Gli adempimenti e gli obblighi per le Istituzioni scolastiche in materia di Privacy: il Documento Programmatico per la Sicurezza e i compiti del Direttore dei Servizi Generali ed Amministrativi

A cura di Patrizia Pavatti – Dirigente Scolastico Direzione Regionale per il Friuli Venezia Giulia

1. Premessa

Il Codice in materia di protezione dei dati personali, D.Lgs. n. 196 del 30 giugno 2003, è entrato in vigore il 1° gennaio 2004, aggiornando ed ampliando la disciplina già regolata in precedenza dalla legge n. 675 del 31 dicembre1996.

L'ampliamento della disciplina in materia di protezione e trattamento dei dati personali prevede l'estensione a tutti i soggetti pubblici e privati dell'applicazione delle misure minime di sicurezza entro la data del 31 dicembre 2004.

Tra queste misure, particolare rilevanza viene data alla redazione del Documento Programmatico per la Sicurezza (DPS), che corrisponde ad una mappatura della situazione esistente, da mettere a norma e da registrare nel Documento Programmatico. Tale adempimento deve essere assolto da tutti i titolari di trattamento di dati sensibili e/o giudiziari effettuato con strumenti elettronici. Risulta evidente che le Istituzioni scolastiche si trovano nella fattispecie prevista dalla norma, in quanto il sistema di archiviazione e di trattamento dei dati è ormai informatizzato in tutti gli uffici, in parte attraverso la rete intranet ministeriale, che ne conserva la banca dati, in parte attraverso programmi interni all'Istituto. Va precisato che le Istituzioni scolastiche sono tra i soggetti che per la prima volta, entro la data del 31 dicembre 2004, sono obbligati a redigere il DPS, a differenza, quindi, dei soggetti che, già in precedenza, in base alla legge n. 675/1996, erano tenuti a dotarsi del testo di ricognizione dei rischi, indicando gli interventi previsti a tutela della sicurezza dei dati.

Ciò significa che il primo Documento programmatico per la Sicurezza è da considerarsi un documento "base", suscettibile di successivi aggiornamenti ed ampliamenti in relazione alla registrazione dei provvedimenti adottati e delle modifiche effettuate successivamente.

E' necessario, comunque, riflettere sul fatto che la tematica Privacy non deve essere considerata un'incombenza che va a gravare ulteriormente gli impegni dell'Istituto scolastico, bensì inserirsi in una dimensione di cultura della sicurezza per la tutela del cittadino e di chi, a qualsiasi titolo, conosce e trattiene dati personali e sensibili.

Il dato ha a che fare con la Documentazione. Una corretta documentazione produce conoscenza e informazione. Il dato assume rilevanza nel momento in cui diventa informazione impregnata di significato. Un elenco di nomi non è significativo, ma lo diventa nel momento in cui un nome particolare fornisce una determinata informazione. E poiché quella informazione riguarda una persona, deve essere salvaguardato il diritto del cittadino alla riservatezza, alla privacy appunto.

2.I soggetti

I soggetti che effettuano la protezione e il trattamento dei dati si distinguono nelle seguenti figure[1]: **il titolare** del trattamento, che coincide con il rappresentante legale dell'Istituto scolastico; **il responsabile** del trattamento, che può essere nominato dal titolare ovvero può coincidere con il titolare medesimo. Qualora venga designato un responsabile, questi dovrà dimostrare di possedere capacità ed affidabilità in materia di sicurezza. Solitamente la figura del responsabile, attese le specifiche competenze e le funzioni attribuite dal ruolo[2], coincide con il Direttore dei Servizi Generali e Amministrativi. E' comunque prevista la possibilità di nomine di responsabilità plurima, laddove la particolare complessità organizzativa determini una suddivisione di compiti.
Il responsabile, a sua volta, nomina **gli incaricati** del trattamento, i quali devono scrupolosamente attenersi alle consegne ricevute dal responsabile. Le istruzioni per il responsabile e per gli incaricati devono essere impartire per iscritto con l'individuazione puntuale dei compiti assegnati e dell'ambito di trattamento consentito. Solitamente gli incaricati coincidono con gli Assistenti Amministrativi, in quanto le segreterie scolastiche sono il luogo dell'Istituto in cui vengono di fatto conservati e trattati i dati del personale, degli alunni e delle famiglie. Particolare attenzione va riposta anche nella figura strumentale di sostegno all'handicap, qualora nominata, poiché tratta i dati sensibili degli alunni diversamente abili, tiene i contatti con l'azienda sanitaria, l'assistenza sociale e le famiglie e sovrintende i gruppi di lavoro sull'handicap. Tale figura dovrebbe essere adeguatamente formata sul Codice Privacy per poter coordinare e istruire i docenti sul trattamento dei dati sensibili.

2. Il trattamento

I Programmi informatici in uso nelle segreterie sono per una parte forniti dal Ministero, collegato agli istituti attraverso il gestore del sistema con la rete SIMPI, attiva in determinati periodi per aree specifiche. Il Programma SISSI, fornito dal Ministero alle segreterie scolastiche, contiene i dati personali e sensibili, relativi agli alunni, al personale, al bilancio, al magazzino e alla retribuzione. I dati vengono inseriti ed aggiornati in locale. Vi è poi un diffuso utilizzo di altri Programmi, oltre agli applicativi Word e Excel, ad esempio nella compilazione del modello di previsione per la richiesta delle ore del docente di sostegno per gli alunni in situazione di handicap, in cui compare anche l'indicazione della diagnosi. Molteplici sono inoltre le attività d'ufficio riferite al personale e agli alunni con dati che testimoniano della religione, etnia, stato civile, maternità e quant'altro.
La scuola ha delle specificità proprie, per questo nella redazione del DPS particolare attenzione deve essere posta al trattamento dei dati sensibili e giudiziari, agli uffici che li svolgono, alle qualifiche dei responsabili e degli incaricati, alle strutture di riferimento, all'uso corretto del Protocollo, per cui spesso succede che lo stesso atto sia presente in più luoghi (protocollo generale, protocollo riservato, fascicolo personale..).
Si può inoltre verificare la circostanza per cui nell'Istituto scolastico viene fatto un uso improprio di dati sensibili da parte dei plessi scolastici. Ciò avviene in

[1] cfr. Titolo IV artt. 28-30 d.lgs. 196/2003 in http://www.garanteprivacy.it
[2] Riferimento al C.C.N.L. 2002-2005 art. 47 "Compiti del personale ATA"

quanto gli insegnanti possono avere costruito banche dati in forma abusiva, ancorchè in buona fede, contenenti elenchi di alunni associati a informazioni personali e sensibili. Il dimensionamento della rete scolastica, realizzato in tutte le regioni italiane tra il 1999 e il 2000 con l'introduzione dell'autonomia delle Istituzioni scolastiche e l'attribuzione della Dirigenza ai Capi d'Istituto[3], ha portato alla creazione di Istituzioni molto complesse costituite da un numero elevato di plessi scolastici. Ci sono, quindi, in molti casi sedi cosiddette staccate rispetto alla scuola del capoluogo con una piccola segreteria succursale che può trattenere una parte di archivio con dati riferiti agli alunni e al personale.
Va inoltre evidenziata la **complessità organizzativa e gestionale** degli Istituti, per cui all'interno della segreteria devono essere distinti l'Ufficio didattico da quello del personale, da quello contabile-amministrativo. Negli Istituti professionali è presente anche un ufficio tecnico per la gestione degli acquisti e dei bandi di gara.
Risulta evidente che il Direttore dei Servizi Generali e Amministrativi deve chiaramente distinguere per ogni Incaricato le differenti categorie di dati e di informazioni a cui ciascun operatore può accedere per il servizio richiesto.
Al fine di proteggere i dati in possesso dell'Istituto, il Documento Programmatico per la Sicurezza previsto dal Codice Privacy deve indicare chiaramente quali siano **i rischi incombenti sui dati** e quali le misure messe in atto per contrastarli. Il rischio può essere legato alla persona che per incuria, per errore o per dolo può fare un uso scorretto dei dati; può essere legato agli strumenti poiché a causa di virus o di intrusione piratesca si può causare l'alienazione o la distruzione dei dati; può infine essere legato ad eventi accidentali, naturali, artificiali o dolosi.
E' quindi necessario da parte del Direttore dei Servizi e del Dirigente Scolastico registrare i rischi possibili e adottare tutte le misure necessarie a limitare quei rischi. E' opportuno anche, periodicamente, effettuare prove di ripristino in seguito a simulazione di danno.
Una misura minima di sicurezza risulta la password di accesso al PC, oltre all'accesso limitato al server in base alla USER ID che permette accessi differenziati a seconda dell'ambito di competenza dell'incaricato. La sicurezza fisica può essere controllata con sistemi antifurto ed antiintrusione, armadi blindati, gruppi di continuità.
Il Documento Programmatico per la Sicurezza deve essere un **documento partecipato**, nell'istruttoria, nella redazione e negli aggiornamenti, dal titolare e dal responsabile della protezione dei dati nell'Istituto scolastico. Le linee guida fornite dal Garante[4] sono un utile strumento di partenza, ma devono intendersi come guida generale e sommaria, in quanto destinata a tutti i soggetti pubblici e privati chiamati ad adempiere agli obblighi previsti dalla legge. Solo chi conosce la complessità e la specificità della scuola, operandovi quotidianamente dall'interno, può consapevolmente calarsi nella particolare situazione organizzativa, amministrativa e didattica. Per questo la fase istruttoria e di redazione del DPS deve essere particolarmente curata attraverso una riflessione e un'indagine approfondite sul contesto in ordine al

[3] cfr. art. 21 Legge n. 59 del 15.03.1997 e D.P.R. n. 275 dell'8.03.1999
[4] cfr. "Guida operativa per redigere il DPS", 11 giugno 2004, consultabile in http://www.garanteprivacy.it

trattamento dei dati, agli uffici di riferimento, alle competenze degli incaricati, ai rischi incombenti e alle misure di sicurezza adottate.

3. Una comunità di pratica

Da quanto sopra detto risulta evidente che la diffusione della cultura della sicurezza tra gli operatori scolastici, intesa come protezione e trattamento dei dati personali, necessita di uno specifico intervento formativo. La cultura della sicurezza non deve essere ridotta ad una serie di adempimenti formali, bensì divenire consapevolezza di comportamenti corretti che concorrono alla convivenza civile e democratica. E' bene allora programmare **un solido piano di formazione**, attraverso moduli monotematici di approfondimento, possibilmente in ambiente *e.learning* integrato, modalità che permette di offrire ai professionisti in formazione uno spazio e un tempo per il confronto, lo scambio e la discussione. Il piano formativo deve prevedere anche la consulenza dell'esperto, che interviene sulle questioni giurisprudenziali e sugli aggiornamenti normativi e dottrinari inerenti la progressiva applicazione del D.Lgs. 196/2003 presso le Istituzioni scolastiche. Al fine di ottimizzare le risorse e poter fruire di una formazione e di una consulenza di qualità si suggerisce la costituzione di reti tra gli Istituti scolastici[5], con una partecipazione finanziaria a carico di ogni Istituto per la realizzazione del progetto. Nel Friuli Venezia Giulia tutti gli Istituti scolastici della Regione hanno costituito una rete per la formazione con la Direzione Scolastica Regionale, a cui è stato affidato il coordinamento del piano formativo, versando un contributo minimo, quasi simbolico, per la realizzazione del progetto. Il costo è stato quasi nullo in termini di spesa per il singolo Istituto scolastico, ma altissimo per i destinatari in termini di ricaduta formativa.
L'obiettivo del progetto formativo è, infatti, supportare e sostenere le conoscenze degli operatori scolastici in ordine al Codice Privacy per finalizzarle all' applicazione di comportamenti corretti a tutela del diritto alla riservatezza.

[5] art. 7 D.P.R. 275 dell'8.03.1999

LA TUTELA DELLA PRIVACY IN AMBITO SCOLASTICO – PROFILI OPERATIVI (D.LVO 30 GIUGNO 2003 N. 196 ARTT. 95-96)

BENEDETTO MARZOCCHI BURATTI - AVVOCATO

1. STRUTTURA DEL CODICE DELLA PRIVACY E NORME DI RIFERIMENTO

Il tema trattato consente di accennare brevemente alla struttura del Codice della Privacy, onde agevolare l'operatore nella individuazione delle norme generalmente applicabili.

Il Codice è suddiviso in tre parti, nella prima, composta di 45 articoli, sono raccolte le disposizioni generali riferibili a qualsivoglia tipo di trattamento, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle specifiche disposizioni contenute nella seconda parte del Codice (Cfr. art. 6).

In tale seconda parte (artt. da 46 a 140), vi è la disciplina riservata dal Codice della Privacy al trattamento dei dati personali in determinati settori (tra cui quello della istruzione art. 95 e 96).

Nella terza ed ultima parte (artt. 140 – 180), sono contenute le norme a tutela dei diritti degli interessati, la composizione ed i compiti del Garante per la Protezione dei Dati Personali e le sanzioni di natura amministrativa e penale.

Di fondamentale importanza, pertanto, sono le norme contenute nella prima parte del Codice, applicabili a tutti i tipi di trattamento compresi quelli in ambito scolastico.

Negli articoli da 1 a 4 sono contenuti i principi cardine del sistema di tutela della riservatezza individuale, da cui possono sintetizzarsi i seguenti principi:

- Diritto di ognuno alla protezione dei propri dati personali (art. 1);
- Garanzia del trattamento dei dati personali nel rispetto delle libertà fondamentali dell'individuo e della sua dignità;
- Principio di necessità del trattamento, preferendo quando possibile l'utilizzo di dati anonimi in grado di impedire l'identificazione dell'interessato.

In altre parole, i dati personali sono beni giuridici meritevoli di tutela per il cui trattamento ed utilizzo sono posti limiti e cautele specifiche:

- principio di liceità e correttezza del trattamento (applicazione concreta del generale principio di buona fede) ex art. 11, comma 1, lett. a);
- principio di finalizzazione del trattamento che deve perseguire scopi leciti ed espliciti ex art. 11 lett. b);
- principio di correttezza dei dati, che dovranno essere continuamente aggiornati, revisionati ed eventualmente corretti anche su richiesta dell'interessato, ex art. 11 lett. c);
- principio di pertinenza, completezza e non ridondanza dei dati in rapporto alle finalità del trattamento, ex art. 11, comma 1, lett. d);
- principio di conservazione e durata per il tempo necessario al raggiungimento delle finalità del trattamento, ex art. 11 lett. e);

La violazione anche di uno solo di tali principi nel trattamento dei dati personali, determina la inutilizzabilità degli stessi[6].

[6] Cfr. comma 2 art. 11 Codice della Privacy: "I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati".

Il Codice della Privacy, in ogni modo, non si limita solamente a porre le linee guida per il trattamento dei dati personali ma individua (per la consultazione diretta si veda l'Allegato B. al codice della privacy) le cosiddette misure minime da adottare per garantire la sicurezza e l'integrità dei dati trattati.
Inoltre, nell'art. 13 vengono stabiliti i contenuti obbligatori della informativa che il titolare ed il responsabile del trattamento devono fornire all'interessato affinché sia posto in grado di esprimere consapevolmente il consenso al trattamento dei propri dati ed esercitare compiutamente i propri diritti[7].

1.1 LA TUTELA DELLA PRIVACY ED IL SETTORE DELL'ISTRUZIONE

Come accennato, tale normativa di carattere generale, deve essere interpretata alla luce delle specifiche disposizioni che il Codice della Privacy riserva al settore dell'istruzione scolastica (Parte II Titolo VI Istruzione Capo I Profili Generali artt. 95 e 96).
In tali norme, il legislatore ha precisato che sono di rilevante interesse pubblico, ai sensi degli artt. 20 e 21 dello stesso Codice, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario.
E' stata anche salvaguardata - art. 96 - la permanenza in vigore delle disposizioni concernenti la pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.
Pertanto sulla base del dato normativo, possono essere così riassunti gli adempimenti del titolare e del responsabile del trattamento di dati personali, comuni e sensibili, in ambito scolastico:

a) è necessaria l'informativa ai sensi dell'art. 13 che, nel caso di trattamento di dati sensibili, dovrà anche contenere l'indicazione della legge che ne prevede e consente il trattamento. Essa, come precisato dal Garante, potrà essere anche rilasciata per il tramite di apposite modalità di diffusione come ad esempio **l'affissione nei locali istituzionali**;
b) non è necessario ottenere il consenso per il trattamento di dati comuni, fatta salva la disposizione dell'art. 96 comma 1[8], ma il trattamento è consentito solo per le specifiche finalità istituzionali;
c) generalmente, non è necessario ottenere dai soggetti interessati il consenso alla comunicazione dei dati comuni. Tuttavia, se la comunicazione di dati comuni da soggetto pubblico a soggetto pubblico non è prevista da una specifica disposizione di legge o regolamento, occorre inviare una comunicazione al Garante che, ai sensi dell'art. 154 lett. G), definirà modalità e finalità della

[7] I contenuti dell'informativa sono i seguenti: a) finalità e modalità di trattamento; b) obbligo o facoltà in capo al soggetto interessato di conferire i dati; c) conseguenze del rifiuto di rispondere; d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi; e) diritti dell'interessato e modalità di esercizio; f) estremi del titolare e del responsabile (Cfr. art. 13 D.lgs 196/03).

[8] Art. 96 comma 1 D. lgs. 196/03: "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 dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità".

comunicazione. La comunicazione da soggetto pubblico a soggetto privato è invece consentita solo se prevista da legge o regolamento;

d) il trattamento dei dati sensibili è consentito solo in presenza di specifiche disposizioni di legge e di un regolamento che individui dati trattabili ed operazioni eseguibili;
e) è necessario richiedere il consenso per il trattamento dei dati sanitari.

I punti d) ed e) impongono ulteriori riflessioni su come il funzionario debba atteggiarsi nel trattamento dei dati sensibili relativi al corpo docente od agli alunni, non essendo infrequente la loro presenza in ambito scolastico.
Basti pensare, in primo luogo, alla eterogeneità sempre più marcata di provenienza culturale, etnica o religiosa degli alunni la cui non corretta gestione potrebbe comportare pesanti conseguenze, anche di rilievo penale, nei confronti del titolare del trattamento.
Per tali tipi di dati, c.d. sensibili, il Codice della Privacy ha giustamente previsto una disciplina più rigorosa prevedendo restrizioni più diffuse per il loro trattamento (Cfr. punti d) ed e) del presente paragrafo) nonché una loro specifica indicazione: "***d) "dati sensibili", 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, nonchè i dati personali idonei a rivelare lo stato di salute e la vita sessuale***" (art. 4 comma 1 lett. d) D.lgs 196/03).
L'operatore, pertanto, potrà trattare tali tipi di dati solo in presenza di specifiche disposizioni normative, acquisendo il consenso consapevole dell'interessato.
Tuttavia, nel concreto, tali dati dovranno essere resi per quanto possibile in forma anonima con la individuazione di criteri alternativi che non consentano l'identificazione dell'interessato[9].
In altre parole, allorché il funzionario responsabile debba indicare e pertanto trattare per ragioni del suo ufficio un dato idoneo a rivelare le condizioni di salute, le convinzioni religiose, la provenienza etnica etc. del soggetto interessato come:

- la partecipazione dell'alunno a corsi per la disassuefazione al fumo;
- ragioni di dispensa dell'alunno dalla partecipazione alle lezioni di educazione fisica per ragioni di salute;
- la partecipazione a corsi di natura religiosa etc.

la diffusione dovrà essere limitata ai dati essenziali per lo scopo del trattamento evitando il più possibile la identificazione del soggetto interessato, preferendo allo scopo l'utilizzo di alternativi **codici alfanumerici**.

[9] Sul punto, l'Autorità Garante ha avuto già modo di pronunciarsi affermando che: "*Costituisce diffusione indiscriminata di dati idonei a rilevare lo stato di salute, e risulta quindi in contrasto con la disciplina posta dalla legge n. 675/1996 e dal d.lg. n. 135/1999 in materia di trattamento dei dati sensibili da parte di soggetti pubblici, l'inserimento della dicitura "portatore di handicap", riferita ad un'insegnante, nella graduatoria dei trasferimenti affissa nella bacheca di un provveditorato agli studi. Le esigenze di pubblicità dell'amministrazione possono essere soddisfatte attraverso l'apposizione di diciture generiche o codice numerici*". Il provvedimento integrale del Garante della Privacy è consultabile al link: www.garanteprivacy.it/garante/document?ID=996804 pag. 51 e ss.

Perché il trattamento, di dati comuni o sensibili, avvenga correttamente, il titolare ed il responsabile per il trattamento in ambito scolastico sono tenuti, anche nel nuovo impianto normativo, a porre in essere tutti quegli accorgimenti necessari per la protezione dei dati personali, adottando le prescritte misure di sicurezza.
Permane un obbligo, di carattere generale, di ridurre al minimo determinati rischi (manomissione, distruzione, perdita di dati o di trattamenti non consentiti), a cui si affianca l'obbligo specifico di adottare le misure minime di sicurezza così come previste dall'Allegato B. al Codice della Privacy.
Particolarmente vigile, pertanto, dovrà essere l'osservanza di tale obbligo in ambito scolastico, considerata la frequente presenza di minori, al fine di evitare nella misura più ampia possibile il rischio che i dati siano dispersi, distrutti, conoscibili al di fuori dei casi consentiti od utilizzati in modo illecito.
La reazione dell'attuale sistema normativo alla violazione di tale obbligo di sicurezza comporta non solo la illiceità del trattamento anche in assenza di un danno per l'interessato ma, costituendo violazione dei diritti degli interessati (compreso quello fondamentale alla protezione dei dati personali), espone l'autore dell'illecito al risarcimento del danno, anche non patrimoniale, nella scomoda posizione, per il presunto trasgressore, di dover provare di aver assolto a tutte le precauzioni necessarie ex art. 2050 c.c. (c.d inversione dell'onere della prova).
Difficilmente, pertanto, potrà essere fornita la prova liberatoria senza aver preventivamente adottato le misure minime di sicurezza, misure che dovranno anche essere idonee in relazione alle specifiche modalità di trattamento dei dati.
Il funzionario responsabile del trattamento, pertanto, adoperando la dovuta diligenza, dovrà adottare tutte quelle misure che appaiono ragionevolmente idonee a ridurre il rischio in base alla cognizioni tecniche al momento disponibili, da aggiornarsi in base al successivo progresso od alla accertata carenza delle stesse. Oltre alla responsabilità di natura civile ed amministrativa, l'autore dell'illecito (solitamente il titolare del trattamento ed i responsabili dello stesso), possono incorrere in responsabilità di natura penale. Difatti, per l'inosservanza delle misure minime di sicurezza, l'art. 169 del Codice prevede una responsabilità penale per l'ipotesi di mancata adozione delle misure minime previste ex art. 33, con reato avente struttura omissiva propria, di pericolo presunto che si perfeziona quindi anche in assenza di danno.

1. L'esercizio del Diritto di Accesso in Ambito Scolastico e la Tutela della Riservatezza

Chiariti i principi e gli obblighi a cui il Direttore dei Servizi Generali ed Amministrativi deve uniformarsi, è necessario esporre come nel concreto possa mostrarsi il trattamento dei dati personali in ambito scolastico e l'accesso agli stessi.
Va subito detto che, in tema di diritto di accesso, lunga e complessa è stata ed è tuttora la disamina della dottrina e della giurisprudenza che hanno cercato di armonizzare la disciplina del Codice della Privacy a quella della L. 241/90 in materia di accesso agli atti amministrativi.

Basti qui considerare che il legislatore, in tema di privacy, è intervenuto prima con l'approvazione del D.lgs n. 135/99 e poi con l'approvazione del D.lgs. n. 196/03, offrendo agli operatori i mezzi per poter risolvere la composizione degli interessi in gioco – diritto di accesso ex L. 241/90 e diritto alla riservatezza ex L. 675/96 e la concreta antinomia tra i due istituti.
In proposito, è stato introdotto un fondamentale principio che, in presenza di dati sensibili idonei a rilevare l'origine razziale, etnica, il credo religioso o filosofico (alunni oramai provenienti da variegate realtà etniche e religiose), lo stato di salute (alunni dispensati per tali motivi dal frequentare i corsi di educazione fisica etc.) o la vita sessuale, consente il loro trattamento, la loro comunicazione o diffusione solo qualora il diritto da far valere o difendere, mediante richiesta d'ostensione, sia di "*rango pari a quello dell'interessato*" alla tutela della propria privacy.
E', pertanto, compito ed onere dei Dirigenti Scolastici responsabili del trattamento dei dati, procedere al concreto bilanciamento degli interessi, con la possibilità di rivolgersi per un parere preventivo direttamente al Garante ex art.154 lett. G) del Codice della Privacy.

1.1. L'INTERPRETAZIONE DEL DIRITTO DI ACCESSO IN AMBITO SCOLASTICO SCATURENTE DALL'ATTIVITÀ DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In questo difficile compito di valutazione e ponderazione delle diverse esigenze, il destinatario finale di tali richieste di accesso ha a sua disposizione,come detto, un autorevole e sicuro contributo, sollecitabile anche direttamente, costituito dal lavoro dell'Autorità Garante per la Protezione dei Dati Personali.
Dall'analisi dell'attività del Garante si evince la particolare attenzione dello stesso in ambito scolastico, rappresentata da continui interventi volti a chiarire l'operatività delle norme in tale settore ed alla risoluzione di casi pratici, sia per mezzo di segnalazioni e ricorsi diretti, sia intervenendo in merito a notizie apparse sugli organi di informazione.
La sintesi di tale attività è riversata nelle relazioni che, con cadenza annuale, il Garante propone al Parlamento sulla propria attività istituzionale.
Dalla lettura di tali relazioni, nonché dal raffronto delle decisioni di tale Authority, emergono con chiarezza gli aspetti che con maggiore frequenza si pongono per gli operatori del settore nella tutela della riservatezza dei dati personali in ambito scolastico.
Va detto che in materia di diritto di accesso, la linea del Garante si pone nel solco tracciato dalla giurisprudenza[10], affermando che la normativa sulla protezione dei dati personali non può essere invocata quale limite o negazione del diritto di accesso poiché spetta sempre alla pubblica amministrazione valutare in concreto la sussistenza delle condizioni per accedere ai documenti amministrativi[11].

[10] Cfr. Cons. Stato, Sez. VI, 30/03/2001, n. 1882 in Giur. It., II, 405 con nota di Cassano.
[11] In proposito si veda la relazione annuale al Parlamento del Garante per l'anno 2001 ove si registra una propensione da parte delle pubbliche amministrazioni a confondere le distinte condizioni di applicazione delle due normative (L. 241/90 e L. 675/96 ora D.lgs. 196/03). La relazione è consultabile in

Tale indirizzo interpretativo ha consentito al Garante una difficile ma efficace sintesi tra la necessità di tutelare la riservatezza dei dati personali in ambito scolastico con l'altrettanto significativo bisogno di implementare le attività di divulgazione e promozione scolastica e scientifica.
Particolarmente significativo, in questo senso, è stato l'intervento del Garante su un quesito posto da un istituto scolastico in merito alla liceità della comunicazione alle famiglie dei nominativi degli alunni iscritti ad un corso di disassuefazione al fumo.
Tale quesito, pur nella sua apparente banalità, evidenzia la difficoltà di gestione del diritto di riservatezza in ambito scolastico ove, come appunto nel caso citato, possano sorgere potenziali conflitti di interesse tra il titolare del diritto (lo studente minore) e chi (generalmente i genitori esercenti la potestà) materialmente, in sua vece, ne controlla il rispetto e reagisce alle violazioni od ai trattamenti illeciti.
La soluzione interpretativa offerta dal Garante, pur non dissipando alla radice i dubbi prospettati, si pone su di una via intermedia contemperando le diverse esigenze.
Si è precisato, infatti, che tali tipi di informazioni – come la partecipazione ad un corso di disassuefazione al fumo – possano comportare, in determinate situazioni, la comunicazione dello stato di salute dei soggetti interessati; in tale ottica, il Garante ha pertanto consigliato all'istituto scolastico di **indicare genericamente le finalità** del corso con formule del tipo "all'educazione alla salute e alla prevenzione"[12].
Correlato all'esercizio per la tutela dei dati personali vi è un altro nodo da sciogliere, ovvero chi sia legittimato in ambito scolastico ad esercitare il diritto di accesso, tematica anch'essa affrontata dal Garante che, con provvedimento dell'11 settembre 2001 (pubblicato sul Bollettino del Garante luglio – settembre 2001[13]), ha accolto il ricorso di un genitore che, a nome del proprio figlio, chiedeva l'accesso ai dati personali detenuti da un istituto scolastico.
Più delicata, invece, appare l'ipotesi in cui il coniuge separato (o divorziato) non affidatario del minore (o comunque portatore di interessi in conflitto con l'altro genitore), richieda l'accesso ai dati personali del figlio, detenuti dall'istituto scolastico che frequenta, al fine di utilizzarli in ambito giudiziario per precostituirsi prove nei confronti dell'altro genitore o per ottenere migliori condizioni di affidamento.
Pur essendo comunque preferibile richiedere sul punto un parere preventivo al Garante ai sensi dell'art. 154 lett. G) del codice della Privacy, per risolvere tale questione dovranno essere comparati i diritti del coniuge o genitore richiedente, rappresentati dall'interesse ad agire per ottenere un provvedimento a lui favorevole e che collimano parzialmente con quelli del figlio minore a cui deve essere sempre garantito un adeguato sviluppo educativo (il cui onere di vigilanza spetta ad entrambi i coniugi), con quelli di

---

http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento%2F2001 .

[12] La decisione, non pubblicata, è commentata nella relazione annuale al Parlamento per l'anno 2002: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp?folderpath=Attivit%E0+dell%27Autorit%E0%2FRelazioni+annuali+al+Parlamento%2F2002

[13] Consultabile al link: www.garanteprivacy.it/garante/document?ID=996823

riservatezza del minore sanciti dall'art. 2 comma 2 del D.P.R. n. 249/88[14] nonché infine con quelli del coniuge o genitore non richiedente.
Indubbiamente, il coniuge che voglia accedere ai dati personali di natura scolastica del figlio, onde verificare l'adempimento di tutti gli oneri derivanti ad esempio dall'art. 155 cod. civ. al coniuge affidatario, esercita un diritto a lui direttamente derivante dall'ultimo comma dello stesso art. 155 c.c.[15].
Tale azione è anche posta a tutela dello stesso sviluppo della prole che, ai sensi dell'art. 147 c.c., deve essere garantita dai coniugi tenendo conto delle capacità, dell'inclinazione naturale e delle aspirazioni dei figli; pertanto, ove vi fosse uno scarso od un pessimo rendimento scolastico, la conoscenza di tale dato personale per il coniuge non affidatario potrebbe consentire di attivare quelle procedure di modifica del regime di affidamento poste in primo luogo a tutela della prole.
In altre parole, nel caso ora prospettato, il coniuge non affidatario, nel richiedere l'accesso ai dati personali del figlio in ambito scolastico, verrebbe ad esercitare un diritto superiore, o quantomeno pari, a quello di tutela della riservatezza degli stessi dati, formulando una richiesta più che legittima.

3. LA RISOLUZIONE DI CASI PRATICI NELLA ATTIVITÀ DEL GARANTE DELLA PRIVACY

Esaminando ancor più nel concreto le difficoltà che quotidianamente devono essere affrontate per la gestione del sistema "privacy" in ambito scolastico, è utile passare in rassegna le decisioni prese dal Garante, alcune delle quali anche sollecitate da richieste banali che ben testimoniano l'attuale imbarazzo e forse l'eccessiva cautela degli operatori.
Questo perché, obiettivamente, l'approvazione della L. 675/96 ed i successivi interventi legislativi in materia sino al D.lgs. 196/03, hanno comportato una vera e propria rivoluzione culturale e giuridica che necessita di continui chiarimenti per la sua concreta applicazione.
Significativo, in questo senso, è stato il parere emesso dal Garante su segnalazione della Unione Nazionale Consumatori, con provvedimento del 4 marzo 1999 (pubblicato sul Bollettino ufficiale di Attività del Garante[16]), ove si è chiarita la assoluta liceità della assegnazione di temi da parte degli insegnanti che comportano la rivelazione di dati e fatti personali e familiari a volte anche sensibili, pur rimanendo fermo per il corpo docente l'obbligo del segreto di ufficio e professionale e l'adozione di cautele nella lettura in classe degli elaborati su tali argomenti.
Altro caso portato all'attenzione del Garante dai genitori di un minore che hanno proposto ricorso, con successo, nei confronti di un istituto scolastico che aveva diffuso una circolare a tutte le famiglie degli alunni relativa ai provvedimenti disciplinari adottati in occasione di litigi tra studenti.

[14] La cui vigenza è stata confermata dal comma 2° dell'art. 96 del Codice della Privacy.
[15] Ultimo Comma art. 155 c.c. "I coniugi hanno diritto di chiedere in ogni tempo la revisione delle disposizioni concernenti l'affidamento dei figli, l'attribuzione dell'esercizio della potestà su di essi e le disposizione relative alla misura e alle modalità del contributo".
[16] Il testo del provvedimento è consultabile all'indirizzo: www.garanteprivacy.it/garante/document?ID=996886.

In tale occasione, il Garante ha precisato che la diffusione di notizie sugli eventi della vita scolastica, pur rientrando nelle prerogative di ogni istituto, deve essere bilanciato con l'**esigenza di tutelare la personalità dei minori**[17].
Diffusa è stata anche l'opinione, avanzata dallo stesso Ministero dell' Istruzione, che la diffusione delle valutazioni finali analitiche a carico dei "bocciati" o dei non ammessi agli esami potesse costituire una violazione delle norme sulla tutela dei dati personali. Anche in questo caso, il Garante, nella persona del Prof. Ugo De Siervo, è intervenuto per chiarire che la pubblicità degli esiti scolastici è regola generale[18].
Ancora, in un comunicato del 17 dicembre 2003[19], il Garante è dovuto intervenire per ribadire la assoluta liceità delle riprese video e fotografiche effettuate da genitori in occasione di recite scolastiche in quanto si tratta di immagini non destinate a diffusione, ma raccolte per fini personali e destinate ad un ambito familiare o amicale.
Da questa breve analisi delle decisioni del Garante emerge chiaramente come, tuttora, l'applicazione della normativa sulla tutela dei dati personali in ambito scolastico sia ancora in fase di "rodaggio" e che sia ancora diffuso il timore che tale normativa costituisca una sorta di ingessatura che limita i movimenti in tale settore.
In realtà, anche e soprattutto per il tramite dell'assiduo intervento chiarificatore del Garante, si ritiene che questa convinzione possa essere superata e che la tutela dei dati personali possa tramutarsi da costo in risorsa per la tutela dei cittadini nell'utilizzo delle nuove e sempre più invasive tecnologie.
In proposito, con provvedimento del 29 aprile 2004[20], volto a regolamentare il fenomeno della video-sorveglianza, è stata dettata anche la disciplina con riferimento agli istituti scolastici ove tali impianti potranno essere installati (salvaguardando la riservatezza degli studenti) in casi di assoluta indispensabilità come ad esempio per il protrarsi di atti vandalici.
Ancora una volta dunque, si dimostra la sensibilità del Garante a prevenire, per quanto possibile, ogni profilo concreto di applicazione della normativa sulla privacy, fatto che porterà in breve tempo a regime l'intero impianto legislativo.

L'APPROVAZIONE DEL DOCUMENTO PROGRAMMATICO DELLA SICUREZZA: UN ATTO A COMPETENZA MULTIPLA ?

A cura di Andrea Baldanza – Magistrato Corte dei Conti

[17] Il comunicato stampa è consultabile al link: www.garanteprivacy.it/garante/doc.jsp?ID=46989.
[18] Il chiarimento è riportato nella newsletter 12-18 giugno 2000 consultabile al link: http://www.garanteprivacy.it/garante/doc.jsp?ID=46725.

[19] Testo consultabile all'indirizzo www.garanteprivacy.it/garante/doc.jsp?ID=476650.
[20] Il testo integrale è consultabile all'indirizzo http://www.garanteprivacy.it/garante/doc.jsp?ID=1003482#4_3.

Il punto 19 dell'allegato "B" connesso agli articoli da 33 a 36 del d.lgs. 30 Giugno 2003 n. 196, recante il "Codice in materia di protezione dei dati personali", prevede che "entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari rediga, anche attraverso il responsabile, se designato, un Documento Programmatico sulla Sicurezza [in seguito DPS] delle misure minime di sicurezza". Il termine per l'approvazione di siffatto documento è stato spostato, dall'art.3 della legge 27 luglio 2004, n.188, di conversione del decreto-legge 24 giugno 2004, n.158, al 31 dicembre 2004. Costituisce quindi questione di stretta attualità l'individuazione dell'autorità legittimata ad adottare il DPS, anche in considerazione delle sanzioni penali previste in caso di omissione (sul punto si rinvia all'elaborato di L.Palamara).

L'art.33 del d.lgs. n.196/2003 precisa che "i titolari del trattamento sono comunque tenuti ad adottare le misure minime". La qualifica di "**titolare**", ai sensi dell'art.4, comma 1, lett. f) del d.lgs. n.196/2003, si intesta alla "pubblica amministrazione … cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza". L'attribuzione della qualità di "titolare" costituisce conseguenza dell'esistenza di un potere decisionale rispetto alle "modalità, finalità, [alla disponibilità] degli strumenti ed al [potere di assicurare] la sicurezza nel trattamento dei dati". Siffatta definizione ammette che nella medesima struttura/persona giuridica coesistano più trattamenti di dati, ciascuno sottoposto ad una propria disciplina organizzativa e con un diverso "titolare", tant'è che lo stesso art.4, comma 1, lett.f) del d.lgs. n.196/2003, prevede che la suddetta qualifica possa spettare "anche unitamente ad altro titolare". Oltre ad una pluralità di titolari interni all'amministrazione, deve anche ritenersi fisiologica l'attribuzione della titolarità del trattamento a soggetti esterni all'apparato pubblico. Costituisce infatti fattispecie molto diffusa l'attribuzione a soggetti estranei all'amministrazione dei compiti di manutenzione degli strumenti informatici. In tali ipotesi il contraente dell'amministrazione, in quanto occasionalmente in possesso dei dati raccolti dall'amministrazione (si pensi alle riparazioni effettuate nei locali della società), deve assumere la qualifica di "titolare" del trattamento. Si osservi che, nel primo caso, si hanno più "titolari" all'interno dell'amministrazione, in ragione dell'autonomo potere decisionale rispetto alle strutture di riferimento; nel secondo, si hanno più "titolari" rispetto ai medesimi dati, in ragione della loro occasionale diversa allocazione logistica.

L'individuazione di più soggetti come titolari del trattamento dei dati costituisce anche il naturale portato di un'organizzazione diffusa qual è il sistema di istruzione nazionale. Si osservi che nell'ambito dell'amministrazione scolastica, alla struttura ministeriale (ed alle articolazioni regionali), si affiancano le istituzioni scolastiche dotate, ai sensi dell'art.21 della legge 15 marzo 1997, n. 59 di personalità giuridica, nonché, ai sensi dell'art.1 del d.P.R. 8 marzo 1999, n. 275, "**di autonomia funzionale**". Poiché le suddette strutture/articolazioni effettuano autonomi trattamenti di dati, appare inevitabile l'individuazione di più "titolari".

Particolarmente delicata appare l'individuazione del "titolare" nell'ambito della struttura ministeriale, coabitando organi di indirizzo politico (il Ministro) ed organi burocratici (l'apparato dirigenziale). Se si esaminano le opzioni espresse dalle amministrazioni che hanno già reso pubblico l'atto di adozione del DPS, appaiono evidenti due orientamenti contrastanti. La maggior parte delle amministrazioni ha adottato il DPS mediante delibera dell'organo esecutivo[21]; esistono tuttavia casi (non così sparuti), di approvazioni del medesimo documento effettuate mediante determina dirigenziale[22].

La c.d. "separazione fra la politica e l'amministrazione" introdotta nel nostro ordinamento dalla legge 8 giugno 1990, n.142, di riforma degli enti locali ed estesa a tutti gli apparati pubblici dal d.lgs. 3 febbraio 1993, n.29 preclude la permanenza di una competenza binaria. Mentre nel regime anteriore all'approvazione delle suddette disposizioni, il vertice politico, in quanto organo gerarchicamente sovraordinato, disponeva di tutte le competenze degli organi subordinati, talchè poteva ammettersi l'esercizio di un potere sostitutivo da parte del Ministro rispetto agli apparati subordinati (si pensi ai casi di avocazione, riforma in sede di decisione dei ricorsi gerarchici, annullamento d'ufficio ecc.), nel nuovo assetto, suddetta concorrenza non appare più compatibile. Un atto, o rientra fra le competenze dell'organo di indirizzo politico, ovvero deve ricondursi nell'ambito degli atti di gestione, di pertinenza degli organi burocratici. Non è concepibile che un atto possa essere, indifferentemente, di competenza di un organo politico o di un organo burocratico.

Al fine di meglio comprendere entro quale area deve ascriversi l'atto di approvazione del DPS, appare utile richiamare il rapporto presupposto fra il "titolare" e gli "incaricati", ossia "le persone fisiche autorizzate a compiere operazioni di trattamento". L'art.30 del d.lgs. n.196/2003, dispone che "le operazioni di trattamento possano essere effettuate solo da incaricati che operino sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite". Siffatto dettato normativo induce a ravvisare che fra il "titolare" e l'"**incaricato**" debba sussistere un rapporto di subordinazione e che si abbia una continua elaborazione di istruzioni. Tali condizioni non sembrano concretamente ravvisabili in nessun rapporto fra organi di indirizzo politico ed organi burocratici. Il principio della separazione delle due aree, infatti, preclude a qualsiasi organo politico di poter agire con "diretta autorità" rispetto al personale burocratico: ad un regime gerarchico, si è sostituito un sistema fondato sul potere direttivo dell'organo politico. Ancor più difficile, appare l'elaborazione di istruzioni da parte di un qualsiasi organo politico: questo è deputato a curare gli atti quadro o di organizzazione, non certamente minute disposizioni. Se poi si scende nel dettaglio dei contenuti del DPS appare evidente come nessun Ministro possa impegnarsi per dettare istruzioni in merito all'effettiva corrispondenza, da parte dei dipendenti dell'apparato cui

[21] A titolo di mero esempio si citano la Provincia di Udine ed il Comune di Crespellano (Bo): entrambe queste amministrazioni hanno approvato il DPS con delibera della giunta. Per la Provincia di Udine si rinvia alla delibera del 23 giugno 2004, mentre per il Comune di Crespellano alla delibera del 2 settembre 2004. Entrambi i documenti sono consultabili sui rispettivi siti istituzionali.

[22] Anche in questo caso, a titolo di mero esempio, si cita la determina del Segretario generale del Comune di Prato, che ha approvato il DPS con atto del 30 giugno 2004 n.2080, consultabile sul sito istituzionale del Comune di Prato.

il medesimo è preposto, dell'uso degli strumenti elettronici secondo modalità conformi alle prescrizioni ordinamentali.

Sulla scorta di siffatti argomenti, l'intestazione della competenza ad approvare il DPS in capo all'esecutivo (ossia, presso gli enti locali, in capo alle giunte comunali o provinciali) appare disarmonica rispetto al riparto delle competenze contenuto nella legge n.142/1990 e ribadito dal d.lgs. n.29/93. Non appare concepibile che una scelta attinente all'area della gestione amministrativa, quale deve ritenersi, a titolo di esempio, l'individuazione dei soggetti autorizzati al trattamento dei dati personali possa essere ricondotta nel novero degli atti … di indirizzo politico. Analoghe considerazioni possono estendersi rispetto all'adozione delle "necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato" (punto 4 dell'allegato "B").

Se poi si considera che l'esigenza di vigilare sul rispetto delle prescrizioni impartite presuppone un'adeguata flessibilità di azione, l'approvazione del DPS da parte di un organo collegiale (quale, ad esempio una giunta) risulta particolarmente infelice. Un qualsiasi organo collegiale appare inadatto a compiere attività di monitoraggio continuo rispetto all'adesione delle proprie determinazioni. La nomina di un responsabile quale soggetto delegato dall'organo politico (monocratico o collegiale) alle attività di vigilanza, non potrebbe sanare il vizio che affetta l'atto di approvazione del DPS, in considerazione della circostanza che la delega, non potrebbe integrare un trasferimento di funzioni. Il d.lgs. n.196/2003 impone all'autorità che adotti il DPS di vigilare sulla continuità delle informazioni ivi contenute, attesa la necessaria quanto indefettibile corrispondenza che deve sussistere fra le informazioni contenute nel documento e la concreta prassi operativa. L'attribuzione di un potere di vigilanza ad un responsabile, oltre che cozzare con la facoltatività di tale nomina, non potrebbe comunque far evaporare le competenze dell'autorità delegante. Di conseguenza, l'organo politico, successivamente all'adozione del DPS, anche in presenza di una delega dell'attività di vigilanza ad un responsabile, non potrebbe mai disinteressarsi della rappresentazione dell'azione dell'amministrazione cristallizzata nell'atto.

Se le informazioni contenute nel DPS appartengono all'attività di esecuzione dell'amministrazione, anche la responsabilità riguardo all'approvazione, all'effettivo rispetto delle indicazioni enunciate e all'aggiornamento del documento non possono che competere agli organi burocratici. L'intera area del trattamento dei dati personali e sensibili, pur integrando uno dei fini necessari dell'azione pubblica, non sembra coinvolgere decisioni di carattere politico. Le amministrazioni pubbliche devono perseguire i fini istituzionali, nel rispetto della legalità (nel cui ambito vive anche la disciplina del trattamento dei dati personali), avvalendosi delle risorse strumentali ed umane di cui sono in possesso. Le modalità di utilizzazione delle risorse strumentali ed umane integra una decisione tecnica di competenza degli organi burocratici.

Le conseguenze connesse all'approvazione del DPS da parte di un organo incompetente, devono essere apprezzate su più piani.

Sotto il profilo penale, appare evidente l'inapplicabilità di qualsiasi sanzione. Il principio di tassatività, impone che possa essere sanzionata solo la condotta corrispondente a quella descritta nella fattispecie. L'art.169 del d.lgs. n.196/2003 intende punire colui che "ometta di adottare le misure minime" previste nella stessa fonte. Equiparare la mancata adozione del DPS, all'approvazione di un DPS da parte di un organo incompetente, integrerebbe una forma di "disapplicazione in *malam partem*", contraria ai principi di civiltà giuridica. Il DPS, infatti, seppur promanato da un organo incompetente, risulta essere stato comunque approvato; l'equiparazione atto illegittimo = omessa adozione dell'atto, finirebbe allora per ampliare (indebitamente) l'ambito di applicazione della prescrizione sanzionatoria. Verrebbe infatti sanzionata una condotta non descritta dal legislatore.

Sul piano amministrativo, è di tutta evidenza che l'adozione di un atto da parte di un organo incompetente possa comportare la caducazione in sede giudiziaria. Per adire l'autorità giurisdizionale amministrativa, occorre lamentare una violazione di un interesse: l'atto deve cioè ledere una situazione giuridica differenziata. Sotto questo profilo, il DPS non appare idoneo ad innovare le altrui sfere giuridiche, atteso che il medesimo si limita a registrare la situazione di fatto. Colui che deducesse una violazione della propria sfera giuridica non potrebbe accollare la medesima all'approvazione del DPS, ma, semmai, agli atti (di carattere organizzativo o ordinatorio) sottostanti. Il DPS può essere l'occasione da cui si trae conoscenza di talune determinazioni dell'amministrazione, non la fonte costitutiva.

Riguardo alle conseguenze civilistiche, non si possono che ripetere le considerazioni sopra avanzate: il DPS non integra un atto idoneo a ledere situazioni giuridiche soggettive aventi la consistenza di un diritto soggettivo, in ragione della sua natura meramente dichiarativa.

La difficoltà di accesso al sindacato giurisdizionale, al fine di far valere l'incompetenza nell'adozione del DPS, non consentono tuttavia di relegare il problema dell'esatta enucleazione dell'organo competente, nell'ambito dell'irrilevante giuridico.

Una volta affermata la competenza degli organi di indirizzo politico ad adottare il DPS, appare improbo sollevare gli stessi dai relativi oneri di vigilanza. Da qui un vero e proprio *impasse* istituzionale: una volta che un organo politico abbia approvato il documento, il medesimo non può disinteressarsi dell'effettiva corrispondenza fra quanto dichiarato e la prassi amministrativa. Appare tuttavia difficile ipotizzare un percorso mediante il quale intestare direttamente agli organi politici la competenza ad impartire gli ordini di servizio necessari per un corretto trattamento dei dati ovvero per procedere ai necessari aggiustamenti in conseguenza di sopravvenienze e modifiche delle situazioni di fatto. Da qui l'esigenza di una generalizzata presa di coscienza che il trattamento dei dati personali e sensibili integri materia strumentale ai fini perseguiti dalle amministrazioni pubbliche. In quanto tale, la medesima deve vivere all'interno dell'ordinaria attività gestionale, senza alcuna interferenza di carattere politico.

"IL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA: RIFLESSI PENALI". ANALISI DELLA FATTISPECIE PENALE RISPETTO ALLA REDAZIONE INCOMPLETA, FALSA O OMESSA DEL DPS.

A cura di Luca PALAMARA – Pubblico Ministero

1**. PREMESSA**

Dal l gennaio 2004 è in vigore il Decreto Legislativo 30 giugno 2003, n. 196, meglio noto come "Codice in materia di protezione dei dati personali", che sostituisce, innovandola, la precedente normativa contenuta nella legge 31 dicembre 1996 n. 675.

La normativa impone ad enti ed imprese una serie di nuovi obblighi a cui sono tenuti tutti coloro che trattano dati di persone fisiche nonché di persone giuridiche, enti e associazioni, tra cui la redazione del Documento Programmatico sulla Sicurezza (in seguito DPS**).**

Il termine per l'approvazione del DPS**, originariamente fissato al 31 marzo 2004, è stato spostato, in virtù dell'articolo 3 della legge 27 luglio 2004, n.154, di conversione del decreto-legge 24 giugno 2004, n.158, al 31 dicembre 2004.**

2. LA QUALIFICA SOGGETTIVA QUALE PRESUPPOSTO DELLA PENALE RESPONSABILITA'

Dovendosi analizzare le **conseguenze penali derivanti dalla incompleta, falsa o omessa redazione del DPS**, occorre preliminarmente individuare a quale figura soggettiva, all'interno della istituzione scolastica, competa l'adozione del documento in questione.

Tale accertamento costituisce, infatti, momento prodromico per l'affermazione della penale responsabilità in caso di redazione falsa, incompleta o omessa del DPS**, poiché l'articolo 27 della nostra Carta Costituzionale consacra, nel diritto penale, il principio della responsabilità personale.**

Sul punto si osserva che il dirigente scolastico**, all'interno della istituzione scolastica, deve essere individuato come titolare del trattamento dei dati, in quanto autorità dotata di potere decisionale in ordine alle finalità, alle modalità del trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.**

A sostegno di tale argomentazione si richiama l'articolo 25 bis, del Decreto legislativo 3 febbraio 1993, n. 29 che attribuisce al dirigente scolastico **i seguenti compiti:**

- **gestione unitaria dell'istituzione scolastica dotata ai sensi dell'art. 21 della legge 15 marzo 1997 di personalità giuridica, nonché ai sensi dell'art.1 del Decreto del Presidente della Repubblica 8 marzo 1999, 275 di autonomia funzionale ;**
- **legale rappresentanza;**
- **responsabilità della gestione delle risorse finanziarie e strumentali;**
- **responsabilità dei risultati del servizio.**

Ciò premesso va, tuttavia, evidenziato che - in virtù dell'articolo 29 del "Codice in materia di protezione di dati personali" che distingue tra titolare e responsabile dei dati - il dirigente scolastico **ha la possibilità di delegare la responsabilità dei dati, tra cui la materiale adozione del** DPS**, anche al direttore dei servizi generali amministrativi delle istituzioni scolastiche (**DSGA**).**

Che anche il **DSGA** possa essere designato quale responsabile del trattamento dei dati lo si desume dall'articolo 25 bis, quinto comma, del Decreto legislativo 3 febbraio 1993, n. 29, il quale, stabilisce che il **dirigente scolastico** nello svolgimento delle proprie funzioni organizzative e amministrative è coadiuvato dal responsabile amministrativo, che sovrintende, con autonomia operativa, nell'ambito delle direttive di massima impartite e degli obiettivi assegnati, ai servizi amministrativi ed ai servizi generali dell'istituzione scolastica, coordinando il relativo personale.

L'articolo 29 del "Codice in materia di protezione di dati personali" pone, tuttavia, delle precise regole nella scelta del responsabile stabilendo che quest'ultimo deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Inoltre l'articolo 29 in questione disciplina i rapporti tra titolare e responsabile prevedendo che:

- i compiti affidati al responsabile devono essere analiticamente specificati per iscritto dal titolare dei dati;
- il responsabile deve effettuare il trattamento attenendosi alle istruzioni impartite dal titolare dei dati ;
- sul titolare incombe l'obbligo di vigilanza, anche, tramite verifiche periodiche delle osservanza delle disposizioni impartite.

Si tratta di una scelta rigorosa intesa a configurare, in capo al soggetto che dirige il trattamento, una responsabilità non eludibile attraverso l'esercizio della delega.

Quindi la nomina del responsabile, anche con ampi poteri, non ha effetti liberatori nei confronti del titolare per quanto attiene ai doveri connessi alla generale direzione dei trattamenti.

Al riguardo occorre, inoltre, ribadire che sul responsabile del trattamento dei dati incombono, secondo quanto precisato dal Garante, due distinti obblighi:

a)l'obbligo più generale di ridurre al minimo determinati rischi, la cui osservanza, a sua volta, comporta:

- la necessità di custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito;
- **l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze, avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi (articolo 31" Codice in materia di protezione dei dati personali");**

b) nell'ambito del predetto obbligo più generale, il dovere di adottare in ogni caso le "**misure minime**" di sicurezza.
In proposito giova, altresì, evidenziare come l'inosservanza dell'obbligo generale di ridurre al minimo i rischi dei dati trattati:

- rende il trattamento illecito anche se non si determina un danno per gli interessati;
- viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, terzo comma, del" Codice in materia di protezione dei dati personali");
- espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del " Codice in materia di protezione dei dati personali");
- espone, secondo quanto disposto dall'articolo 167 del citato Codice, a responsabilità penale nell'ipotesi in cui si sia proceduto in maniera illecita al trattamento dei dati - per tale intendendosi la diffusione e comunicazione dei dati al di fuori dei casi e dei modi previsti dal "Codice in materia di protezione dei dati personali" e precisamente dagli articoli 18, 19, 23, 123, 126 e 130- comportando l'applicazione della pena della reclusione da sei a diciotto mesi, se dal fatto deriva nocumento, e la reclusione da sei a ventiquattro mesi o, se il fatto consiste nella comunicazione o diffusione.

A conclusione della individuazione delle figure soggettive si evidenzia, infine, che alla base della piramide organizzativa prefigurata dal "Codice in materia di protezione dei dati personali" stanno gli incaricati del trattamento, che devono elaborare i dati personali ai quali hanno accesso, attenendosi a loro volta alle istruzioni del titolare o del responsabile secondo quanto stabilito dall'articolo 30 del Codice in questione.

3.IL DOCUMENTO PROGRAMMATICO PER LA SICUREZZA: CONTENUTI

Una volta individuate, all'interno della istituzione scolastica, le figure soggettive alle quali compete la redazione del documento programmatico per la sicurezza, occorre quindi volgere brevemente l'attenzione sulla normativa disciplinante il contenuto del DPS **che risulta essere costituita dall'allegato "B" del "Codice in materia di protezione dei dati personali".**

In proposito deve evidenziarsi che il **DPS** si pone come una vera e propria "fotografia" delle "**misure minime**" di sicurezza che vengono adottate dal titolare, dal responsabile o dall'incaricato, nel trattamento dei dati personali, all'interno dell'istituto scolastico .
Sotto tale profilo il "Codice in materia di protezione dei dati personali" ha aggiornato l'elenco delle "**misure minime**" di sicurezza stabilendo che il **DPS** deve contenere idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;

- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a 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 della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e 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;
- l'individuazione dei criteri da adottare per la cifratura o per la separazione dei dati relativi allo stato di salute e alla vita sessuale dagli altri dati personali dell'interessato.

4. **CONSEGUENZE PENALI RISPETTO ALLA REDAZIONE INCOMPLETA, FALSA O OMESSA DEL DPS.**

Alla luce di quanto sin qui esposto si tratta ora di stabilire se i comportamenti consistenti nella omessa, incompleta o falsa redazione del DPS **rilevino penalmente e dunque se determinino l'applicazione di una** sanzione penale**.**

In proposito il punto di partenza è costituito dall'articolo 169 del "Codice in materia di protezione dei dati personali" il quale punisce con la pena dell'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro chiunque, essendovi tenuto, omette di adottare le misure minime **previste dall'articolo 33 dello stesso testo normativo.**

Alcune considerazioni si impongono sul reato in questione.

In primo luogo il reato può essere commesso non da "chiunque" come erroneamente indicato dal legislatore ma solamente dai soggetti aventi una delle qualifiche soggettive sopraindicate.

In secondo luogo l'articolo 169 in questione, avuto riguardo alla pena prevista, configura l'omessa adozione delle **misure minime** di sicurezza come un reato contravvenzionale, ad integrare il quale dal punto di vista dell'elemento soggettivo del reato è sufficiente, ex articolo 42, quarto comma, del codice penale, la mera colpa.

Infine, la fattispecie *de qua* costituisce una tipica norma penale in bianco, in quanto la concretizzazione del precetto della fattispecie penale risulta affidata alle sopra richiamate prescrizioni legislative e regolamentari; prescrizioni destinate a delineare quelle **misure minime** di sicurezza la cui omissione dà luogo ad un così macroscopico e grave pericolo di lesione dei diritti della persona tale da legittimare il ricorso allo strumento penale.

Ciò premesso, al fine di meglio comprendere la rilevanza penale dei comportamenti sopradescritti, appare opportuno esaminare separatamente le diverse situazioni.

a) Rilevanza penale della omessa redazione del DPS.

Sul punto deve, infatti, rilevarsi che dubbi e perplessità, circa la rilevanza penale della omessa redazione **del** DPS**, derivano dal fatto che a stretto rigore il documento programmatico non costituisce una misura di sicurezza ma più correttamente, come sopradetto, una "fotografia" per la loro predisposizione.**

Alla luce di ciò, da un lato è sostenibile che la mancata adozione del **DPS** non si collochi all'interno del meccanismo sanzionatorio e dia quindi luogo ad un precetto senza sanzione.

Dall'altro lato, viceversa, è più correttamente ritenere che la mancata adozione del **DPS** comunque determina una violazione delle prescrizioni regolamentari in materia di **misure minime** di sicurezza e come tale rientri nel meccanismo sanzionatorio delineato dall'articolo 169 del "Codice in materia di protezione dei dati personali".

Deve ritinersi, invece, non applicabile la norma in questione nel caso di mancata adozione delle misure indicate nel DPS**.**

A sostegno di tale argomentazione si evidenzia, infatti, che:

- le prescrizioni contenute in ogni singolo **DPS** solo indirettamente derivano dalla richiamata normativa legislativa e regolamentare;
- ammettere una responsabilità significherebbe, infatti, ipotizzare paradossalmente un precetto posto dallo stesso destinatario della norma penale.

b) Incompleta redazione del DPS.

Anche per quanto riguarda la** incompleta **redazione del** DPS**, occorre riprendere il ragionamento sopra sviluppato e quindi stabilire se nonostante tale incompletezza risultino o meno soddisfatti i requisiti minimi di sicurezza.

A tal fine occorre accertare se il contenuto del** DPS **contenga o meno le informazioni essenziali richieste dall'allegato "B".

Così un** DPS **che nulla dica in merito ai criteri ed alle modalità per ripristinare la disponibilità dei dati in caso di distruzione o danneggiamento delle informazioni o degli strumenti elettronici nonché in merito alle indicazioni concernenti i criteri da adottare per cifrare o per separare i dati idonei a rivelare lo stato di salute e la vita sessuale dovrà ritenersi privo delle informazioni essenziali.

In tal caso si concretizzerà una vera e propria condotta omissiva - come tale integrante il disposto dell'articolo 169 del "Codice di protezione dei dati in materia personale"- in quanto la redazione del** DPS **risulterebbe inidonea a garantire le condizioni minime di sicurezza per la protezione dei dati personali.

C) Falsa redazione del DPS.

Nella ipotesi di **falsità** del documento la normativa di richiamo è costituita dall'articolo 479 del codice penale il quale punisce con la pena della reclusione da uno a sei anni il pubblico ufficiale che, ricevendo o formando un atto nell'esercizio delle sue funzioni, attesta falsamente fatti dei quali l'atto è destinato a provare la verità.

Infatti, attestare falsamente che sono stati adottati determinati criteri per soddisfare le** misure minime **di sicurezza, sopra elencate, costituisce attestare falsamente fatti dei quali l'atto è destinato a provare la verità e quindi condotta tale da integrare il disposto di cui all'articolo 479 del codice penale.

Sul punto deve inoltre evidenziarsi che anche il documento programmatico sulla sicurezza si configura come un atto pubblico. Infatti il costante orientamento giurisprudenziale ritiene atto pubblico non solo quello attraverso il quale la pubblica amministrazione manifesta la propria volontà, ma anche l'atto interno, in quanto documentante una attività compiuta da un pubblico ufficiale.

d) Il concorso di persone nel reato.

Stabilita dunque la rilevanza penale dei comportamenti sopraindicati, occorre ora stabilire se la responsabilità penale si radichi solamente sul responsabile del trattamento dei dati o si estenda, alla luce dei richiamati poteri di controllo, anche sul titolare del trattamento.

Al riguardo in dottrina è stato osservato che l'accentuazione della funzione di vigilanza configura per il titolare una posizione di garanzia in ordine all'impedimento di reati.

Muovendo da tale premessa si afferma pertanto che anche il titolare del trattamento dei dati concorre negli illeciti in caso di omissione del comportamento doveroso, utile ad impedire l'evento.

Infatti l'articolo 40, secondo comma, del codice penale stabilisce che non impedire un evento che si ha l'obbligo giuridico di impedire equivale a cagionarlo.

Pertanto in caso di omessa ed** incompleta **redazione del** DPS**, anche il titolare risponderà a titolo di colpa - ex articolo 40, secondo comma, del codice penale - nella ipotesi in cui abbia omesso di attivare i suoi poteri di vigilanza e di controllo.

Nel caso invece di falsità del **DPS** una eventuale responsabilità a titolo di concorso nel reato, ex articolo 110 del codice penale, potrà ritenersi configurabile esclusivamente a titolo di dolo, quando cioè tanto il titolare quanto il responsabile della redazione del **DPS** abbiano agito comunemente e siano pertanto consapevoli della falsità delle informazioni contenute nel documento.

e) Le cause di estinzione del reato

L'articolo 169 prevede infine una speciale causa di** estinzione del reato **stabilendo che:

- ***all'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi;***

- ***nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione;***
- ***l'adempimento e il pagamento estinguono il reato.***

f) Conclusioni.

In conclusione deve evidenziarsi come attraverso la **sanzione penale** il legislatore abbia inteso fornire adeguata protezione alle informazioni personali al fine di evitare pericolo di pregiudizio ai diritti degli interessati.

A tal fine tuttavia il legislatore non si preoccupa di punire solamente il titolare ed il responsabile dei dati trattati ma anche di punire chi dall'esterno tenta di aggredire di procurarsi illecitamente i dati.

Così l'articolo 615 ter del codice penale espressamente sanziona con la pena della reclusione fino a tre anni, l'accesso, in mancanza del relativo diritto, ad un sistema o ad una rete informatica in violazione delle regole di sicurezza, costruito come una sorta di violazione di domicilio informatico.

Le sanzioni amministrative di cui agli artt. 161 e segg. del D.L.vo n. 196 del 2003

A CURA DI STEFANO TOSCHEI – MAGISTRATO TAR

1. – Premessa introduttiva

Il testo del codice della privacy (D.L.vo 30 giugno 2003, entrato in vigore in data 1 gennaio 2004) è corredato nella Parte terza, intitolata "Tutela dell'interessato e sanzioni", di un Titolo III (sanzioni) composto degli artt. da 161 a 166.

La presenza di queste disposizioni nel codice della privacy (d'ora in poi, per brevità, Codice) è collegata ad una tecnica di redazione abbastanza usuale nella produzione legislativa degli ultimi anni.

Partendo dal presupposto che nessuna prescrizione di legge può dirsi realmente effettiva se non è accompagnata dalla previsione di una reazione dell'ordinamento, nei casi in cui il destinatario della norma contravvenga all'ordine che con essa gli è imposto ovvero al comportamento nella stessa norma descritto come doveroso, appare evidente che tale reazione deve essere equilibrata e corrispondere alla gravità delle violazioni contestate all'agente (cioè a colui che ha violato la norma).

Ecco, pertanto, che il Legislatore, nel redigere le disposizioni che disciplinano una determinata materia, provvede a corredare queste ultime con previsioni punitive che possono essere di natura civilistica, amministrativo-sanzionatoria ovvero penalistica:

1) nel primo caso (norme di **natura civilistica**) verrà stabilito nella legge l'obbligo per l'agente di risarcire il danno patrimoniale (e talvolta anche non patrimoniale, come il danno morale) subito dal destinatario del comportamento scorretto;
2) nel secondo caso (norme di **natura amministrativo-sanzionatoria**) sarà fatto obbligo all'agente di pagare una sanzione pecuniaria in conseguenza del comportamento tenuto che, pur essendo caratterizzato dall'aver violato prescrizioni contenute nella stessa legge che non possono considerarsi di assoluto rilievo (perché non collegate alla tutela di beni che nel comune sentire della Società sono collocati all'apice di una ipotetica scala di valori), resta comunque meritevole di una reazione da parte dell'ordinamento ed è definibile quale "illecito amministrativo";
3) nel terzo caso (norme **penali**), la reazione dell'ordinamento è la massima possibile perché l'agente, con il suo comportamento posto in essere in contrasto con la norma di legge, ha violato delle prescrizioni tese a salvaguardare beni assoluti della vita, rispetto ai quali la legge intende approntare la più adeguata formula di tutela, con la conseguenza che quel comportamento, una volta accertato dal giudice nel suo verificarsi, comporterà l'attribuzione di una sanzione penale a carico dell'agente secondo l'importanza del bene che si voleva tutelare e la gravità dei fatti (reclusione o pena pecuniaria), dando luogo ad una fattispecie di "illecito penale".

Chiarite le differenze tra i vari tipi di norme che prevedono conseguenze afflittive in danno di colui che, con il proprio comportamento, viola disposizioni di legge fissate al fine di tutelare un "bene della vita" (come è considerato, ad esempio, con riferimento al caso qui in esame, il diritto del cittadino a che non vengano divulgati e fatti conoscere all'esterno, della propria sfera di intimità, aspetti personali e condizioni a lui riferibili: c.d. privacy), secondo una scala di valori di tutela e, dunque, corrispondentemente, di gravità nella reazione dell'ordinamento, è opportuno precisare alcune caratteristiche proprie dell'illecito amministrativo in genere e delle sanzioni ad esso collegate, per poi "calare" queste nozioni nelle previsioni che sono contenute nel testo del Codice.

2. – Principi generali in materia di sanzioni amministrative.

La categoria delle sanzioni amministrative conosce una disciplina generale di riferimento contenuta nella legge 24 novembre 1981 n. 689.

Quest'ultima contiene le norme applicabili, in genere, a tutte le fattispecie nelle quali è possibile individuare nel comportamento dell'agente la realizzazione di un **illecito amministrativo** e fissa le modalità per l'irrogazione della relativa pena, costituita, per l'appunto, dal pagamento di una somma di denaro quale sanzione amministrativa.

La legge n. 689 del 1981, dunque:

- per un verso individua i casi e le modalità secondo i quali un comportamento da parte di un soggetto può essere ascritto nel novero degli illeciti amministrativi;
- per altro verso descrive la procedura attraverso la quale la conseguenza di quel comportamento, cioè la sanzione, può essere applicata, fissando anche le modalità per la definizione dell'ammontare della pena pecuniaria ed individuando sia l'Amministrazione i cui agenti possono effettuare i controlli volti ad individuare i violatori sia l'Ente in favore del quale deve essere effettuato il versamento della somma dovuta.

A tali prescrizioni, se ne aggiungono altre tese a descrivere i modi di opposizione alla sanzione comminata, al fine di permettere al sanzionato di chiedere al giudice la verifica sulla effettiva illiceità del comportamento ascrittogli e sulla correttezza dell'ammontare della sanzione inflittagli dall'Amministrazione.

In via di estrema sintesi, le regole generali per la riferibilità di un comportamento tenuto da un soggetto alla categoria degli illeciti amministrativi, di modo che si renda necessario infliggergli una **sanzione amministrativa pecuniaria**, sono le seguenti:

a) occorre che il comportamento sia indicato come "illecito amministrativo" o "violazione amministrativa" in una disposizione contenuta in una fonte legislativa e che esso sia stato posto in essere in un'epoca precedente rispetto alla data di entrata in vigore della norma stessa (principio di legalità)[23];

[23] Ciò vuol dire che, per gli illeciti amministrativi, non è applicabile il principio più favorevole al reo previsto per l'illecito penale dall'art. 2 c.p., secondo il quale nel contrasto di norme da applicarsi, perché vi è stata una successione di leggi nel tempo, prevale la legge più favorevole per il reo. Sulla inapplicabilità di detto principio al sistema degli illeciti amministrativi, si veda, da ultimo, Cass., Sez. lav., 5 novembre 2003 n. 16630 (in *Giust. civ. Mass.* 2003, f. 11), secondo la quale "In materia di illeciti amministrativi,

b) seppure ha posto in essere la condotta illecita, non può subire la irrogazione della sanzione chi, al momento del fatto, non aveva compiuto i diciotto anni o non aveva, in base ai criteri indicati nel codice penale, la capacità di intendere e di volere, salvo che lo stato di incapacità non derivi da sua colpa o sia stato da lui preordinato (principio della capacità)[24];
c) il comportamento, per essere sanzionabile, deve essere stato realizzato, con una azione ovvero una omissione, volontariamente e coscientemente e senza che l'agente si trovasse in una delle condizioni di scusabilità (adempimento di un dovere, esercizio di una facoltà legittima, stato di necessità o di legittima difesa, violazione commessa per ordine dell'Autorità) descritte nella stessa legge n. 689 del 1990 (elemento soggettivo)[25];
d) se la condotta è stata realizzata grazie all'utilizzo di un bene appartenente a persona diversa dall'agente, quest'ultimo ne risponde divenendo obbligato in solido, con l'autore della violazione, per il pagamento della sanzione pecuniaria (principio di solidarietà);
e) l'obbligazione di pagare la sanzione amministrativa non si trasmette agli eredi e, dunque, si estingue con la morte dell'autore della violazione (principio di intrasmissibilità);

---

l'operatività dei principi di legalità, di irretroattività e di divieto di analogia, risultante dall'art. 1 della legge n. 689 del 1981, comporta l'assoggettamento della condotta considerata alla legge del tempo del suo verificarsi, con conseguente inapplicabilità della disciplina posteriore più favorevole e, al fine di escludere l'applicabilità della norma sopravvenuta, resta determinante il momento della commissione dell'illecito (come per il decorso della prescrizione ai sensi dell'art. 28, legge n. 689 del 1981), integrando l'ordinanza - ingiunzione non un provvedimento amministrativo costitutivo, ma un atto puramente esecutivo, preordinato soltanto alla riscossione di un credito già sorto per effetto della violazione commessa".

24 Da tale principio discende che l'illecito amministrativo deve essere sempre collegato ad una condotta tenuta da una persona fisica, anche se formalmente questa agisce per una persona giuridica (Ente, pubblico, Società, ecc.). In argomento Cass., Sez. I, 30 maggio 2001 n. 7351 (in Giust. civ., Mass. 2001, 1088) che ha chiarito come "Le sanzioni amministrative rientrano tra quelle sanzioni repressive per le quali è richiesta, oltre alla capacità di intendere e volere la colpa o il dolo (art. 2 e 3 della legge n. 689 del 1981); conseguentemente, una persona giuridica non può considerarsi autore della violazione alla quale la legge riconnetta dette sanzioni ma, ai sensi dell'art. 6 della legge n. 689 del 1981, è solo obbligata in solido per le violazioni commesse, "nell'esercizio delle proprie funzioni o incombenze", dal suo rappresentante o dai suoi dipendenti, con diritto di regresso nei confronti degli stessi; a tal fine non è sufficiente che l'attività di questi sia imputabile alla persona giuridica ma occorre anche che sia posta in essere nell'interesse della stessa".

25 E' però vero che non tutti gli ordini amministrativi possono essere considerati quali elementi di giustificazione di un comportamento dell'agente costituente illecito amministrativo, tanto più se quel comportamento è posto in essere sulla base di una prassi amministrativa che, di per sé, non può rilevare quale elemento di scusante. In tal senso si è espressa la Corte di cassazione, Sezione lavoro, nella sentenza 2 ottobre 2001 n. 14168 (in *Foro amm. CDS* 2002, 2325), affermando che "Con riguardo ad infrazione amministrativa, un comportamento od una prassi di mera tolleranza da parte della p.a. non possono essere invocati come esimente, nè sotto il profilo del difetto di coscienza e volontarietà dell'azione (art. 3, comma 1, l. 24 novembre 1981 n. 689), il quale ricorre solo in presenza di azioni non dominabili dalla sfera psichica dell'agente, nè sotto il profilo dell'errore incolpevole (comma 2 del citato art. 3), mancando i requisiti della scusabilità ed inevitabilità dell'errore medesimo".

f) se l'agente viola con una azione od omissione più disposizioni di legge che prevedono sanzioni amministrative o commette più violazioni della stessa disposizione, deve rispondere della sanzione prevista per la violazione più grave, aumentata sino al triplo (concorso di sanzioni)[26].

La sanzione può essere irrogata solo all'esito di un **procedimento** al quale l'agente, una volta contestatagli la violazione della norma, può partecipare producendo atti difensivi o chiedendo di essere sentito. Una volta definita la sanzione ed emanato il relativo provvedimento (di **ingiunzione** al pagamento di una somma di denaro in favore dell'Amministrazione competente), quest'ultimo può essere impugnato dinanzi al giudice ordinario (giudice di pace o Tribunale secondo l'entità della sanzione ovvero il tipo di violazione) che, eventualmente, accogliendo il ricorso potrà annullare la sanzione ovvero ridurne l'importo.

3. – Gli illeciti amministrativi previsti nel codice della privacy.

Si è detto che la legge n. 689 del 1981 contiene la disciplina generale sulle sanzioni amministrative. Tali norme, però, debbono tenere conto dell'esistenza di regole speciali fissate da altre e diverse leggi che, a loro volta, regolamentano settori particolari. In altri termini, in un determinato settore la legge speciale individua la disciplina delle sanzioni amministrative per quella materia, tenendo conto anche dei principi fissati nella legge n. 689 del 1981: laddove un certo aspetto di una materia, relativo agli illeciti amministrativi, non sia regolamentato dalla legge speciale, dovrà applicarsi la disciplina generale contenuta nella legge n. 689 del 1981.

Per quanto riguarda il Codice, i comportamenti che danno luogo ad **illecito amministrativo** sono descritti negli artt. 161-165, attraverso fattispecie che, qui di seguito, si provvede ad analizzare singolarmente.

Preliminarmente si precisa che del comportamento considerato illecito dal Codice dovrà rispondere astrattamente l'Ente quale "titolare" del trattamento dei dati, ma concretamente la sanzione sarà ascritta, secondo le regole generali di cui alla legge n. 689 del 1981, al responsabile del trattamento dei dati nella qualità di trasgressore e (se le due figure non dovessero coincidere) al dirigente della struttura che ha nominato il

[26] Più in particolare, in materia si è detto che "In tema di sanzioni amministrative, l'art. 5 della legge n. 689 del 1981, il quale contempla il concorso di persone nella commissione di illeciti amministrativi, recepisce i principi fissati in materia dal codice penale, rendendo applicabile la pena pecuniaria a tutti coloro che abbiano offerto un contributo alla realizzazione dell'illecito, concepito come una struttura unitaria, nella quale confluiscono tutti gli atti dei quali l'evento punito costituisce il risultato, anche se detti atti, atomisticamente considerati, possono non essere illeciti, sempre che sussista nei singoli partecipi la consapevolezza del collegamento finalistico dei vari atti, e, cioè, la coscienza e volontà di portare un contributo materiale e psicologico alla realizzazione dell'illecito perseguito da tutti" (così Cass., Sez. I, 19 luglio 2001 n. 9837, in *Giust. civ. Mass.* 2001, 1426).

.

responsabile del trattamento e che, dunque, ha il dovere di controllare ed il potere di intervenire sui comportamenti di detto responsabile, in solido con quest'ultimo. Conseguentemente, nell'esposizione, si farà riferimento all'Ente come soggetto passivo della sanzione, ma quest'ultima dovrà intendersi riferita sia al responsabile del trattamento dei dati (quale **trasgressore**) sia al titolare, cioè al rappresentante legale dell'Ente ovvero al direttore dell'unità organizzativa che ha individuato il responsabile dei dati (quale **responsabile in solido**).

Omessa o inidonea informativa all'interessato (art. 161). Il comportamento punito consiste nella violazione delle prescrizioni contenute nell'art. 13 del Codice che fissa le modalità attraverso le quali deve effettuarsi l'informativa all'interessato sulla circostanza che l'Ente è in possesso di suoi dati personali, comunicandogli (per iscritto, sarebbe consigliabile ovvero oralmente):

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7 (cioè il diritto all'accesso ai dati e gli altri diritti che riguardano la tenuta e la gestione degli stessi);
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

Nel caso in cui sia omessa una delle prescrizioni sopra elencate ovvero essa sia comunicata con mezzi, forme e modalità inidonee si provocheranno due ordini di conseguenze:

- da un lato l'eventuale consenso prestato dall'interessato sarà da considerarsi invalido, sicché sarà illegittimo ogni successivo trattamento dei suoi dati;
- per altro verso, comunque, l'Ente sarà condannato al pagamento di una sanzione che potrà essere tanto più elevata nel suo ammontare in quanto il trattamento riguardi dati sensibili o giudiziari ovvero dal mancato consenso si sia cagionato un pregiudizio all'interessato particolarmente grave.

La cessione dei dati (art. 162). In questo caso il Codice ha voluto punire la cessione a terzi di dati in violazione di quanto previsto dall'art. 16, comnm1, lett. b) dello stesso Codice o in altre disposizioni in materia di disciplina di trattamento dei dati personali. L'art. 16, comma 1, lett. b) del Codice, infatti, non esclude che i dati personali possano essere ceduti ad altro titolare, purché siano destinati ad un trattamento compatibile con gli scopi per i quali i dati sono stati raccolti. Ciò sta a significare che il responsabile dei dati dovrà spingere la propria diligenza, nel trattamento degli stessi, fino al punto

di assicurarsi che dopo la cessione il trattamento da parte del nuovo utilizzatore avvenga nei limiti degli scopi che ne avevano consentito, originariamente, la raccolta. Pertanto l'Ente cedente dovrà condizionare la cessione al rispetto degli scopi che hanno originato la raccolta nonché, qualora il comportamento del cessionario non fosse improntato al rispetto di tale condizione, venendone a conoscenza (e solo se ne sia venuto a conoscenza) l'Ente cedente dovrà denunciare il fatto ed inibire l'utilizzo dei dati da parte del cessionario. Un diverso comportamento nel momento della cessione dei dati e (verosimilmente e solo nei limiti sopra riferiti) successivamente, a cessione avvenuta, espone l'Ente alla comminazione della sanzione amministrativa consistente nel pagamento di una somma da 5 mila euro a 30 mila euro.

In particolare, al secondo comma dell'art. 162 del Codice si punisce, con la sanzione pari ad una somma da 500 euro a 3000 euro, chi abbia violato la prescrizione dell'art. 84 del Codice che, a propria volta, fissa una speciale procedura per la conoscenza di dati sanitari, richiedendo che ciò avvenga solo per il tramite di un medico designato dall'interessato ovvero dall'Ente titolare dei dati.

Omessa o incompleta notificazione (art. 163). L'art. 37 del Codice stabilisce che il titolare dei dati ha l'obbligo di notificare al Garante, secondo le rigide modalità descritte nel successivo art. 38, un documento con il quale segnala, prima del loro trattamento, i dati personali in ordine ai quali intende procedere al trattamento stesso - nel caso in cui ci si riferisca a dati di un certo rilievo per l'interessato (e indicati nell'elencazione contenuta nell'art. 37) – oltre ad illustrare la struttura organizzativa dell'Ente medesimo, le caratteristiche del trattamento dei dati, l'apparato di sicurezza degli archivi dei dati. Chiunque, essendovi tenuto, non provveda tempestivamente alla notificazione, la effettui con modalità non corretta ovvero indichi elementi in modo incompleto, è punito con una sanzione amministrativa consistente nel pagamento di una somma da 10 mila euro a 60 mila euro, oltre a subire la pubblicazione dell'ordinanza-ingiunzione attraverso la quale la sanzione gli è comminata, per intero o per estratto, in uno o più giornali indicati nella stessa ordinanza.

Omessa informazione o esibizione al Garante (art. 164). Il comportamento punito è quello del titolare o del responsabile dei dati che, nel corso di una procedura giustiziale (a seguito di ricorso proposto dall'interessato) che si sta svolgendo innanzi al Garante, richiesto da quest'ultimo di riferire in merito ai fatti, non adempia fornendo le richieste informazioni ovvero non dia luogo alla produzione di documenti siccome richiesti. La sanzione prevista è quella del pagamento di una somma da 4000 euro a 24 mila euro.

Alle disposizioni sugli illeciti amministrativi previsti dal Codice, seguono:

A) l'art. 165 che stabilisce che sia in facoltà del Garante (quale autorità preposta ad irrogare le sanzioni amministrative qui descritte) di comminare, oltre alla pena pecuniaria, la sanzione accessoria consistente nella pubblicazione del provvedimento ingiuntivo, per intero o per estratto, su uno o più giornali indicati nello stesso provvedimento; ciò nei casi di inflizione della sanzione per la condotta concretizzante illecito amministrativo ai sensi degli artt. 161 (omessa o inidonea informativa all'interessato), 162 (cessione dei dati e conoscenza

impropria di dati sanitari) e 164 (omessa informazione o esibizione al Garante);

B) l'art. 166 che fissa le regole di procedura per la comminazione della sanzione, rinviando a quelle contenute nella legge generale sulle sanzioni amministrative (legge n. 689 del 1981) ed individuando nel Garante l'autorità preposta a svolgere il relativo procedimento di valutazione dell'illiceità del comportamento tenuto dal rappresentante (titolare o responsabile del trattamento dei dati) dell'Ente nonché la materiale adozione del provvedimento con il quale si applica (al trasgressore ed al responsabile in solido, con le peculiarità più sopra riferite) la sanzione amministrativa.

LA PRIVACY. L'ESPERIENZA DELL'UFFICIO SCOLASTICO REGIONALE A SERVIZIO DELLE SCUOLE DEL FRIULI VENEZIA GIULIA

A cura di Pier Giorgio Cataldi – Direttore Generale Ufficio Scolastico Regionale per il Friuli Venezia Giulia

Stare dalla parte delle scuole per i servizi che sono tenute a svolgere come istituzioni diffuse nel territorio.

Servizi, non parlo di quelli didattico-formativi, che una società regolata in modo sempre più sofisticato come quella italiana richiedono in misura crescente ed assillante.

Un passo indietro: la legge 241 del 1990, abbandonando il modello cavouriano di amministrazione pubblica, a sua volta di derivazione francese, tolse al potere autoritativo degli organi deputati a funzioni o servizi pubblici la presunzione di legittimità degli atti, salvo i ricorsi. Impose le regole del procedimento partecipato, responsabile, trasparente.

L'Amministrazione fu chiamata a guardare dentro se stessa e a… farsi guardare in trasparenza. Di qui la faticosa regolamentazione dei propri atti e l'esposizione di ogni pubblico funzionario a rispondere del proprio procedere prima ancora del proprio provvedimento.

Un portato più recente di civiltà è quello della c.d. privacy: l'individuo, protetto nei confronti dell'Amministrazione come fruitore o destinatario di provvedimenti è, ancor prima, da proteggere come persona nella sua soggettività nell'ambito di qualsiasi rapporto di carattere pubblico o privato in cui venga a trovarsi coinvolto.

Parlo della normativa che, da ultimo, si è condensata nel Decreto Legislativo 196 del 2003, Testo Unico sulla privacy.

A maggio di questo anno – come al solito la febbre viene quando si deve partire – si constata che una norma inderogabile e sanzionata penalmente dal Testo Unico, impone a tutti i soggetti, pubblici o privati detentori di dati personale, di predisporre entro la fine di giugno il "Documento Programmatico per la Sicurezza", la regolamentazione, cioè, del modo di trattare e conservare dati personali che, in un modo o in un altro, per ragioni di salute, razziali o religiose, si presentassero come dati "sensibili".

A maggio ci si rende conto, si rendono conto i Dirigenti Scolastici, che le scuole – ogni scuola – integrano perfettamente la figura istituzionale del soggetto tenuto a predisporre il DPS.

Nella mia Regione, dove l'Ufficio Scolastico ha la consuetudine di curare molto i rapporti non solo formali ma anche di sostanziale collaborazione con l'Avvocatura dello Stato e con la Corte dei Conti, una rapida consultazione consente di scoprire che un magistrato della Corte dei Conti di Trieste ed un suo collega della Corte dei Conti di Milano – anche per rapporti professionali con il Garante della privacy – hanno studiato approfonditamente il problema.

Dunque: da una parte la domanda diffusa nel territorio di istruzioni, indicazioni, aiuti; dall'altra parte l'accessibilità da parte dell'Ufficio Scolastico Regionale ad una consulenza esperta.

Al 29 di maggio era già organizzato un incontro informativo con tutti i Dirigenti scolastici della Regione su: "Il testo unico sulla privacy – esame degli obblighi gravanti sulle amministrazioni scolastiche". Relatori magistrati contabili esperti.

Dal seminario – nel senso che si seminò consapevolezza del problema – emerse la domanda dei Dirigenti scolastici di avere dall'Ufficio Scolastico Regionale una traccia di DPS, piuttosto che acquistarla singolarmente a privati che si erano proposti come esperti.

A quel punto il mio Ufficio si sbilanciò nel promettere… l'opera dei due magistrati ed effettivamente, in un successivo incontro del 19 giugno, esteso questa volta anche ai Direttori dei Servizi Generali ed Amministrativi, consegnò uno schema dettagliato di DPS, studiato anche previa l'intervista di Dirigenti scolastici che avevano prospettato tutte le possibili situazioni di trattamento o di conservazione dei dati personali, verificabili a scuola.

Anche se un decreto legge ha poi prorogato a fine dicembre 2004 il termine ultimo per predisporre il DPS, è evidente quanto decisivo era stato il servizio organizzato centralmente dall'Ufficio Scolastico Regionale rispetto alla domanda diffusa delle Istituzioni scolastiche. Servizio richiesto ancora dai Dirigenti e predisposto dall'Ufficio in termini di prosecuzione del percorso di formazione sulla materia della privacy, sul suo raffronto con gli obblighi della trasparenza, sullo studio di caso, sulla giurisprudenza e sulle pronunce del Garante: tutte tematiche che occuperanno la fine di questo anno e l'inizio del prossimo.

Per completezza di informazione non va dimenticato che gli stessi obblighi di predisposizione del DPS e di formazione circa le problematiche della privacy incombono sugli uffici dell'Amministrazione. Per questa ragione, lo stesso percorso previsto per i Dirigenti scolastici è stato destinato ai Dirigenti ed ai Funzionari della Direzione Generale e dei Centri Servizi Amministrativi della Regione.

Tutto l'articolato percorso offerto alle scuole del Friuli Venezia Giulia è poi sembrato prezioso al Ministero – Direzione Generale del personale della scuola – che ha pensato, attraverso un progetto nazionale, di metterlo a disposizione di tutte le Istituzioni scolastiche del Paese, attraverso gli Uffici Scolastici Regionali propensi all'impegno.

Ed è questo un esempio di come essere dalla parte delle scuole per i servizi che sono tenute a svolgere in modo diffuso nel territorio.