settore che ne facessero richiesta e al mero fine di avviamento professionale o approfondimento culturale.

# LA COMUNICAZIONE DEI DATI RELATIVI AGLI STUDENTI PER MOTIVI DI RICERCA O DI STUDIO

Merita un cenno l'eventualità che all'istituto scolastico sia chiesto di comunicare dati personali relativi a ex-alunni da parte di soggetti che intendono utilizzare quelle informazioni nell'ambito di ricerche di carattere storico. Qualora l'obbiettivo della ricerca sia indicato esaurientemente dall'istante e siano fornite adeguate assicurazioni sulla correttezza e trasparenza dell'uso che si intende effettuare delle informazioni, possono trovare applicazione le disposizioni del Codice (artt. 97-99) che riconoscono la compatibilità del trattamento a fini storici con i diversi scopi per i quali i dati sono stati originariamente raccolti e consentono che tale trattamento si protragga anche oltre il periodo necessario per conseguire gli obbiettivi propri del trattamento "originario". In vista della realizzazione della ricerca storica, i dati personali possono essere ceduti a terzi anche dopo la conclusione del trattamento "originario". Comunque, è opportuno che gli istituti scolastici evitino di consegnare "in blocco" grandi quantità di informazioni: le modalità e i termini della comunicazione devono essere concordati con l'istante, tenendo conto anche della natura (riservata o addirittura sensibile) dei dati coinvolti.

Analoghe precauzioni devono essere assunte per lo svolgimento di ricerche a scopo scientifico coinvolgenti gli studenti attualmente iscritti. In tal senso si è espresso il Garante all'inizio del 2005, vietando la pubblicazione di una ricerca svolta da una laureanda in sociologia, la quale, con la collaborazione di una scuola elementare ma senza darne previa informativa ai genitori (anche con riferimento alla facoltatività dell'adesione all'iniziativa), aveva sottoposto gli alunni a una rilevazione sul maltrattamento infantile, idonea a rivelare i loro dati personali, talora anche sensibili.

# L'ACCESSO DEGLI ALUNNI O DEI LORO GENITORI AGLI ELABORATI, AI REGISTRI DI CLASSE E AI VERBALI DEI CONSIGLI DI CLASSE

È abbastanza frequente che i genitori degli alunni (o direttamente gli studenti, se maggiorenni) si rivolgano all'istituto scolastico per accedere agli elaborati prodotti a scuola (es. compiti in classe).

Sicuramente il diritto di accesso deve essere riconosciuto sugli elaborati propri o del proprio figlio.

Per quanto riguarda la possibilità di accedere ai compiti altrui, in dottrina e in giurisprudenza amministrativa sono state additate varie soluzioni a seconda dei casi.

Di regola, l'accesso agli elaborati altrui è escluso, poiché fra le prestazioni degli alunni non si ravvisa un rapporto di reciproca comparazione (quale quello che sussiste, per esempio, fra i candidati che partecipano a un concorso): ne consegue l'impossibilità di ravvisare un interesse giuridicamente rilevante alla conoscenza del livello di preparazione di terzi.

Si ritiene che la situazione possa cambiare (benché non sempre la giurisprudenza abbia condiviso questo orientamento) se l'interessato intende verificare la correttezza del metro valutativo adottato dal docente. Precisamente, qualora l'intento dell'istante sia di dimostrare di essere stato vittima di una disparità di trattamento rispetto agli altri studenti, egli può essere autorizzato ad esaminare gli elaborati altrui. In questa ipotesi, non è detto che si ponga un problema di tutela della riservatezza (dipende in massima parte dal contenuto dell'elaborato); peraltro, potrebbe essere comunque opportuno oscurare il nominativo dell'autore del compito, il quale può essere scelto non necessariamente fra i compagni di classe dell'interessato, ma fra tutti gli alunni, anche di classi diverse, assegnati al medesimo docente.

Per quanto riguarda l'accesso ai registri di classe, pare ragionevole seguire i criteri ora indicati. Pertanto, è consentito l'accesso alle annotazioni che riguardano personalmente l'interessato; è escluso, al contrario, l'accesso alle annotazioni che riguardano terzi, a meno che l'intento dell'istante sia quello di accertare eventuali disparità di trattamento. Nella seconda ipotesi, però, potrebbe essere opportuno proteggere la riservatezza del titolare dell'informazione criptando il suo nominativo.

Del tutto analoga sembra anche la situazione relativa alle richieste di accesso ai verbali dei consigli di classe, allorché l'istanza di pubblicità sia presentata da un soggetto esterno al collegio (studente maggiorenne o genitore di quello minorenne). Qualora, invece, l'istanza sia presentata da un componente il collegio, dato il suo ruolo istituzionale non gli si possono opporre esigenze di riservatezza altrui per limitare quantitativamente le informazioni cui egli ha accesso, salvo l'obbligo in suo capo (che deriva dalle regole di correttezza) di mantenere, se del caso, il riserbo sui dati appresi.

## L'ACCESSO DEL DOCENTE INTERESSATO ALLE "LETTERE DI PROTESTA"

Può accadere che gli studenti maggiorenni o i genitori di quelli minorenni, in presenza di scontri o tensioni con uno o più docenti, decidano di mettere per iscritto le loro rimostranze, inviando all'uopo una lettera al dirigente scolastico con l'intento di ottenere l'attivazione di un procedimento disciplinare o, quanto meno, di misure idonee a determinare la cessazione dei comportamenti ritenuti illegittimi.

In questo caso, l'insegnante coinvolto certamente ha interesse ad apprendere i termini delle rimostranze avanzate nei suoi confronti e il suo diritto alla conoscenza rispecchia indubbiamente anche il principio costituzionale del giusto procedimento. D'altra parte, non sarebbe corretto sottovalutare il diritto alla riservatezza dei soggetti che si sono attivati, i quali potrebbero essere esposti, per così dire, a "ritorsioni" da parte del docente.

Pertanto, può essere utile applicare in via analogica un criterio che la giurisprudenza amministrativa ha adottato in altri campi (es. accesso del datore di lavoro agli atti di denuncia dei suoi dipendenti per infrazioni alle norme di sicurezza e sulla regolarità contributiva), ammettendo l'accesso dell'interessato alla documentazione, previa cancellazione delle generalità dei mittenti e di ogni elemento tale da consentirne il riconoscimento.

## IL PROBLEMA DELLA TUTELA DELLA RISERVATEZZA NELLE CIRCOLARI SCOLASTICHE

Il Garante ha precisato che anche le circolari scolastiche devono rispettare il Codice e non possono, pertanto, contenere dati personali riservati degli studenti che consentano di risalire, sia pure in modo indiretto, alla loro identità.

In un caso di specie, è stato accolto il ricorso presentato dai genitori di un minore nei confronti di una scuola che aveva inviato a tutte le famiglie una comunicazione relativa ai provvedimenti disciplinari adottati in occasione di litigi tra studenti. Poiché nella circolare erano contenuti elementi suscettibili di rendere possibile l'identificazione del figlio, gli istanti si erano rivolti al Garante per impedire che l'istituto procedesse a un'ulteriore diffusione del documento, ove, tra l'altro, si faceva riferimento a comportamenti ritenuti violenti. Il Garante ha riconosciuto la lamentata lesione della riservatezza e della dignità del ragazzo, ammettendo che ciò avrebbe anche potuto provocare riflessi sulla sua personalità e su quella di altri minori iscritti allo stesso istituto. Si è chiarito che il diritto - dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere in ogni caso bilanciato con l'esigenza di tutelare la personalità dei minori.

Comunicazioni come quelle considerate nella vicenda segnalata possono avvenire, dunque, esclusivamente se l'istituto scolastico garantisce l'omissione o la conversione in forma generica dei riferimenti originariamente suscettibili di permettere l'individuazione degli interessati.

## LE IMMAGINI FOTOGRAFICHE E FOTOCINEMATOGRAFICHE

Spesso gli istituti scolastici raccolgono o conservano immagini fotografiche o filmati che ritraggono gli studenti mentre svolgono varie attività, non necessariamente curricolari. Queste operazioni configurano certamente un trattamento di dati personali ed è assai consistente la tesi in base alla quale la riproduzione di immagini degli individui coinvolge comunque dati sensibili di costoro (si pensi all'idoneità dell'immagine a rivelare l'origine razziale o lo stato di disabilità).

Pertanto, la raccolta di tali informazioni da parte delle scuole è ammissibile esclusivamente previa idonea informativa alle famiglie

degli alunni (e/o a questi, se maggiorenni) e soltanto se emerge con chiarezza un nesso logico e funzionale fra tale operazione e i compiti istituzionali dell'ente.

## L'INSTALLAZIONE DI SISTEMI DI VIDEOSORVEGLIANZA

La disciplina generale in materia di sistemi di video sorveglianza è contenuta, oltre che nel Codice, nel provvedimento generale del Garante emanato in data 29 aprile 2004.

Vi si precisa che tale operazione può avvenire esclusivamente nel rispetto dei principi di liceità (anche in relazione alle disposizioni a protezione dei dipendenti dell'ente titolare del trattamento, contenute nell'art. 4 dello Statuto dei lavoratori), necessità e proporzionalità del trattamento e soltanto in vista della realizzazione dei fini istituzionali del titolare del trattamento. Particolare importanza assume il principio di necessità, poiché l'installazione di sistemi di videosorveglianza rappresenta una consistente limitazione delle libertà fondamentali (tra cui, *in primis*, il diritto alla riservatezza) dei singoli. Pertanto, essa si giustifica solo a fronte di serie esigenze di prevenzione e/o repressione di comportamenti gravemente illegittimi.

Se possibile, quindi, il sistema va conformato fin dall'origine in modo da impedire l'elaborazione di immagini di persone riconoscibili e comunque deve essere predisposta la cancellazione periodica delle immagini registrate. Inoltre, le telecamere vanno installate, a pena di illegittimità del trattamento, solo se davvero l'area interessata è sottoposta a reale pericolo: tale valutazione spetta, naturalmente, al titolare del trattamento. L'informativa agli interessati deve essere effettuata mediante l'affissione di cartelli collocati nella zona videosorvegliata (reperibili in *fac-simile* nel sito internet www.garanteprivacy.it).

Alla luce dei principi indicati, che comportano la leale informazione dei soggetti coinvolti nel trattamento, suscita perplessità l'installazione di telecamere finte o non funzionanti. Infatti, nonostante in questo caso non si ravvisi alcun trattamento di dati in senso tecnico, appare palesemente leso il principio di correttezza.

Per quanto riguarda la videosorveglianza nei locali scolastici, oltre ai profili segnalati è necessario tenere nella massima considerazione l'esi-

genza di proteggere la riservatezza degli studenti, soprattutto in quanto si tratta (almeno, per la maggior parte) di persone minorenni. Di conseguenza, l'ambito di ammissibilità del trattamento deve essere attentamente delimitato. Per esempio, si ritiene che l'operazione si possa giustificare a fronte della commissione di atti vandalici all'interno dell'istituto, ma solo con riferimento all'area coinvolta ed esclusivamente nell'orario di chiusura.

# IL TRATTAMENTO "INFORMATICO"

## PREMESSA

Come in parte si è già visto (v. *supra*, **Glossario**, voce ***Misure minime***), il Codice dedica molta attenzione alle modalità della gestione informatica dei dati personali, che vengono nettamente distinte da quelle richieste per il trattamento cartaceo. È opportuno, dunque, esaminare attentamente i principali profili di questa tematica.

Il trattamento effettuato *con* ***strumenti elettronici*** è consentito solo se sono adottate alcune **misure minime**.

## L'AUTENTICAZIONE

In primo luogo, deve essere predisposta l'**autenticazione informatica** per gli incaricati del trattamento, i quali devono essere dotati di un codice per l'identificazione (associato a una **parola chiave** riservata) oppure di un dispositivo di autenticazione riservato (eventualmente associato a un codice identificativo o a una parola chiave). In alternativa, l'autenticazione può operare mediante l'utilizzo di una caratteristica biometrica dell'incaricato (eventualmente associata a un codice identificativo o a una parola chiave). Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi. Per quanto concerne la parola chiave, quando è prevista dal sistema di autenticazione, essa è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo per-

metta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi.

Inoltre, è necessaria l'adozione di procedure di gestione delle **credenziali di autenticazione**. Queste devono essere disattivate, salvo qualora fossero state preventivamente autorizzate per soli scopi di gestione tecnica, ove non siano utilizzate da almeno sei mesi oppure se l'incaricato perde le qualità che gli consentivano l'accesso ai dati.

Fra le istruzioni impartite agli incaricati rientra la prescrizione di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in loro possesso ed uso esclusivo. Devono, poi, essere impartite idonee e preventive disposizioni scritte, volte a individuare le modalità con le quali il titolare può assicurare la disponibilità di dati o degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso, la custodia delle copie delle credenziali è organizzata garantendone la segretezza e individuando preventivamente per iscritto i soggetti chiamati ad assicurarne in concreto la salvaguardia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Particolare cautela deve essere adottata per il trattamento di dati sensibili, cui devono essere applicate tecniche di cifratura, codici identificativi o altre soluzioni che li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

## SALVATAGGI E PROTEZIONE DAI TRATTAMENTI ILLECITI

L'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici deve essere sottoposta ad aggiornamento periodico, con cadenza almeno annuale. I soggetti indicati possono essere elencati anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

È molto importante assicurare la protezione dei dati rispetto a

trattamenti illeciti, ad accessi non consentiti e a virus (contro i quali sono attivati adeguati strumenti elettronici, da aggiornare con cadenza almeno semestrale). A questo fine, devono essere impartite istruzioni agli incaricati perché lo strumento elettronico non sia lasciato incustodito e accessibile durante una sessione di trattamento e in vista della custodia e dell'uso dei supporti rimovibili su cui sono memorizzati i dati. Questi ultimi, ove servano al trattamento di dati sensibili, se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

Devono essere adottate apposite procedure scritte per la custodia di copie di sicurezza, nonché per il ripristino della disponibilità dei dati e dei sistemi. Pertanto, sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. Per prevenire i rischi di deterioramento, è consigliabile che le cassette su cui è effettuato il salvataggio dei dati siano sostituite frequentemente; i nastri devono essere attentamente conservati e sarebbe opportuno realizzarne una copia, da conservare in luogo diverso. Come si è visto (v. *supra*, ***Glossario***), è anche predisposto e periodicamente aggiornato il **documento programmatico sulla sicurezza**.

Qualora le misure minime di sicurezza siano predisposte avvalendosi della collaborazione di soggetti esterni alla struttura del titolare del trattamento, costui deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni vigenti.

Inoltre, se gli strumenti elettronici di cui il titolare dispone non consentono (in tutto o in parte) l'immediata applicazione delle misure minime per obiettive ragioni tecniche, egli deve indicare tali ragioni in un documento a data certa da conservare presso la propria struttura. In questo caso, il titolare adotta nel frattempo ogni possibile misura di sicurezza praticabile. Il termine ultimo per l'adeguamento è fissato ad oggi al 31 marzo 2006.

## L'UTILIZZO DEGLI STRUMENTI INFORMATICI DA PARTE DEGLI ALUNNI

Negli istituti scolastici, non è infrequente che agli alunni sia consentito l'accesso a un laboratorio informatico per motivi di studio. In tal caso, le **banche di dati** utilizzate dagli uffici amministrativi devono essere mantenute nettamente separate dai *files* di uso comune impiegati a fini didattici e devono essere apprestate idonee garanzie, atte ad evitare che i ragazzi vi possano accedere. Nell'ambito della rete informatica locale, dunque, si distinguono due settori, uno dedicato alle attività di segreteria (nell'ambito delle quali – come già si è segnalato: v. *supra*, *La riservatezza…a scuola* – vanno tenute distinte la gestione dei dati relativi agli alunni e quella dei dati relativi ai dipendenti dell'istituto), l'altro dedicato alla didattica.

Poiché assai difficilmente le attività svolte a scopi didattici dagli studenti si configurano come trattamento di dati personali, in generale nulla impedisce che sia assegnata loro una parola chiave cumulativa.