



Ministero dell'Istruzione, dell'Università e della Ricerca
Ufficio Scolastico Regionale per il Piemonte
Direzione Generale

Prot. n. 1711/U

Torino, 6 marzo 2015

Ai Dirigenti
delle istituzioni scolastiche
di ogni ordine e grado
statali e paritarie
del Piemonte

p.c. ai Dirigenti e Reggenti
degli Ambiti Territoriali
del Piemonte

Oggetto: la privacy a scuola – Normativa, giurisprudenza e casi pratici

Nel corso degli ultimi anni la tematica della protezione dei dati personali ha subito molteplici cambiamenti in ogni ambito, compreso quello scolastico. In quest'ultimo settore da un lato è mutato il rapporto tra il diritto alla riservatezza e la tutela di altri valori, quali il diritto alla sicurezza e il diritto alla conoscenza, aspetti ormai fondamentali dell'epoca attuale. Dall'altro lato, lo sviluppo dei sistemi di telecomunicazione offre continuamente nuove possibilità di acquisizione, conservazione, utilizzazione dei dati e delle informazioni, a costi sempre più contenuti. L'incrocio di questi fenomeni – come sostiene l'uscente Presidente Francesco Pizzetti nella relazione annuale del 2010 - è il terreno sul quale la protezione dei dati personali è costantemente sfidata.

La presente trattazione intende prendere in esame - secondo una divisione per macro argomenti (comprendente un quadro sintetico e un approfondimento) – le principali pronunce e i provvedimenti normativi intervenuti sul tema nell'ultimo decennio. L'obiettivo è quello di integrare con casi pratici e riferimenti normativi il vademecum già noto alle scuole dal titolo "La privacy tra i banchi di scuola". Una particolare attenzione è stata altresì rivolta al Codice della Privacy le cui norme, per agevolazione di lettura del presente documento, sono state per lo più riportate in nota.

INDICE

PARTE I

Telecamere, videofonini, foto, registrazioni, videosorveglianza e biometria pag. 1

PARTE II

Privacy e trasparenza sul web - Informazioni e dati relativi agli studenti e alle loro famiglie pag.16

PARTE III

Cyberbullismo pag. 35

PARTE IV

Accesso agli atti pag. 50

PARTE I

Telecamere, videofonini, foto, registrazioni, videosorveglianza e biometria

Quadro sintetico

Si possono in generale installare **telecamere** o sistemi di **videosorveglianza** all'interno degli istituti scolastici, ma devono funzionare solo negli orari di chiusura degli istituti e la loro presenza deve essere segnalata con cartelli visibili anche di notte. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato. L'utilizzo di tali sistemi è

ammesso in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici. Le immagini registrate possono essere conservate solo per brevi periodi e devono essere cancellate in generale dopo 24 ore. E' vietato attivare le telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola. Deve, in ogni caso, essere garantito *"il diritto dello studente alla riservatezza"* (art. 2, comma 2, D.P.R. n. 249/1998¹), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo della personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione.

L'utilizzo di videofonini, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per fini personali e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte, in particolare della loro immagine e dignità. Le istituzioni scolastiche possono comunque, nella loro autonomia, decidere come regolamentare o se vietare del tutto l'uso dei **cellulari, smartphone e tablet** all'interno delle aule di lezione o nelle scuole stesse. Non si possono, in ogni caso, diffondere immagini, video o foto sul *web* o comunicare sistematicamente i dati personali di altre persone senza aver prima informato adeguatamente le persone coinvolte e averne ottenuto l'esplicito consenso. Gli studenti e gli altri membri della comunità scolastica devono quindi prestare particolare attenzione a non mettere *on line* immagini (ad esempio su *blog*, siti *web*, *social network*) o a diffonderle tramite *app* di messaggistica istantanea. Succede spesso, infatti, che una fotografia inviata a un amico/familiare, poi venga inoltrata ad altri destinatari, generando involontariamente una comunicazione a catena dei dati personali raccolti. Tale pratica può dar luogo a gravi violazioni del diritto alla riservatezza delle persone riprese, facendo incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati.

E' possibile **registrare la lezione** esclusivamente per scopi personali, ad esempio per motivi di studio individuale. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare adeguatamente le persone coinvolte nella registrazione (professori, studenti, ecc...) e ottenere il loro esplicito consenso. Nell'ambito dell'autonomia scolastica gli istituti possono decidere di regolamentare diversamente o anche di inibire gli apparecchi in grado di registrare.

Non violano la privacy le **riprese video** e le **fotografie** raccolte dai genitori, **durante le recite, le gite e i saggi scolastici**. Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione. Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet e sui *social network* in particolare. In caso di comunicazione sistematica o diffusione diventa, infatti, necessario, di regola, ottenere il consenso delle persone presenti nelle fotografie e nei video.

E' in linea generale vietato il trattamento dei **dati biometrici** riferiti ai lavoratori e agli studenti: l'utilizzo delle impronte digitali o di altri dati biometrici per rilevare la presenza di un gruppo di individui è giustificato soltanto dall'esistenza di reali esigenze di sicurezza, determinate da concrete e gravi situazioni di rischio. Il sistema di rilevamento delle impronte digitali, ad esempio, è stato giudicato sproporzionato rispetto all'obiettivo di consentire agli studenti l'accesso ai servizi di mensa universitaria.

¹ In **D.P.R. 249/1998** "Regolamento recante lo Statuto delle studentesse e degli studenti della scuola secondaria", **art. 2** "Diritti", comma 2: "La comunità scolastica promuove la solidarietà tra i suoi componenti e tutela il diritto dello studente alla riservatezza".

Approfondimento: casi pratici e normativa di riferimento

- Provvedimento Garante n. 262 del 30 maggio 2013 – Argomento: dispositivo “a riconoscimento biometrico”

Con segnalazione del 31 ottobre 2012 si è lamentato che presso l'Istituto Tecnico Industriale “E. M.” di M. sarebbe stato installato un dispositivo “a riconoscimento biometrico (impronta digitale)” per finalità di “controllo del rispetto dell’orario di servizio” del personale amministrativo tecnico e ausiliario (c.d. A.T.A.) senza che allo stesso fosse stata prestata una “informativa specifica” (anche per quanto riguarda l’indicazione delle categorie di soggetti che hanno accesso ai dati personali biometrici trattati). Tale trattamento, secondo quanto lamentato, non rispetterebbe le condizioni di liceità stabilite dal Garante in relazione ai dati biometrici dei lavoratori. Nel caso di specie il D.S. aveva sostenuto l’indispensabilità del provvedimento per esigenze di sicurezza di beni e persone; aveva segnalato il verificarsi di “numerosi casi di allontanamento e/o di ritardo dal servizio dopo aver (...) regolarmente firmato il foglio delle presenze”, nonché il verificarsi di casi di “sparizione di documenti riservatissimi”; aveva inoltre informato “tutto il personale A.T.A.” circa la decisione di adottare il menzionato sistema di rilevazione presenze, sia verbalmente sia con apposita circolare. Il Garante, più volte interpellato in relazione alla valutazione di liceità dei trattamenti dei dati biometrici riferiti ai lavoratori, precisa che *“tali dati possono essere di regola utilizzati solo in casi particolari, tenuto conto delle finalità perseguite dal titolare e del contesto in cui il trattamento viene effettuato, nonché – con specifico riguardo ai luoghi di lavoro – per presidiare l’accesso ad “aree sensibili” in considerazione della natura delle attività ivi svolte”*. In particolare, il Garante ritiene *“ammissibile il ricorso a tecniche biometriche di autenticazione quale necessaria misura di sicurezza”* (ad esempio, in relazione ad operazioni concernenti i dati di traffico telefonico e telematico) e *“ne riconosce altresì la legittimità e la proporzionalità per finalità di autenticazione dell’utente nell’ambito di servizi di firma digitale remota”*. Tali presupposti non risultano tuttavia ricorrere nella fattispecie in esame, posto che il sistema biometrico risulta essere stato installato presso l'Istituto allo scopo di effettuare la rilevazione delle presenze dei dipendenti. *“A tale proposito, con riferimento all’applicazione dei principi di necessità, nonché di pertinenza e non eccedenza (art. 11, comma 1, lett. d), del Codice²) dei trattamenti effettuati in relazione alle finalità perseguite, il Garante ha di regola ritenuto sproporzionato l’impiego generalizzato di dati biometrici per finalità di rilevazione delle presenze dei lavoratori. Tale valutazione tiene conto della possibilità di utilizzare idonee modalità alternative, adottando soluzioni tecnico-organizzative che non incidano sulla libertà e la dignità stessa dei lavoratori interessati (art. 2 del Codice³), preordinate all’accertamento parimenti efficace e rigoroso dell’effettiva presenza dei dipendenti in servizio. Il titolare del trattamento, infatti, allo scopo di verificare il puntuale rispetto dell’orario di lavoro ben può disporre di altre (più “ordinarie”) misure, meno invasive della sfera personale nonché della libertà individuale del lavoratore, che non ne coinvolgano la dimensione corporale. Aspetti, questi, costitutivi della dignità personale, a presidio della quale sono dettate le discipline di protezione dei dati personali, come emerge dall’art. 2 del Codice”. (...) Né è risultata comprovata (ma solo allegata) l’inefficacia del possibile utilizzo degli strumenti automatici di rilevazione delle presenze d’uso comune (si pensi a badge marcatempo), come pure degli ordinari controlli, se del caso a campione, circa la presenza dei lavoratori (che solo a domanda possono*

² Per l’art. 11 C.P. vedi *infra* nota n. 4, pag. 4.

³ In Parte I “Disposizioni generali”, Titolo I “Principi generali”, art. 2 Codice Privacy (di seguito C.P.) “Finalità” : “1. Il presente testo unico, di seguito denominato “codice”, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell’interessato, con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali. 2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l’adempimento degli obblighi da parte dei titolari del trattamento”.

assentarsi temporaneamente dal lavoro), da effettuarsi per il tramite del personale direttivo (sul quale anzitutto incombe la verifica quotidiana, peraltro di immediata evidenza e comunque di agevole accertamento all'interno di un istituto scolastico). (...) Peraltro il trattamento dei dati biometrici per la finalità qui considerata, oltre ad essere in linea di principio (nonché, per quanto detto, nel caso di specie) sproporzionato, potrebbe comunque in concreto rivelarsi di scarsa utilità nel contrasto delle asserite (pur limitate) ipotesi di allontanamento dal servizio, atteso che, in difetto di efficaci sistemi di controllo e vigilanza sull'effettiva (operosa) presenza dei lavoratori durante l'arco dell'intera giornata lavorativa, la prospettata modalità di rilevazione delle presenze non è di per sé in grado di assicurare l'effettiva presenza sul luogo di lavoro di dipendenti infedeli (...). Tanto premesso, il Garante, ritenuto che il trattamento effettuato dall'Istituto nel caso di specie sia avvenuto in violazione dei principi di liceità, necessità, pertinenza e non eccedenza rispetto agli scopi perseguiti (artt. 11, comma 1, lett. a) e d) del Codice⁴), ha dichiarato illecito il trattamento dei dati biometrici riferiti ai lavoratori e ne ha disposto il divieto ai sensi degli artt. 154, comma 1, lett. d)⁵, 144 e 143, comma 1, lett. c)⁶, del Codice.

- Provvedimento Garante n. 261 del 30 maggio 2013 – Argomento: dispositivo “a riconoscimento biometrico” e sistema di videosorveglianza

Analogo provvedimento (deciso nella stessa data) ha riguardato il Liceo Scientifico “Y” di R.. Nel caso di specie si trattava dell'installazione di alcune telecamere all'interno dell'istituto nonché del trattamento di dati biometrici ricavati dalle impronte digitali di alcuni docenti (e anche del personale non docente) finalizzato alla rilevazione delle presenze dei dipendenti. In particolare, nella segnalazione veniva rappresentato che all'interno dell'istituto scolastico sarebbero state presenti, senza che ne fosse stato formalmente informato il personale, alcune telecamere per le quali non erano state rese note né le ragioni dell'installazione, né l'orario di attivazione, né se fossero state effettuate registrazioni, né chi fosse a conoscenza delle *password* per accedere alle riprese o alle registrazioni. In prossimità dell'area videosorvegliata inoltre non erano stati apposti i dovuti cartelli di segnalazione. Gli ispettori della Direzione territoriale del Lavoro di Roma informavano il Garante di aver rilevato, oltre alle telecamere, un apparecchio di rilevazione digitale delle presenze del personale docente senza che la predetta installazione risultasse avvenuta in conformità alla legge n. 300/1970 (Statuto dei lavoratori). Ottemperato all'ordine di disinstallazione, l'istituto scolastico presentava istanza per essere autorizzato a reinstallare l'impianto di videosorveglianza e il dispositivo a riconoscimento biometrico chiedendo al Garante un “parere sulla legittimità dell'utilizzo di un tale sistema di rilevazione presenze”. Il Garante si pronunciava negli stessi

⁴ In Parte I “Disposizioni generali”, Titolo III “Regole generali per il trattamento dei dati”, Capo II “Regole per tutti i trattamenti”, art. 11 C.P. “Modalità del trattamento e requisiti dei dati”: “1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; (...) d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati (...)”.

⁵ In Parte III “Tutela dell'interessato e sanzioni”, Titolo II “L'Autorità”, Capo I “Il Garante per la protezione dei dati personali”, art. 154 C.P. “Compiti”: “1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: (...) d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporre il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali; (...)”.

⁶ In Parte III “Tutela dell'interessato e sanzioni”, Titolo I “Tutela amministrativa e giurisdizionale”, Capo I “Tutela dinanzi al Garante”, Sezione II “Tutela amministrativa”, art. 143 C.P. “Procedimento per i reclami”: “1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento: (...) c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati; (...); art. 144 C.P. “Segnalazioni”: “I provvedimenti di cui all'articolo 143 possono essere adottati anche a seguito delle segnalazioni (...), se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento (...)”.

termini di cui al precedente provvedimento, richiamando i **principi di necessità, di pertinenza e non eccedenza** e sottolineando la **sproporzione dell'impiego generalizzato di dati biometrici per finalità di rilevazione delle presenze dei lavoratori**. Evidenziava altresì, anche in questo caso, la **possibilità di utilizzare idonee modalità alternative, adottando soluzioni tecnico-organizzative che non incidessero sulla libertà e la dignità stessa dei lavoratori**. A fronte della lamentata difficoltà da parte del Dirigente Scolastico di verificare l'effettiva presenza dei lavoratori al fine di erogare eventuali compensi per lavoro straordinario, il Garante sottolineava l'opportunità di adottare altri più "ordinari" sistemi (quali ad es. la compilazione dell'apposito foglio firme o del registro di classe) **meno invasivi della sfera personale e della libertà individuale del lavoratore, che non ne coinvolgessero la dimensione corporale**. Non essendo pertanto stati rappresentati dal titolare del trattamento concreti elementi in base ai quali poter desumere l'inidoneità delle ordinarie misure di controllo e, correlativamente, la indispensabilità del trattamento dei dati biometrici, il trattamento degli stessi doveva considerarsi illecito. Quanto poi all'installazione delle telecamere, il Liceo non aveva fornito alcun elemento né con riguardo alle ragioni che ne avrebbero reso necessaria l'installazione all'interno dell'istituto, né con riguardo alle modalità con le quali l'informativa avrebbe dovuto essere resa non solo ai lavoratori, ma anche all'intera popolazione studentesca (nonché alle famiglie degli allievi). Tanto premesso, anche il trattamento di dati personali effettuato mediante il sistema di videosorveglianza veniva ritenuto illecito, in quanto in violazione della disciplina prevista dagli artt. 13⁷, 114 del Codice e 4, comma 2, l. n. 300/1970⁸.

⁷ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo I "Regole per tutti i trattamenti", **art. 13 C.P. "Informativa"**: 1. *L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:*

- 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;*
- 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.*
- 2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.*
- 3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.*
- 4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.*
- 5. La disposizione di cui al comma 4 non si applica quando:*
 - a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;*
 - b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;*
 - c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.*
- 5-bis. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f)".*

- **Provvedimento Garante n. 230 dell'8 maggio 2013 – Argomento: sistema di videosorveglianza tramite webcam in asilo nido**

Il tema dei sistemi di videosorveglianza ha di recente formato oggetto di un interessante provvedimento. Nel caso di specie l'Autorità, attraverso un articolo pubblicato su un quotidiano nazionale, veniva a conoscenza del fatto che l'asilo nido "X" aveva installato presso la propria struttura un sistema di videosorveglianza dotato di webcam, in grado di consentire ai genitori di controllare i propri figli minori durante il periodo di permanenza al nido ("quando questi sono affidati alle maestre"). Stanti le evidenti implicazioni in tema di riservatezza derivanti dall'installazione di tale sistema, il Garante inviava all'asilo nido precise richieste di informazioni al fine di acquisire specifici ragguagli sulla vicenda e, segnatamente, per conoscere le modalità di funzionamento e le finalità del sistema, i presupposti che ne avrebbero giustificato l'installazione, le modalità impiegate per rendere un'adeguata informativa agli interessati e le misure di sicurezza adottate per evitare eventuali accessi non autorizzati alle immagini o, comunque, eventuali trattamenti di dati non conformi a legge. La scuola dichiarava che la *webcam* sarebbe stata installata "sia per motivi di sicurezza a protezione dei beni e delle persone (...), sia per venire incontro alle esigenze rappresentate dai genitori". In particolare, sosteneva che il sistema avrebbe costituito un valido deterrente – "ormai generalmente utilizzato in luoghi pubblici e privati" - contro eventuali malintenzionati, in quanto l'ubicazione al piano terreno della struttura la rendeva "facilmente raggiungibile e accessibile"; inoltre, la società affermava che "la presenza di una *webcam* all'interno degli asili", costituiva oramai una realtà consolidata in altre nazioni tipo gli Stati Uniti. Più esattamente, si trattava di un servizio sempre più richiesto da mamme e papà impegnati sul posto di lavoro che così avrebbero avuto "un prezioso strumento per partecipare alla crescita dei loro figli ed alla magia di vederli maturare mentre sviluppano le loro cognizioni sociali", rispondendo altresì ad un'istanza legata alla sicurezza". La società ha dichiarato inoltre che i genitori/tutori dei minori iscritti avrebbero sottoscritto un'apposita informativa recante l'indicazione della presenza della *webcam*, nonché, riguardo al possibile controllo a distanza dei lavoratori, che il personale sarebbe stato informato dell'esistenza della *webcam* e che, in merito, gli insegnanti avrebbero rilasciato un'apposita liberatoria.

Il Garante, investito del caso, ha riaffrontato il tema della videosorveglianza riaffermando la **preminenza dell'interesse generale del minore quale criterio informatore delle scelte che lo riguardano anche sotto il profilo della tutela dei dati personali** e ammettendo **l'impiego di tali sistemi nei soli casi in cui l'installazione risulti effettivamente necessaria e proporzionata**. Tali principi sono stati poi ribaditi dalla Commissione europea in occasione di un'interrogazione parlamentare formulata proprio in relazione alla tematica dell'installazione di sistemi di videosorveglianza presso gli asili nido. In tale occasione, la Commissione europea ha precisato che **"l'installazione di sistemi di videosorveglianza per la protezione e la sicurezza di bambini e studenti nei centri per l'infanzia, negli asili nido e nelle scuole può essere un interesse legittimo, purché siano rispettati i principi della protezione dei dati, come i principi di necessità e proporzionalità"** stabiliti a livello nazionale ed europeo e fermo restando il **monitoraggio delle competenti autorità di controllo nazionali della protezione dei dati**". In piena condivisione con questi principi, l'Autorità conclude che la possibilità di installare sistemi di videosorveglianza presso gli asili nido debba essere valutata con estrema cautela, tenendo presenti i

⁸ In "Statuto dei Lavoratori" (L. 300/1970), Titolo I "Della libertà e dignità del lavoratore", art. 4 "Impianti audiovisivi", comma 2: "Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti". L'art. 114 C.P. rubricato "Controllo a distanza" effettua tale richiamo statuendo che: "Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300".

principi generali posti dal Codice, segnatamente, di necessità, proporzionalità, finalità e correttezza del trattamento (artt. 3 e 11), richiamati dalla stessa Autorità anche nel provvedimento dell'8 aprile 2010⁹.

Con specifico riferimento al caso di specie, il Garante rileva che gli scopi che la società ha dichiarato di perseguire con l'implementazione del sistema consistevano nella tutela della sicurezza delle persone e del patrimonio aziendale, nonché nella necessità di soddisfare le "esigenze rappresentate dai genitori". Riguardo alla tutela dell'incolumità fisica dei minori, l'Autorità evidenzia che tale finalità, senz'altro lecita, deve essere assicurata cercando di salvaguardare, al contempo, anche altri interessi fondamentali di costoro, tra i quali quello alla loro riservatezza, soprattutto attraverso il rispetto dei principi di necessità e proporzionalità posti dal Codice. Inoltre, **affinché l'utilizzazione dell'impianto possa ritenersi proporzionata, occorre che presso i luoghi deputati a ricevere i minori sussistano significative situazioni di obiettivo rischio, tali da renderne effettivamente necessaria – e non eccedente - l'installazione**. Ciò premesso, nel caso in questione nessuno dei suddetti elementi risultava provato.

Infatti, né l'asilo ha mai dimostrato che la finalità di garantire la sicurezza dei minori iscritti, nonostante la presenza di altre telecamere presso la struttura, possa essere assicurata solo attraverso l'introduzione di un ulteriore strumento di videosorveglianza, in grado di identificare direttamente ed immediatamente gli interessati anche all'interno della "zona didattica". Né risulta che l'asilo sia ubicato in un contesto ambientale "difficile", mentre le "tradizionali" scelte organizzative adottate per gestire la struttura sino al momento dell'introduzione della *webcam* si sono sempre dimostrate in grado di impedire il verificarsi degli episodi che si intenderebbe scongiurare. Ne consegue, secondo l'Autorità, che l'installazione della *webcam* all'interno dell'area didattica riservata ai minori non solo non può considerarsi necessaria, ma neanche proporzionata. Non solo: la finalità di tutela della sicurezza dei minori non avrebbe comunque richiesto la necessaria implementazione, in favore dei genitori dei minori iscritti, di forme di collegamento via *web* con il sistema, posto che siffatta opportunità, per stessa ammissione della società, non era finalizzata alla tutela della sicurezza dei minori (peraltro, già assicurata dalla presenza di altre telecamere posizionate fuori dell'area didattica), quanto a placare eventuali ansie o a soddisfare semplici curiosità dei genitori. Infine la stessa sicurezza del sistema prospettato risultava dubbia poiché l'utilizzo di collegamenti telematici a vantaggio di terzi non offre garanzie sufficienti per la tutela degli interessati, in quanto la veicolazione continua tramite Internet delle immagini, consultabili in ogni momento da qualsiasi terminale ovunque ubicato, risulta problematica sia perché il sistema non assicura che la loro visione resti circoscritta ai soli soggetti muniti di credenziali sia perché la visione da parte dei genitori/tutori abilitati non è limitata esclusivamente alle attività del proprio figlio, ma si estende anche alla condotta degli altri minori iscritti e dei docenti. Ne derivava, in conclusione, la dichiarazione di illiceità, da parte del Garante, del trattamento delle immagini ed il divieto di prosecuzione dello stesso.

- Provvedimento generale Garante dell'8 aprile 2010 – Argomento: videosorveglianza

In questo provvedimento il Garante sottolinea la necessità che l'eventuale installazione di sistemi di videosorveglianza presso gli istituti scolastici garantisca **"il diritto dello studente alla riservatezza (art. 2, comma 2, D.P.R. n. 249/1998¹⁰), prevedendo opportune cautele al fine di assicurare l'armonico sviluppo delle personalità dei minori in relazione alla loro vita, al loro processo di maturazione ed al loro diritto all'educazione"**. In particolare, si precisa che in tale quadro, è **"ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio ed i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate ed attivando gli impianti negli orari di chiusura degli istituti; vietando, altresì, di attivare le**

⁹ Per il provvedimento generale del Garante dell'8 aprile 2010 vedi *infra* pag. 7.

¹⁰ Per l'art. 2 D.P.R. 249/1998 vedi *supra* nota n. 1, pag. 2.

telecamere in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgano all'interno della scuola". Il mancato rispetto di tali prescrizioni comporta infine l'applicazione di una pesante sanzione amministrativa (pagamento di una somma da trentamila a centottantamila euro così come stabilito dall'art. 162, comma 2-ter, del Codice¹¹).

- Provvedimento Garante del 4 settembre 2009 e newsletter¹² n. 328 del 22 settembre 2009 – Argomento: contro atti vandalici sì a telecamere, ma con limiti precisi

Il Garante privacy, a fronte di una richiesta di verifica preliminare ex art. 17¹³ del Codice, ha dato il via libera all'installazione di un impianto di videosorveglianza presso un istituto scolastico di Verona. Si tratta di un sì condizionato, ma dettato dalla consapevolezza che contro teppismo e atti vandalici nelle scuole le telecamere possono rappresentare un valido strumento di prevenzione e deterrenza. Vanno tuttavia **rispettate precise condizioni a tutela di ragazzi, docenti e personale scolastico. Le telecamere devono riprendere esclusivamente le mura esterne e funzionare solo negli orari di chiusura degli istituti**. Nel caso di specie, l'impianto, sottoposto a verifica preliminare dell'Autorità, si inseriva in un più ampio progetto, denominato "Scuole sicure", messo a punto dalla provincia della città veneta con l'obiettivo di tutelare la sicurezza del patrimonio scolastico e di dissuadere da atti di vandalismo e teppismo. In particolare, il Garante prescrive che: **le telecamere, non inquadrino dettagli dei volti delle persone, siano segnalate da appositi cartelli**, posizionati nelle vicinanze dei luoghi ripresi ed entrino in funzione solo in orari in cui le strutture scolastiche non sono presidiate da personale in servizio (dalle 22,30 alle 6,30). **Le immagini, non visualizzate in tempo reale, devono essere conservate in un server e cancellate dopo 72 ore. Solo in caso di segnalazione di furti, atti di vandalismo o danneggiamenti le immagini vengono messe a disposizione di polizia e autorità giudiziaria**. Considerate le finalità di tutela del patrimonio perseguite dal sistema, l'Autorità ha ritenuto le misure adottate, le modalità di attivazione e le caratteristiche tecniche equilibrate, in linea con i principi affermati dalle norme sulla protezione dei dati personali e conformi con quanto stabilito dal Garante nel sopracitato provvedimento generale in materia di videosorveglianza. Sono tuttavia state prescritte alla Provincia alcune ulteriori misure al fine di assicurare maggiori garanzie per studenti, docenti e personale scolastico ed, in particolare: la limitazione dell'angolo di ripresa delle telecamere ai soli muri perimetrali dell'edificio, con esclusione delle aree esterne circostanti; la visualizzazione delle immagini consentita solo a polizia e autorità giudiziaria; la definizione, in accordo con il dirigente scolastico, degli orari di funzionamento delle telecamere in caso di attività all'interno della scuola che potrebbero iniziare e concludersi in coincidenza con l'orario di attivazione delle telecamere; l'adozione di misure che rendano visibili i cartelli anche di notte. Trattandosi di un progetto che riguardava anche altre scuole della provincia, l'Autorità ha spiegato che, qualora le caratteristiche

¹¹ In Parte III "Tutela dell'interessato e sanzioni", Titolo III "Sanzioni", Capo I "Violazioni amministrative", **art. 162** C.P. "Altre fattispecie": "(...) 2-ter. In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieti di cui all'art. 154 (...), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da 30.000 a 180.000 euro".

¹² Le newsletters e i comunicati stampa hanno valore informativo e divulgativo, nell'esercizio della funzione di cui all'art. 154, comma 1, lett. h) C.P. che assegna al Garante il compito di curare la conoscenza fra il pubblico della disciplina rilevante in materia di trattamento dei dati personali.

¹³ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo I "Regole per tutti i trattamenti" **art. 17** C.P. "Trattamento che presenta rischi specifici": "1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare".

dei sistemi di videosorveglianza da installare corrispondano a quelle autorizzate, non sarà necessario richiedere una ulteriore verifica preliminare.

- Sentenza n. 3134 del 9 novembre 2009 – Tribunale di Monza, Sez. VI – Argomento: videoripresa di un docente con telefono cellulare e diffusione immagini su youtube

Anche il Tribunale Ordinario è stato investito in più occasioni di questioni inerenti le videoriprese. Nel caso di specie, un alunno aveva ritratto per mezzo di un telefono cellulare l'atteggiamento irriverente di alcuni compagni nei confronti della docente durante le ore di lezione della stessa e, dopo avere inserito dei commenti scritti ai filmati, li aveva divulgati tramite internet sul sito *youtube*. Il Tribunale, nell'escludere la responsabilità dell'amministrazione scolastica *ex art. 2048 c.c.*¹⁴ per non avere la stessa docente impedito il fatto - e cioè la videoripresa tramite il telefono cellulare - osservava in primo luogo che gli artt. 10 c.c. e 96 e segg. L. 633/1941¹⁵, vietano la pubblicazione di filmati, senza il consenso della persona ritratta, in quanto tale atto costituisce una violazione del diritto all'immagine, oltre che alla privacy. In secondo luogo l'Organo giudicante rilevava che **"il fatto illecito, imputato al convenuto, non è stato posto in essere durante il tempo in cui l'alunno si trovava sotto la sorveglianza della professoressa, in quanto la semplice registrazione di immagini, con il telefono cellulare, non costituisce un illecito. Il fatto illecito, che ha causato danno, è invece l'aver reso pubbliche tali immagini su internet e tale evento è avvenuto in un momento successivo, quando il convenuto non si trovava più sotto il controllo dell'attrice"**. Sulla base di tali principi i genitori esercenti la patria potestà venivano quindi condannati al risarcimento del danno a favore della professoressa.

- Direttiva ministeriale n. 104 del 30 novembre 2007 – Argomento: uso dei telefoni cellulari

La sentenza sopracitata offre lo spunto per richiamare la direttiva ministeriale di cui in epigrafe con la quale il M.I.U.R. ha dettato linee di indirizzo e chiarimenti interpretativi ed applicativi anche in ordine alla normativa posta a tutela della privacy in materia di utilizzo di telefoni cellulari e di altri dispositivi elettronici durante l'attività didattica, richiamando l'attenzione delle scuole sulla corresponsabilità dei genitori.

In particolare, il Garante evidenzia l'importanza di distinguere due diverse situazioni giuridiche: da un lato, l'ipotesi che l'acquisizione dei dati personali sia finalizzata ad una successiva divulgazione verso terzi, dall'altro che avvenga esclusivamente per un uso personale.

In ogni caso, il Garante enuncia specifiche cautele di carattere generale: **chi utilizza i dati personali raccolti (immagini, filmati, registrazioni vocali, ecc...) indipendentemente dal fatto che lo faccia per fini personali o per diffonderli, deve, anche successivamente, rispettare gli specifici obblighi previsti a tutela dei terzi dalla comune disciplina in campo civile e penale.** Infatti, **anche nel caso di uso dei dati per fini esclusivamente personali, la raccolta, la comunicazione e l'eventuale diffusione di immagini e suoni deve avere comunque luogo nel rispetto dei diritti e delle libertà fondamentali degli interessati, utilizzando l'immagine altrui nei modi e nei casi consentiti dall'ordinamento.** Il riferimento è, nella fattispecie, all'art. 10 c.c.,

¹⁴ L'art. 2048 c.c. rubricato "Responsabilità dei genitori, dei tutori, dei precettori e dei maestri d'arte" dispone che: "Il padre e la madre, o il tutore, sono responsabili del danno cagionato dal fatto illecito dei figli minori non emancipati o delle persone soggette alla tutela, che abitano con essi. La stessa disposizione si applica all'affiliante. I precettori e coloro che insegnano un mestiere o un'arte sono responsabili del danno cagionato dal fatto illecito dei loro allievi e apprendisti nel tempo in cui sono sotto la loro vigilanza. Le persone indicate dai commi precedenti sono liberate dalla responsabilità soltanto se provano di non avere potuto impedire il fatto".

La responsabilità genitoriale di cui all'art. 2048 c.c. sarà richiamata anche *infra* alla nota n. 78, pag. 36, alla nota n. 86 pag. 40 e alle pagine 40, 46 e 49.

¹⁵ Per l'art. 10 c.c. vedi *infra* nota n. 16 e per gli artt. 96 e 97 L. 633/1941 vedi nota n. 17, pag. 10.

rubricato “*Abuso dell’immagine altrui*”¹⁶; agli artt. 96 e 97 L. 633/1941 sul diritto d’autore, sezione II “*Diritti relativi al ritratto*”¹⁷ che prevedono una serie di garanzie per l’esposizione, la riproduzione e la messa in commercio non consensuali del ritratto di una persona, salvo la sua notorietà; ai generici obblighi del *neminem laedere* di cui all’art. 2043 c.c. che prevede altri divieti sanzionati penalmente¹⁸.

In conclusione, **chi utilizza dati personali (immagini, filmati, registrazioni vocali,...), raccolti con il proprio cellulare o altri dispositivi, deve vagliare tutte queste circostanze e porre attenzione a che i propri comportamenti non ledano i diritti dei terzi, ad esempio evitando di riprendere persone in atteggiamenti o situazioni che possano lederne la dignità o astenendosi dal divulgare immagini, anche occasionalmente, ad un numero elevato di soggetti senza che la persona fotografata o filmata ne sia a conoscenza e possa attivarsi al fine di tutelare la propria sfera privata.** Ancor più delicata è l’ipotesi in cui i dati personali siano acquisiti per una divulgazione verso terzi. Come è noto, i moderni telefoni cellulari, così come altri dispositivi elettronici, consentono facilmente, ed in ogni momento, agli utenti di scattare fotografie o registrare suoni o filmati, riconducibili a delle persone fisiche. Tali strumenti consentono anche l’invio ad altre persone di fotografie o registrazioni nonché la possibilità di utilizzare i suddetti dati per la pubblicazione su siti internet. Di fronte a queste opportunità fornite dall’utilizzo delle nuove tecnologie, il Garante chiarisce che **“la diffusione di dati personali di questo genere, ai sensi della normativa vigente, non può avvenire sulla base della libera volontà di chi li ha acquisiti,** in quanto ciascuna persona è titolare del diritto alla protezione dei dati personali. Di conseguenza, **la diffusione o la comunicazione** in via sistematica di dati personali, specie se ad una pluralità di destinatari, **può avvenire soltanto dopo che la persona interessata sia stata debitamente informata in ordine alle successive modalità di utilizzo dei dati,** con particolare riferimento all’eventualità che i dati siano diffusi o comunicati sistematicamente, **ed abbia manifestato il suo consenso** (ai sensi degli artt. 13¹⁹ e 23²⁰ del predetto Codice). Nel caso di dati sensibili il consenso dovrà essere espresso in forma scritta, fermo restando comunque il divieto di divulgare dati sulla salute”.

Tali regole di carattere generale valgono anche nell’ambito delle comunità scolastiche nelle quali assume un particolare significato culturale nei confronti dei giovani l’esigenza di assicurare la conoscenza ed il rispetto delle norme poste a tutela dei diritti dei singoli. In pratica, gli studenti, i docenti o altri soggetti della comunità scolastica che vorranno scattare fotografie o effettuare registrazioni audio o video all’interno delle istituzioni scolastiche, con il proprio telefono cellulare o altri dispositivi, e successivamente utilizzare, divulgare, inviare i dati personali acquisiti sono obbligati - oltre ad acquisire il consenso espresso dell’interessato (scritto se i dati sono sensibili) – ad informare la persona interessata circa le finalità e le modalità del trattamento, circa i diritti di cui

¹⁶ L’art. 10 c.c. dispone che: “Qualora l’immagine di una persona o dei genitori, del coniuge o dei figli sia stata esposta o pubblicata fuori dei casi in cui l’esposizione o la pubblicazione è dalla legge consentita, ovvero con pregiudizio al decoro o alla reputazione della persona stessa o dei detti congiunti, l’autorità giudiziaria, su richiesta dell’interessato, può disporre che cessi l’abuso, salvo il risarcimento dei danni”.

¹⁷ A mente dell’art. 96 L. 633/1941 “Il ritratto di una persona non può essere esposto, riprodotto o messo in commercio senza il consenso di questa (...)”; l’art. 97 dispone invece che: “Non occorre il consenso della persona ritrattata quando la riproduzione dell’immagine è giustificata dalla notorietà o dall’ufficio pubblico coperto, da necessità di giustizia o di polizia, da scopi scientifici, didattici o culturali, o quando la riproduzione è collegata a fatti, avvenimenti, cerimonie di interesse pubblico o svoltisi in pubblico. Il ritratto non può tuttavia essere esposto o messo in commercio, quando l’esposizione o messa in commercio rechi pregiudizio all’onore, alla reputazione od anche al decoro della persona ritrattata”.

¹⁸ Il riferimento è, in particolare, all’indebita raccolta, rivelazione e diffusione di immagini attinenti alla vita privata che si svolgono in abitazioni altrui o in altri luoghi di privata dimora (art. 615 bis c.p.); al possibile reato di ingiuria, in caso di particolari messaggi inviati per offendere l’onore o il decoro del destinatario (art. 594 c.p.); alle pubblicazioni oscene (art. 528 c.p.); alla tutela dei minori riguardo al materiale pornografico (art. 600 ter c.p. e L. 269/1998).

¹⁹ Per l’art. 13 C.P. vedi *supra* nota n. 7, pag. 5.

²⁰ Per l’art. 23 C.P. vedi *infra* nota n. 77, pag. 35.

è titolare *ex art. 7 C.P.*²¹ (es. diritto di ottenere la cancellazione o la trasformazione in forma anonima dei dati personali) e a fornire gli estremi identificativi di colui che usa il telefono cellulare o altri dispositivi per raccogliere i dati²².

Nel caso in cui, invece, l'acquisizione mediante telefonino avvenga per fini esclusivamente personali non operano gli obblighi di informativa ed acquisizione del consenso, salvo che le informazioni raccolte non siano invece destinate ad una comunicazione sistematica o alla diffusione. Ad esempio nel caso dello scatto di una fotografia e del suo invio occasionale ad amici o familiari, il soggetto agente soddisfa esclusivamente esigenze di carattere strettamente personale (culturali, di svago o di altro genere) e, restando le immagini in un ambito circoscritto di conoscibilità, non operano gli obblighi di informativa e di acquisizione del consenso. Gli obblighi in questione risultano, al contrario, applicabili nel diverso caso in cui, benché per scopi anche semplicemente culturali o informativi, l'immagine sia raccolta per essere diffusa in Internet o comunicata sistematicamente a terzi. Tra queste due ipotesi, come ha chiarito il Garante, vi possono essere peraltro situazioni-limite alle quali va posta particolare attenzione e che vanno esaminate caso per caso. Si pensi all'ipotesi in cui i dati personali (immagini, filmati, registrazioni vocali,...) siano inviati tramite *app* di messaggistica istantanea con una sola comunicazione a terzi diretta, però, ad un numero assai ampio di destinatari: in questo caso, a livello pratico, l'invio pur occasionale dell'immagine avviene con caratteristiche tali da dar vita ad una comunicazione a catena di dati. Ne segue, in conclusione, che **anche l'utilizzo di immagini, filmati o registrazioni vocali per fini esclusivamente personali deve rispettare comunque l'obbligo di mantenere sicure le informazioni raccolte, tenendo conto che il rispetto dei diritti, delle libertà fondamentali e della dignità dei terzi interessati è sotteso anche a questi trattamenti e che, se si cagiona a terzi un eventuale danno anche non patrimoniale, colui che utilizza in modo improprio le immagini o altri dati personali, raccolti con il cellulare o con analogo dispositivo elettronico, deve risarcirlo se non prova di aver adottato tutte le misure idonee ad evitarlo.**

Alla luce di questi principi, occorre quindi analizzare quale possa essere il tenore dei regolamenti di istituto e le possibili sanzioni disciplinari per il mancato rispetto degli obblighi sopra enunciati. Per gli studenti che violano l'onere di preventiva informativa è innanzitutto prevista una sanzione

²¹ In Parte I "Disposizioni generali", Titolo II "Diritti dell'interessato", **art. 7 C.P.** "Diritto di accesso ai dati personali ed altri diritti": "1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

- a) dell'origine dei dati personali;
- b) delle finalità e modalità del trattamento;
- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

- a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

- a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale".

²² L'inosservanza dell'obbligo di preventiva informativa all'interessato comporta il pagamento di una sanzione amministrativa che va da 6.000 a 36.000 euro (cfr. **art. 161 C.P.**).

amministrativa della cui applicazione è competente il Garante. Ma, ancora prima, a monte, è auspicabile che **le istituzioni scolastiche disciplinino - nell'ambito dei regolamenti di istituto - i comportamenti connessi ad un trattamento improprio di dati personali acquisiti mediante telefoni cellulari o altri dispositivi elettronici, sanzionandoli con opportuno rigore e severità** in coerenza con quanto previsto agli artt. 3 e 4, D.P.R. 249/1998 – “Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria”²³.

Le scuole sono dunque tenute a conformare i propri regolamenti secondo i chiarimenti illustrati dal Garante, individuando, nell'ambito della propria autonomia, le sanzioni più appropriate da irrogare nei confronti degli studenti che violano il diritto alla protezione dei dati personali all'interno delle comunità scolastiche. In particolare, nell'ambito della propria autonomia, esse potranno, nei propri regolamenti, inibire, in tutto o in parte, o sottoporre opportunamente a determinate cautele, l'utilizzo di videotelefoni e di app di messaggistica istantanea all'interno delle scuole stesse e nelle aule di lezione. L'istituzione scolastica ha infatti il potere di dettare delle apposite disposizioni organizzative interne all'istituto volte a disciplinare l'utilizzo di *app* di messaggistica istantanea da parte degli studenti, ad esempio vietando l'utilizzo delle fotocamere, delle videocamere o dei registratori vocali, inseriti all'interno di telefoni cellulari o di altri dispositivi elettronici, in assenza di un esplicito consenso manifestato dall'interessato. La violazione di tali regole contenute nei regolamenti di istituto potrà dunque configurare un'infrazione disciplinare, con conseguente applicazione della relativa sanzione individuabile dalla scuola stessa²⁴.

- **Comunicato stampa²⁵ Garante del 6 giugno 2007 (e newsletter n. 195 dell'8-21 dicembre 2003)**
- **Argomento: i genitori possono filmare e fotografare i figli nelle recite scolastiche. Non è una questione di privacy: i divieti sono infondati**

Il Garante ribadisce che **le riprese video e le fotografie raccolte dai genitori, durante recite e saggi scolastici, non violano la privacy.** Si tratta, infatti, di **immagini non destinate a diffusione, ma raccolte per fini personali e destinate ad un ambito familiare o amicale**: il loro uso è quindi del tutto legittimo e non ha niente a che fare con le norme sulla privacy. L'Autorità si era già pronunciata negli stessi termini alcuni anni prima, interpellata a seguito di diverse segnalazioni: il chiarimento si era reso necessario per l'illegittimo divieto, sancito da diverse scuole, a genitori e familiari di fare riprese e foto dei propri bambini in occasione di recite e saggi scolastici.

- **Intervista a Giovanni Buttarelli, Segretario generale del Garante per la protezione dei dati personali del 26 maggio 2006 – Argomenti: foto di classe; pubblicazione di fotografie sul giornalino o sul sito web della scuola; polizze integrative e facoltative a beneficio degli alunni; trattamento dei dati sensibili**

L'intervista viene effettuata per rispondere ad un lettore di un quotidiano locale che segnala, in una lettera pubblicata sul rotocalco, che la scuola della figlia, insegnante elementare, ha così disposto:

²³ Si veda in particolare il comma 4 dell'**art. 3** del **D.P.R. 249/1998** a mente del quale: “*Gli studenti sono tenuti ad osservare le disposizioni organizzative e di sicurezza dettate dai regolamenti dei singoli istituti*” e, soprattutto, il 1° comma dell'**art. 4** che dispone espressamente che “*I regolamenti delle singole istituzioni scolastiche individuano i comportamenti che configurano mancanze disciplinari con riferimento ai doveri elencati nell'articolo 3, al corretto svolgimento dei rapporti all'interno della comunità scolastica e alle situazioni specifiche di ogni singola scuola, le relative sanzioni, gli organi competenti ad irrogarle e il relativo procedimento (...)*”.

²⁴ In considerazione della vasta rilevanza sociale che ha assunto il fenomeno dell'utilizzo dei telefoni cellulari per l'acquisizione ed il trattamento di dati personali nell'ambito delle scuole italiane, è particolarmente auspicabile l'adozione delle misure sopra indicate unitamente all'individuazione di spazi di riflessione e di studio in ordine alle problematiche oggetto della presente direttiva al fine di **favorire tra i giovani la consapevolezza dell'importanza del diritto alla protezione dei dati personali nell'ordinamento vigente nell'ottica di diffondere la cultura della legalità.**

²⁵ Per la definizione di un comunicato stampa vedi *supra* nota n. 12, pag. 8.

“quest’anno, per disposizione del ministero e al fine di tutelare la privacy, non si faranno le tradizionali foto di classe. Stesso provvedimento durante i giochi della gioventù di fine anno”. Seguono lamentele circa l’eccesso di zelo e la bizzarria della decisione. Il Garante smentisce chiarendo che **l’uso di videocamere o macchine fotografiche per documentare eventi scolastici o conservare ricordi dei propri figli non ha niente a che fare con le norme sulla privacy. Si tratta, infatti, di immagini raccolte per fini personali e destinate a un ambito familiare o amicale: il loro uso quindi è del tutto legittimo.**

Effettivamente molte scuole stanno cessando la consuetudine delle foto di classe: sono spaventate da possibili (e ingiustificate) violazioni della privacy, o dall’idea di dover produrre alcune centinaia di documenti contenenti richieste di consenso al solo fine di tenere in vita questa tradizione. In merito, il Segretario Buttarelli distingue tra scuole private e pubbliche: le prime hanno fattispecie per le quali devono richiedere il consenso, mentre **le scuole statali, in quanto enti pubblici operanti per fini istituzionali, che sono quelli di educazione e formazione degli allievi, non hanno obblighi di richiesta di consenso.** Tra l’altro, precisa, la questione del consenso informato all’interno delle scuole è mal posta: o le scuole effettuano dei trattamenti consentiti, oppure no. Nel secondo caso, i trattamenti sono semplicemente illeciti, e nessun consenso può mai sanarli, rendendoli leciti. Quanto alle foto di classe, il Garante ribadisce la piena ammissibilità di riprese video e fotografie raccolte dai genitori, durante recite e saggi scolastici. Quindi i timori sono del tutto ingiustificati.

Nell’intervista viene sollevato anche un altro problema: occorre che la scuola richieda garanzie di sicurezza al fotografo circa la conservazione delle fotografie? La risposta è negativa, precisando che il fotografo è legittimato a conservare i negativi ai sensi della legislazione sulla tutela del diritto d’autore.

La questione delle riproduzioni fotografiche investe anche altre questioni delle attività scolastiche. I capi d’istituto chiedono ragguagli sulla possibilità di pubblicare fotografie degli studenti e del personale sui giornali di istituto e sul sito *web* della scuola. Il Garante risponde che per dare una soluzione certa, **bisogna esaminare la finalità della pubblicazione di una fotografia sul giornalino o sul sito. In linea di massima però non vi sono particolari obblighi cui sottostare: le scuole pubblicano fotografie sul giornalino e sul sito per pubblicizzare le attività dell’istituto, dare una visibilità educativa agli alunni delle classi, indicare il vincitore di una gara o di un concorso che dà lustro alla scuola. In tutti questi casi, il trattamento è legittimo. Per la pubblicazione sul sito web, si può adottare la soluzione "creativa" di considerare il sito web come il giornale on line della scuola, con piena facoltà di pubblicazione delle foto.**

Vengono affrontati anche altri casi critici: la maggior parte delle scuole sottoscrive una polizza integrativa e facoltativa a beneficio degli alunni, nel caso in cui questi si facciano male. Essendo una procedura non necessaria, c’è chi valuta come opportuna in questo caso, e solo in questo caso, la richiesta di consenso informato ai genitori. Chiara la risposta del Garante: il fatto che certi atti siano facoltativi non vuol dire affatto che non facciano parte dei compiti istituzionali della scuola. Quindi anche **nel caso di sottoscrizione di una polizza integrativa e facoltativa a beneficio degli alunni, mancano i requisiti per una richiesta di consenso.** Il problema, però, puntualizzano le scuole, si crea quando lo studente subisce un infortunio: per la richiesta di risarcimento del danno, occorre che la scuola comunichi diagnosi e prognosi dell’infortunato alla compagnia assicurativa, ma non può farlo, perché l’ente pubblico non può trasmettere dati sensibili, in assenza di norma o regolamento. Come è opportuno comportarsi? Il Segretario Buttarelli propone due soluzioni: o far trasmettere diagnosi e prognosi degli studenti direttamente dai genitori all’assicurazione oppure i genitori possono consegnare in busta chiusa i referti medici degli studenti infortunati alle scuole, le quali li trasmetteranno direttamente alle compagnie, senza visionarli.

Un’ultima questione riguarda la **difficoltà delle scuole a trattare dati sensibili “con tecniche di cifratura o mediante l’utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità”.**

Come si devono comportare le scuole che in genere utilizzano *software* di trattamento dati standardizzati, che spesso non consentono la temporanea cifratura dei dati? Anche in questo caso il Garante invita ad essere creativi, facendo rientrare tra le “altre soluzioni” **ad esempio la creazione di un piccolo foglio di calcolo accessorio che separi i dati oggetto di trattamento da quelli sensibili, non oggetto di trattamento e temporaneamente invisibili**. I dati oggetto di trattamento possono essere riversati nella banca dati in un momento successivo, a cura del personale abilitato alla conoscenza di quei dati sensibili.

- Provvedimento generale Garante del 20 gennaio 2005²⁶ – Argomento: videofonini, cautele per un uso legittimo

Il provvedimento riguarda i trattamenti di dati personali effettuati mediante apparecchi di telefonia dotati di videocamere. Il Garante evidenzia che i terminali di nuova generazione applicati alla telefonia mobile consentono con crescente facilità di registrare fotografie e filmati tramite diverse tecnologie di rete, comunicando e diffondendo immagini e suoni in tempo reale.

Si tratta di apparecchiature impiegate per lo più per applicazioni lecite nell’ordinaria vita di relazione interpersonale, ma che, per le loro potenzialità, possono essere utilizzate violando, anche involontariamente, i diritti delle persone interessate dalla comunicazione, come pure di terzi inconsapevoli della ripresa. Si pongono problemi analoghi a quelli dei telefoni dotati di fotocamera e abilitati all’invio di messaggi del tipo *mms* o attraverso *app* di messaggistica istantanea. Rispetto a questi apparecchi, però, gli *smartphone* sono dotati anche di videocamere di dimensioni assai ridotte, orientabili in vario modo sull’apparecchio e dotate di diverse funzioni, anche di ingrandimento di immagini. Attraverso tali videocamere si possono effettuare riprese prima e durante una conversazione, caratterizzate da un grado crescente di risoluzione e realizzabili anche clandestinamente, grazie alla frequente assenza nell’apparecchio di segnali luminosi o acustici che segnalino a terzi la ripresa in atto. È possibile raccogliere immagini e suoni anche nel corso di una chiamata e trasmettere immagini relative al chiamante, al chiamato e a ciò che si svolge attorno a loro. Si tratta – precisa il Garante - di un uso ulteriore rispetto all’utilizzazione ordinaria del mezzo telefonico volta a veicolare voci e testi tra due o più soggetti, risultando assai agevole raccogliere, archiviare, condividere con terzi immagini e suoni anche in rete e diffonderli in tempo reale attraverso strumenti informatici, telematici e televisivi. Anche rispetto a fotocamere e videocamere digitali il collegamento diretto con lo strumento telefonico rappresenta un elemento distintivo di rilievo. Ne segue, come evidenzia il Garante, che **tali tecnologie possono essere impiegate anche per usi invasivi - in luoghi pubblici, aperti al pubblico e privati - della sfera privata e lesivi di altri diritti e libertà fondamentali, tra cui spicca la libertà di conversare e di comunicare in assenza di molestie ed intercettazioni indebite**.

Il Garante interviene in argomento perché le immagini e i suoni realizzati con videocamere possono contenere “dati personali” relativi al chiamante, al chiamato o a terzi, che in alcuni casi possono essere anche “sensibili” riguardando lo stato di salute, la sfera politica, religiosa o sindacale o le abitudini sessuali. Inoltre, la veicolazione di immagini e suoni può arrecare maggiori fastidi agli interessati nella ricezione di comunicazioni indesiderate o di disturbo.

Nel provvedimento si distingue tra videochiamate per fini esclusivamente personali e usi ai quali è applicabile il Codice. Nel primo caso, se i dati non sono diffusi o comunicati sistematicamente a terzi, il complesso normativo del Codice in materia di protezione dei dati non è applicabile. Ciò non significa che chi utilizza l’apparecchio non debba tener conto dei diritti dei terzi: l’utente deve infatti rispettare almeno alcuni obblighi di sicurezza (art. 31 del Codice²⁷), deve risarcire i

²⁶ Il provvedimento in questione è stato emesso in base all’**art. 154**, comma 1, lettera c) del Codice e prevede la segnalazione d’ufficio ai titolari del trattamento (nel caso coloro che utilizzano lo *smartphone*) delle misure indicate ritenute necessarie al fine di rendere il trattamento conforme alle disposizioni del Codice.

²⁷ In Parte I “*Disposizioni generali*”, Titolo V “*Sicurezza dei dati e dei sistemi*”, Capo I “*Misure di sicurezza*”, **art. 31** C.P. “*Obblighi di sicurezza*” : “*I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione*

danni anche morali eventualmente cagionati a terzi (art. 15 del Codice²⁸) e non deve ledere i diritti che gli interessati hanno soprattutto per ciò che riguarda il diritto alla riservatezza, all'immagine e al ritratto. Nel secondo caso, il Garante considera, invece, l'ipotesi che le immagini e i suoni, benché ripresi per uso personale, possano riguardare terzi ed essere comunicati sistematicamente o diffusi tramite Internet o un sito *web* personale. In tali casi il trattamento dei dati personali, che si concreta già al momento della sola raccolta (art. 4, comma 1, lett. a), del Codice²⁹), è lecito unicamente se sono rispettate tutte le disposizioni applicabili del predetto Codice. Ciò comporta, quindi, il dovere di informare preventivamente gli interessati (art. 13 del Codice³⁰), di raccogliere il loro consenso libero, preventivo e informato (che deve essere manifestato per iscritto se i dati sono sensibili) e di osservare tutte le altre ordinarie cautele previste, ad esempio, in tema di requisiti dei dati (art. 11 del Codice³¹). L'informativa e il consenso riguardano non solo le persone in conversazione telefonica, ma anche gli eventuali terzi identificati o identificabili, nonché l'obbligo per l'utente di informare l'altro utente quando, nel corso della conversazione, è consentito l'ascolto della conversazione stessa da parte di altri soggetti. Il Garante richiama poi l'attenzione sull'eventualità che in determinati uffici pubblici, luoghi pubblici e privati o aperti al pubblico, l'uso di videotelefonii sia inibito in tutto o in parte. Si tratta di limiti e cautele (in alcuni Paesi introdotti anche con apposite norme legislative) che possono essere prescritti legittimamente da soggetti pubblici e privati e che condizionano, in tal caso, la liceità e la correttezza del trattamento dei dati: l'utilizzo delle immagini e dei suoni raccolti in violazione di tali prescrizioni non può infatti considerarsi lecito o corretto (art. 11, comma 1, lett. a), del Codice³²). In altri casi, invece, si evidenzia l'eventualità che i detentori di telefonini abilitati partecipino a cosiddette "comunità virtuali" di persone che possono essere contattate consensualmente con videochiamate da parte di utenti di siti *web* che mettono a disposizione appositi spazi sulla rete. In tal caso, i fornitori di tali servizi devono informare compiutamente anche *on line* gli utenti che intendono accedere al servizio, in modo che risulti chiaro, in particolare, l'ambito di conoscibilità dei dati registrati (ad esempio, il fatto che possono

alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".

²⁸ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo I "Regole per tutti i trattamenti", **art. 15** C.P. "Danni cagionati per effetto del trattamento": "1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile (...)". Tale articolo dispone che: "Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno".

²⁹ In Parte I "Disposizioni generali", Titolo I "Principi generali", **art. 4** C.P. "Definizioni": "Ai fini del presente codice si intende per: a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati (...)".

³⁰ Per l'**art. 13** C.P. vedi *supra* nota n. 7, pag. 5.

³¹ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo I "Regole per tutti i trattamenti", **art. 11** C.P. "Modalità del trattamento e requisiti dei dati": "1. I dati personali oggetto di trattamento sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
- c) esatti e, se necessario, aggiornati;
- d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
- e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati".

³² Per l'**art. 11** C.P. vedi subito *supra* nota n. 31.

accedervi solo gli altri soggetti registrati e muniti di particolari codici personali). I fornitori dovranno poi conservare i dati raccolti esclusivamente per il periodo di tempo strettamente necessario alla fornitura del servizio, prestando particolare attenzione ai profili di sicurezza e alla gestione dei suddetti codici personali di accesso (art. 31 e ss. del Codice³³).

PARTE II

Privacy e trasparenza sul web - Informazioni e dati relativi agli studenti e alle loro famiglie

Quadro sintetico

Il delicato rapporto tra privacy e trasparenza sul *web* ha formato oggetto delle recenti **“Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati”** del 15 maggio 2014, adottate ai sensi dell’art. 154, comma 1, lett. h) del Codice Privacy³⁴. Tale documento, sostituendo le precedenti Linee guida del 2 marzo 2011, recepisce le prescrizioni contenute nel recente **d. lgs. 14 marzo 2013, n. 33**³⁵ recante **“Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni”**. In sostanza sono previste tutta una serie di misure e cautele cui le Pubbliche Amministrazioni debbono attenersi al fine di contemperare, anche sul *web*, le esigenze di pubblicità per finalità di trasparenza o per altre finalità con quelle di privacy.

Le istituzioni scolastiche hanno innanzi tutto l’obbligo di rendere noti a studenti e famiglie i **dati personali degli studenti minorenni** che raccolgono e le relative modalità di trattamento che devono limitarsi al perseguimento delle sole finalità istituzionali³⁶. Anche in ambito scolastico, infatti, ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di apprenderne il contenuto, di farle rettificare se erranee, incomplete o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al “titolare del trattamento” (la scuola) anche tramite suoi incaricati o responsabili. Se non si ottiene risposta, o se il riscontro non è sufficiente, è possibile rivolgersi alla magistratura ordinaria o al Garante.

I **dati sensibili e giudiziari** devono poi essere trattati con estrema cautela, verificandone non solo la pertinenza e completezza, ma anche l’indispensabilità rispetto alle “rilevanti finalità pubbliche” che si intendono perseguire.

In particolare, i **dati sulle origini etniche** possono essere trattati dalla scuola per favorire l’inclusione degli alunni stranieri; i **dati sulle convinzioni religiose** per garantire la libertà di credo - che potrebbe richiedere particolari misure per la gestione della mensa scolastica - e per la fruizione dell’insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

³³ Per l’art. 31 C.P. vedi *supra* nota n. 27, pag. 14.

³⁴ In Parte III “Tutela dell’interessato e sanzioni”, Titolo II “L’Autorità”, Capo I “Il Garante per la protezione dei dati personali”, art. 154 C.P. “Compiti”: “1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell’Ufficio e in conformità al presente codice, ha il compito di: (...) h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati”.

³⁵ Per un’analisi più dettagliata del d.lgs. 33/2013 vedi *infra* pagg. 18, 21 e 52 e ss.

³⁶ Si consideri in merito il disposto dell’art. 18 C.P. “Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici”, comma 2: “Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali” e comma 4: “Salvo quanto previsto (...) per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell’interessato”.

I **dati idonei a rivelare lo stato di salute** sono classificabili dal punto di vista amministrativo come “supersensibili” e possono essere trattati per l’assegnazione del sostegno agli alunni con disabilità, per la composizione delle classi, per la gestione delle assenze per malattia, per l’insegnamento domiciliare e ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione. Le **opinioni politiche** possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza, quali le consulte e le associazioni degli studenti e dei genitori. Infine, i **dati di carattere giudiziario** possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione, nonché per le attività connesse ai contenziosi con gli alunni e con le famiglie e per tutte le attività di difesa in giudizio delle istituzioni scolastiche.

Occorre precisare che le **scuole pubbliche** non sono tenute a chiedere il consenso³⁷ per il trattamento dei dati personali degli studenti per finalità istituzionali. Le **scuole private**, invece, sono obbligate non solo a presentare un’informativa completa, ma anche a ottenere il consenso puntuale e liberamente espresso dei soggetti interessati (studenti maggiorenni, famiglie...). Nel caso di trattamento di dati giudiziari e sensibili, gli istituti privati sono tenuti a rispettare anche le prescrizioni contenute nelle autorizzazioni generali del Garante, le quali esplicitano i trattamenti consentiti.

Non commette violazione della privacy l’insegnante che assegna ai propri alunni lo svolgimento di **temi in classe** riguardanti il loro mondo personale o familiare. Nel momento in cui gli elaborati vengono letti in classe – specialmente se sono presenti argomenti delicati - è affidata alla sensibilità di ciascun insegnante la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo al segreto d’ufficio e professionale, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

Non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato, perché le **informazioni sul rendimento scolastico** sono soggette a un regime di trasparenza. Il regime attuale relativo alla conoscibilità dei risultati degli esami di maturità è stabilito dal Ministero dell’Istruzione. Per il principio di trasparenza a garanzia di ciascuno, i voti degli scrutini e degli esami devono essere pubblicati nell’albo degli istituti. È necessario prestare attenzione, però, a non fornire – anche indirettamente – informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti. Ad esempio, il riferimento alle “prove differenziate” sostenute dagli studenti con disabilità non va inserito nei tabelloni affissi all’albo dell’istituto, ma deve essere indicato solamente nell’attestazione da rilasciare allo studente.

Si tenga presente poi che su richiesta degli studenti interessati le scuole possono comunicare, anche a privati e per via telematica, i dati relativi ai loro risultati scolastici per aiutarli nell’**orientamento**, la **formazione** e l’**inserimento professionale** anche all’estero.

³⁷ Si consideri in merito il già citato disposto dell’**art. 18 C.P.** “*Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici*”, comma 4: “*Salvo quanto previsto (...) per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell’interessato*”.

Approfondimento: casi pratici e normativa di riferimento

- Seminario di formazione presso il Garante per la protezione dei dati personali del 15 ottobre 2014 – Argomento: trasparenza e protezione dei dati personali

Si ritiene opportuno far cenno agli argomenti e alle considerazioni emersi nel corso di tale recentissimo seminario al fine di comprendere quale sia l'attuale stato dell'arte in merito.

In particolare, si chiarisce che per **trasparenza amministrativa** si intende la pubblicità di atti, documenti, informazioni e dati propri di ogni amministrazione, resa possibile grazie alla circolazione delle informazioni sulla rete internet a partire dalla pubblicazione sui siti istituzionali delle amministrazioni. E' il **D.lgs. 14 marzo 2013, n. 33 (cd. decreto trasparenza)**, che, adottato a seguito della delega contenuta nella L. 6 novembre 2012, n. 190 (cd. legge anticorruzione), ha riordinato – anche innovandola – la normativa esistente fornendo così una disciplina unitaria della trasparenza amministrativa, precisando in particolare: obblighi di pubblicazione in capo alle amministrazioni; diritti e strumenti per la conoscibilità in capo ai cittadini; regole e limiti a casi e forme di pubblicità; previsioni specifiche per alcuni settori; un annesso apparato di vigilanza e sanzioni.

- Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali del 23 giugno 2014 – Argomento: protezione dei dati

Si ritiene opportuno riportare alcune parti dell'intervista rilasciata di recente dal Presidente dell'Autorità Garante per la privacy Antonello Soro, proprio in vista del semestre italiano di presidenza del Consiglio dell'Unione europea. Soro sottolinea che *“la protezione dei dati non è una disciplina come le altre perché nella società digitale rappresenta forse l'unica misura etica, in quanto è in grado di combinare insieme diritti e tecnologie”*. Alla domanda sul perché il nostro governo dovrebbe spingere in sede UE sulla protezione dei dati, Soro risponde che: *“si è messo in moto un processo di cambiamento e di rinnovata attenzione alla protezione dei dati che vede impegnati tre grandi protagonisti. È in movimento la giurisprudenza europea che ha prodotto sentenze importanti, come quando l'8 aprile la Corte di giustizia Ue ha dichiarato illegittima la direttiva sulla data retention per violazione del principio di proporzionalità nel rapporto tra privacy e sicurezza”³⁸. O come l'altra sentenza³⁹ pronunciata dalla Corte il 13 maggio contro*

³⁸ Trattasi della sentenza della Corte di giustizia dell'8 aprile 2014, nota come **“sentenza sulla data retention”** con la quale la Corte di Giustizia ha dichiarato l'illegittimità della direttiva Frattini (2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE) per violazione del principio di proporzionalità nel bilanciamento tra diritto alla protezione dei dati personali ed esigenze di pubblica sicurezza. All'attenzione della Corte erano, appunto, le disposizioni della direttiva volte a garantire la conservazione dei dati di traffico telefonico e telematico, i dati relativi all'ubicazione e quelli necessari all'identificazione dell'abbonato, per fini di accertamento e repressione dei reati. Come rileva la Corte, si tratta di dati che, pur non attingendo al contenuto della conversazione, forniscono comunque indicazioni importanti sulle comunicazioni intrattenute da ciascuno, sui loro destinatari e sulla loro frequenza. L'accesso a tali dati, da parte dell'autorità pubblica, comporta dunque - ribadisce la Corte - una forte ingerenza nella vita privata dei cittadini, ingenerando peraltro in loro l'idea di essere esposti a una “costante sorveglianza” in quanto la conservazione e il successivo utilizzo dei dati stessi avviene a insaputa dell'interessato. Se, in linea generale, l'accesso a tali dati può giustificarsi in ragione di un obiettivo d'interesse generale quale, appunto, il contrasto a gravi forme di criminalità e, in definitiva, le esigenze di pubblica sicurezza, la direttiva avrebbe, secondo la Corte, ecceduto i limiti imposti dal principio di (stretta) proporzionalità. Limiti, questi, da valutare secondo uno scrutinio particolarmente rigoroso in ragione della rilevanza del diritto fondamentale alla protezione dei dati personali, che in tal modo viene compresso.

La violazione del principio di proporzionalità deriverebbe, secondo la Corte, dall'aver la direttiva: 1) previsto le misure di conservazione dei dati come applicabili in via indifferenziata e generalizzata “all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi”; 2) omissso di prevedere alcun criterio

Google⁴⁰, cruciale non solo per il diritto all'oblio sul web ma in quanto definisce la giurisdizione europea su comportamenti e atti di aziende che hanno sede negli Usa. Al contempo, dopo il Datagate⁴¹, sta crescendo la consapevolezza e anche l'allarme nell'opinione pubblica circa

oggettivo che limiti l'accesso a tali dati per sole esigenze di accertamento di reati "sufficientemente gravi da giustificare una simile ingerenza", ben oltre - dunque - il generico rinvio ai reati gravi definiti da ciascuno Stato membro; 3) omesso di sancire i presupposti sostanziali e procedurali ai quali subordinare l'accesso, da parte delle competenti autorità nazionali, ai dati in esame, in particolare non richiedendo in ogni caso il previo controllo dell'autorità giudiziaria o di un'autorità amministrativa indipendente; 4) omesso di prevedere criteri necessari a differenziare la durata della conservazione dei dati, limitandosi a stabilirne i soli termini minimi (6 mesi) e massimi (24); 5) omesso di imporre che i dati così acquisiti siano conservati nel (solo) territorio della Ue.

Si tratta, dunque, di una sentenza che valorizza moltissimo la centralità del diritto alla protezione dei dati personali anche in un settore - quale quello del contrasto al crimine - in cui maggiori sono le limitazioni alle libertà, ammesse per esigenze di interesse generale. Il punto cardine della pronuncia è indubbiamente il principio di stretta proporzionalità tra limitazioni dei diritti fondamentali ed esigenze di pubblica sicurezza; proporzionalità che non va delineata in astratto e in maniera indifferenziata rispetto a qualsiasi reato ma che, al contrario, esige una differenziazione attentamente modulata in base al tipo di delitto, alle esigenze investigative, al tipo di dato e di mezzo di comunicazione utilizzato.

³⁹ Trattasi della sentenza della Corte di giustizia del 13 maggio 2014, nota come **"sentenza sul diritto all'oblio sul web"**. Il diritto all'oblio può definirsi, come emerge dalla sentenza, come "il diritto della persona a opporsi all'indicizzazione dei propri dati personali ad opera del motore di ricerca, qualora la diffusione di tali dati tramite quest'ultimo le arrechi pregiudizio", in particolare, "qualora i dati risultino inadeguati, non siano o non siano più pertinenti". In sintesi, la Corte di giustizia dell'Unione Europea ha stabilito che gli utenti possono chiedere ai motori di ricerca di rimuovere risultati collegati al loro nome. Google ha quindi pubblicato un nuovo strumento per richiedere la rimozione dei contenuti: la richiesta può essere inoltrata da qualunque cittadino ritenga che le informazioni nei risultati associati ad una ricerca del suo nome possano essere – riportando il testo della sentenza – "inadeguati, irrilevanti o non più rilevanti, o eccessivi in relazione agli scopi per cui sono stati pubblicati". Il diritto all'oblio non è stato creato dalla sentenza della Corte di Giustizia del 13 maggio 2014, ma esisteva già prima. Un'importante pronuncia in merito è quella della **Corte di Cassazione, sentenza n. 5525 del 5 aprile 2012** con la quale la Suprema Corte aveva stabilito che le testate online avrebbero dovuto dotare i loro archivi di "un sistema idoneo a segnalare (nel corpo o nel margine) la sussistenza di un seguito o di uno sviluppo della notizia e quale esso sia stato (...) consentendone il rapido e agevole accesso da parte degli utenti ai fini del relativo e adeguato approfondimento". Il caso, giunto davanti alla Corte, riguardava la notizia del coinvolgimento giudiziario di un rappresentante politico lombardo: l'uomo era stato arrestato nel 1993 con accuse di corruzione, ma in seguito era stato prosciolto. La notizia del suo arresto, tuttavia, compariva ancora tra i risultati dei motori di ricerca per via dell'articolo presente sull'archivio storico del Corriere della Sera. Rivolgendosi prima al Garante privacy e poi al Tribunale di Milano, l'uomo aveva chiesto la rimozione dei dati giudiziari che lo riguardavano, lamentando l'assenza di un aggiornamento – all'interno della notizia archiviata – che riportasse l'esito favorevole della vicenda. In alternativa chiedeva l'inserimento di un aggiornamento correlato alla notizia o lo spostamento dell'articolo in un'area del sito non indicizzata dai motori di ricerca. Le richieste, tuttavia, non erano state accettate né dal Garante né dal Tribunale. Chiamata in causa, la Corte di Cassazione aveva invece accolto le motivazioni del ricorrente: pur stabilendo che non esisteva un profilo di diffamazione dal momento che i fatti descritti dall'articolo erano veri all'epoca della sua pubblicazione, la Corte ha riconosciuto la parzialità dell'informazione alla luce degli avvenimenti seguenti. Nel tentativo di **bilanciare l'interesse collettivo, garantito dal diritto di cronaca, con l'interesse individuale, tutelato dal diritto alla riservatezza e dal diritto all'oblio, la Corte ha quindi stabilito che gli articoli archiviati dovessero essere correlati dai relativi aggiornamenti**. La decisione è volta in questo modo a tutelare non solo il diritto all'identità personale e morale della persona coinvolta nei fatti, ma anche il diritto del cittadino utente a ricevere una corretta e completa informazione. La sentenza della Cassazione attribuisce dunque un nuovo valore al diritto all'oblio all'interno dei principi stessi del diritto di cronaca. Nessuna attribuzione di responsabilità era invece stata all'epoca attribuita dalla Corte ai motori di ricerca, ancora una volta definiti come "meri intermediari". Ciò fino alla pronuncia della Corte di Giustizia che, un paio di anni dopo, individua una diretta responsabilità del motore di ricerca.

⁴⁰ Google e Facebook hanno manifestato di recente la volontà di una nuova e profonda revisione delle loro regole per la privacy. *"La decisione assunta da Google sul diritto all'oblio, precisa Soro, va salutata con favore, anche se andranno verificate in concreto le modalità di bilanciamento dei diritti del singolo con la memoria collettiva. (...) L'azienda si sta mettendo in discussione: un segnale importante è che abbia avvertito il bisogno di andare in giro per il mondo a manifestare attenzione nei confronti dei propri utenti. Di fatto le grandi aziende digitali sono preoccupate di perdere la fiducia dei consumatori perché i consumatori hanno acquisito consapevolezza dei rischi per la privacy"*.

⁴¹ Lo **scandalo Datagate** è iniziato con la pubblicazione da parte del quotidiano britannico *Guardian*, nel mese di giugno 2013, di alcuni documenti riservati. Secondo questi documenti, la compagnia di telecomunicazioni *Verizon* consegnerebbe all'*FBI* dati in grado di mettere a rischio la privacy dei propri utenti come i numeri di telefono delle conversazioni, il luogo dal quale partono, orari e durata delle conversazioni telefoniche. La notizia che le comunicazioni

l'effettiva riservatezza dei dati personali. Il terzo attore, e anche probabilmente il più importante, sono le aziende, che cominciano a mostrarsi più disponibili a discutere, solo per fare qualche esempio, di profiling, di consenso o di informative più dettagliate: questo perché, sostanzialmente, temono di perdere utenti. In questo scenario bisognerà che, nel prossimo semestre, anche la politica faccia la sua parte: lo auspichiamo e anzi lo chiediamo esplicitamente. In questo nuovo scenario, è auspicabile che anche i governi prendano iniziative e investano in maniera decisa in protezione dati". E aggiunge: "in un mondo segnato dall'incontenibile affidamento alla tecnologia di parti essenziali della nostra esistenza, proteggere i nostri dati significa proteggere la nostra vita e la nostra libertà. Oggi le persone trascorrono le giornate molto più nello spazio digitale che in quello fisico. Investire nella protezione dei dati significa investire nella sicurezza e nella tutela dei cittadini, è una forma moderna e nuova di tutela dei diritti umani. Ma questo porta con sé la necessità che i governi se ne facciano carico e che non considerino lo sviluppo digitale soltanto

negli Stati Uniti sarebbero sotto controllo ha fatto subito il giro del mondo ed è apparsa su tutti i giornali, richiedendo un commento da parte del presidente Obama.

Rilevante sul tema anche la nota **prescrizione del Garante del 15 ottobre 2010** che ha condannato Google a pagare una sanzione di 1 milione di euro per il servizio *Street View*. I fatti contestati risalgono al 2010 quando le auto del colosso di *Mountain View* percorrevano le strade italiane senza essere perfettamente riconoscibili e non consentendo, in tal modo, alle persone presenti nei luoghi percorsi dalle "Google Cars" di decidere se sottrarsi o meno alla "cattura" delle immagini. Numerose erano state le segnalazioni all'Autorità da parte di persone che non desideravano comparire nelle foto pubblicate *on line* (che, peraltro, permangono in rete per un tempo considerevole e possono essere ingrandite).

Il Garante aveva prescritto pertanto alla società di *Mountain View* di rendere le "Google cars" facilmente individuabili, attraverso cartelli o adesivi ben visibili, di pubblicare sul proprio sito web, tre giorni prima dell'inizio delle riprese, le località visitate dalle vetture di *Street View*, stabilendo che per le grandi città è necessario indicare i quartieri in cui circolano le vetture. Analogo avviso deve essere pubblicato da Google sulle pagine di cronaca locale di almeno due quotidiani e diffuso per mezzo di un'emittente radiofonica locale per ogni regione visitata. Le misure sono state tempestivamente adottate da Google. A conclusione dell'intero procedimento sanzionatorio il Garante ha ritenuto di applicare la sanzione nella cifra complessiva di un milione di euro. Proprio tenendo conto di trovarsi di fronte a una società che, nell'anno 2012, ha registrato un fatturato consolidato pari a oltre 50 miliardi di dollari, il Garante ha deciso di avvalersi della norma del Codice privacy (art. 164 bis, comma 4) che mira a rendere effettive le sanzioni quando sono dirette a soggetti di notevoli dimensioni economiche, applicando l'aumento pari a quattro volte l'importo della sanzione che era di 250.000 euro.

Degno di nota è infine il **provvedimento del Garante n. 555 del 4 dicembre 2014**. Con istanza del 23 settembre 2014 la società Google aveva comunicato all'Autorità l'intenzione di estendere anche al territorio nazionale il programma denominato "Google Special Collects", già attivo altrove, di "raccolta immagini in luoghi unici e remoti, inclusi quelli con particolare valore naturalistico, storico e turistico. In particolare, il servizio consentirà di registrare immagini a 360 gradi in ambienti non raggiungibili dalle tradizionali vetture di "Google Street View", come siti archeologici, parchi nazionali, musei e spiagge. Le apparecchiature fotografiche saranno trasportate a piedi da operatori (*trekker*), o installate su mezzi alternativi, come imbarcazioni o treni. Nella richiesta al Garante, Google affermava che nei musei e in altri luoghi ad accesso limitato, al fine di limitare eventuali riprese di visitatori, avrebbe effettuato le registrazioni negli orari di chiusura al pubblico. Nelle altre aree, come spiagge e spazi aperti, invece, sarebbero stati scelti orari in cui sia meno probabile incontrare passanti. La multinazionale americana avrebbe provveduto inoltre a oscurare i volti e altri particolari identificativi (ad esempio, le targhe dei veicoli), eventualmente memorizzati, prima di rendere disponibili le immagini sul servizio *Google Maps*.

L'Autorità, nell'ambito del bilanciamento di interessi e in base alla peculiarità del servizio rispetto alla versione standard di *Street View*, ha – con il provvedimento citato - imposto alla società l'adozione di adeguate cautele a tutela degli interessati e di misure semplificate per informarli delle riprese in corso. In particolare, Google dovrà pubblicare informazioni sui luoghi di ripresa sul proprio sito web in italiano nei tre giorni antecedenti l'inizio dei lavori. Informazioni dettagliate dovranno essere pubblicate già sette giorni prima dell'inizio delle riprese anche sui siti web e, se esistenti, sulle newsletter o altre pubblicazioni informative dei *partners*, cioè degli enti, strutture, soggetti privati, fondazioni etc.. coinvolti nel programma. Nei luoghi ad accesso controllato, Google o i suoi incaricati dovranno provvedere a informare le persone interessate – anche attraverso appositi avvisi o cartelli affissi all'ingresso dei siti - della imminente registrazione delle immagini, in modo da consentire ai visitatori di esercitare il diritto a non venire inquadrati. La multinazionale americana dovrà inoltre garantire la formazione del personale coinvolto circa il rispetto della normativa sulla protezione dei dati personali. Dovrà infine dotare gli operatori di adesivi o altri segni distintivi ben visibili da applicare sull'abbigliamento e sulle attrezzature, in modo da segnalare chiaramente che si stanno acquisendo immagini da pubblicare *online* su *Google Maps* mediante il servizio *Google Special Collects* nell'ambito di *Street View*.

come sviluppo delle tecnologie, quasi che gli esseri umani non contassero. Le nuove tecnologie presentano ovviamente grandi opportunità, ma anche molti rischi. E anche di questi rischi ci dobbiamo occupare. Il dato positivo, dice Soro, è che “*si è aperta una fase nuova e affascinante che spinge tutti ad affrontare con più responsabilità le contraddizioni della Rete, e a ricercare nuovi equilibri tra fattibilità tecnica, accettabilità giuridica e fondamento etico della società digitale*”.

Infine, a proposito di etica, nella relazione annuale dell'Authority al parlamento, Soro ha ricordato le nuove forme di criminalità in Rete: “*si va dal furto di identità fino alla più organizzata criminalità cibernetica. È un'emorragia stimata in 500 miliardi di dollari l'anno tra identità violate, segreti aziendali razzati, portali messi fuori uso e moneta virtuale sottratta. Inoltre sono sempre più frequenti i casi di incitamento all'odio ma anche fenomeni quali cyberbullismo⁴² e grooming⁴³, spesso alimentati dalla logica del branco o dall'infondata presunzione di anonimato. Sono alcuni dei campi tematici di intervento del Garante per la Privacy*”.

- Sentenza del 13 maggio 2014 – Corte di giustizia e sentenza n. 5525 del 5 aprile 2012 – Corte di Cassazione – Argomento: diritto all'oblio sul web;

sentenza dell'8 aprile 2014 – Corte di giustizia – Argomento: data retention;

scandalo datagate e prescrizione del Garante del 15 ottobre 2010 - Argomento: acquisizione di immagini tramite il servizio Street view;

provvedimento Garante n. 555 del 4 dicembre 2014 – Argomento: parziale esonero dall'informativa in relazione al servizio Google Special Collects

Le pronunce sopra citate sono da ritenersi rilevanti in tema di trattamento dei dati personali e danno ben conto di come la tutela di tali dati debba, specie in tempi recenti, estendersi anche al *web*. Non riguardando direttamente la materia scolastica, si è ritenuto opportuno citarle soltanto in nota nell'ambito del paragrafo precedente (si vedano le note n. 38, 39, 40 e 41).

- Provvedimento Garante n. 243 del 15 maggio 2014 - “Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati”

Sul tema del delicato rapporto tra trasparenza e privacy occorre esaminare, sia pure sinteticamente, questo documento che fornisce importanti direttive alle istituzioni scolastiche. Trattasi di specifiche disposizioni del Garante volte a disciplinare la diffusione di informazioni contenute in documenti amministrativi riportati sui siti istituzionali. Le linee guida⁴⁴, emanate alla luce del recente **decreto legislativo n. 33/2013**⁴⁵, riguardano sia la pubblicazione di dati e documenti che le P.A. devono mettere *on line* per finalità di trasparenza, sia di quelli finalizzati a garantire altri obblighi di pubblicità degli atti amministrativi (es. pubblicazioni matrimoniali, deliberazioni sull'albo pretorio *on line*, avviso di deposito delle cartelle esattoriali, ecc...).

In primo luogo, si ribadisce che è necessario che i dati pubblicati *on line* siano esatti, aggiornati e contestualizzati, nonché che venga rispettato il criterio dell'essenzialità, evitando che siano pubblicate informazioni non strettamente necessarie. Resta fermo il divieto della pubblicazione di dati sulla salute e sulla vita sessuale, mentre i dati sensibili (etnia, religione, appartenenze politiche, etc.) possono essere diffusi solo ed esclusivamente se indispensabili al perseguimento delle finalità di rilevante interesse pubblico.

⁴² Se ne tratterà *infra* nella sezione “**Cyberbullismo**” a pag. 35.

⁴³ Fenomeno per cui pedofili adescano ragazzini in Rete creando un clima di falsa familiarità.

⁴⁴ Le linee guida hanno formato oggetto di un successivo **comunicato stampa del Garante del 28 maggio 2014**. Ad esso si è fatto riferimento per un'analisi sintetica delle stesse.

⁴⁵ Per l'analisi dell'**accesso civico** previsto dal **d.lgs. 33/2013** ed oggetto della **sentenza n. 5515 del 20 novembre 2013 del Consiglio di Stato, sez. VI** vedi anche *infra* pag. 52 e ss.

Viene affrontato anche il tema dell'**indicizzazione** dei dati attraverso i più comuni motori di ricerca: si pensi alla facilità con cui alcune informazioni anche riservate relative ad una persona si possono reperire su Google o altri motori di ricerca con la semplice digitazione del nome e del cognome, casi sui quali l'Autorità è stata spesso chiamata a pronunciarsi. A tale proposito il Garante ha prescritto che l'obbligo di indicizzare i dati nei motori di ricerca generalisti durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza. Vanno dunque esclusi gli altri dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (es. pubblicità legale sull'albo pretorio). E comunque non possono essere indicizzati, e quindi reperibili attraverso i motori di ricerca, i dati sensibili e giudiziari.

Quanto poi agli **open data**⁴⁶ e al **riutilizzo dei dati**, il Garante precisa che i dati pubblicati on line non sono liberamente utilizzabili da chiunque per qualunque finalità: l'obbligo previsto dalla normativa in materia di trasparenza on line della P.A. di pubblicare dati in "formato aperto", non comporta che tali dati siano anche "dati aperti", cioè liberamente utilizzabili da chiunque per qualunque scopo. Il riutilizzo dei dati personali non deve pregiudicare, anche sulla scorta della direttiva europea in materia, il diritto alla privacy. E' opportuno quindi che le P.A. inseriscano nella sezione denominata "Amministrazione trasparente" sui propri siti *web* un *alert* con cui si informa il pubblico che i dati personali sono riutilizzabili in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto delle norme sulla protezione dei dati personali. I dati sensibili e giudiziari, in ogni caso, non possono essere riutilizzati.

Il Garante affronta anche la questione della **durata degli obblighi di pubblicazione**: il periodo di mantenimento on line dei dati è stato generalmente fissato in 5 anni dal decreto legislativo n. 33. Sono previste però alcune deroghe, come nell'ipotesi in cui gli atti producano i loro effetti oltre questa scadenza. In ogni caso, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti hanno prodotto i loro effetti, i dati personali devono essere oscurati anche prima del termine dei 5 anni.

A proposito di **dati sensibili, a tutela di fasce deboli**, persone invalide, disabili o in situazioni di disagio economico destinatari di sovvenzioni o sussidi, sono previste limitazioni nella pubblicazione dei dati identificativi. Non è quindi consentita, ad esempio, la pubblicazione di dati riguardanti la morosità delle famiglie per quanto riguarda il pagamento della mensa scolastica oppure informazioni riferite a situazioni di disabilità nelle graduatorie concorsuali.

Risulta invece proporzionato indicare il compenso complessivo percepito dai singoli dipendenti (determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione). Non è però giustificato riprodurre sul *web* le dichiarazioni fiscali o la versione integrale dei cedolini degli stipendi. Vi è infine l'obbligo di pubblicare la dichiarazione dei redditi di politici e amministratori, con l'esclusione di dati non pertinenti (stato civile, codice fiscale) o dati sensibili (spese mediche, erogazioni di denaro ad enti senza finalità di lucro, ecc...), così come risponde anche ad un preciso obbligo di trasparenza la pubblicazione dei curricula, ad esempio dei titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza.

- Ordinanza di ingiunzione nei confronti della Regione Puglia, provvedimento Garante n. 57 del 6 febbraio 2014 – Argomento: vietata la diffusione in internet di dati che possano rivelare lo stato di salute dei cittadini

Il caso riguarda una segnalazione nella quale si lamentava la diffusione, attraverso il sito *web* istituzionale della Regione Puglia, di alcune graduatorie concernenti la concessione di contributi nei confronti di persone disabili.

⁴⁶ I dati aperti, comunemente chiamati con il termine inglese **open data** anche nel contesto italiano, sono alcune tipologie di dati liberamente accessibili a tutti, privi di brevetti o altre forme di controllo che ne limitino la riproduzione. L'*open data* si richiama alla più ampia disciplina dell'*open government* cioè una dottrina in base alla quale la pubblica amministrazione dovrebbe essere aperta ai cittadini, tanto in termini di trasparenza quanto di partecipazione diretta al processo decisionale, anche attraverso il ricorso alle nuove tecnologie dell'informazione e della comunicazione.

L'Autorità per la privacy verificava, in particolare, che la Regione Puglia aveva pubblicato i nominativi di chi aveva fatto domanda per partecipare ad un bando riservato ai disabili, rivelandone, oltre al nominativo, anche lo stato di salute. I documenti allegati nelle domande, tra l'altro, riportavano anche altri dati che non avrebbero dovuto essere pubblicati in chiaro, come ad esempio per le domande non ammesse, la motivazione dell'esclusione, la data e l'ora dell'istruttoria, l'esito. Tutte queste informazioni, oltre ad essere perfettamente visibili erano anche scaricabili in rete inserendo le generalità nei motori di ricerca.

Per tutte queste motivazioni, il Garante vietava alla Regione Puglia l'ulteriore diffusione di dati personali contenuti in tali documenti, ordinava per il futuro di conformare la pubblicazione di atti pubblici alle disposizioni del Codice privacy, disponendo anche di contattare i responsabili dei maggiori motori di ricerca per sollecitare la rimozione degli allegati dalla copia *web* e dai motori di ricerca stessi. Condannava infine la Regione al pagamento della somma di € 20.000 per violazione dei principi di cui all'art. 22, comma 8 C.P.⁴⁷

- Comunicato stampa Garante dell'11 settembre 2013 – Argomento: sì alla trasparenza, ma senza violare la privacy

In occasione della riapertura delle scuole il Garante per la privacy ricorda alle istituzioni scolastiche di ogni ordine e grado la necessità di tenere presenti alcuni principi stabiliti nei provvedimenti adottati negli anni precedenti in materia di trasparenza in ambito scolastico, a tutela dei dati degli studenti e dei lavoratori che operano nel mondo dell'istruzione. Numerosi sono, infatti, i casi in cui istituti e pubbliche amministrazioni, per un'errata interpretazione della normativa sulla trasparenza o per semplice disattenzione, rendono accessibili informazioni che dovrebbero restare riservate, mettendo in questo modo a rischio la riservatezza e la dignità delle persone. In particolare, si precisa che **le graduatorie pubblicate on line devono contenere solo dati pertinenti**: il Garante è infatti intervenuto più volte contro illeciti compiuti nella pubblicazione *on line* di graduatorie di vario tipo, le quali spesso contengono dati personali non pertinenti o eccedenti le finalità istituzionali perseguite.

Alcuni Comuni, ad esempio, hanno pubblicato *on line* le graduatorie di chi ha diritto ad usufruire del servizio di scuolabus includendo tra le varie informazioni liberamente accessibili, non solo i dati identificativi dei bambini, ma anche l'indirizzo di residenza e il luogo preciso dove lo scuolabus li avrebbe fatti salire e scendere. La diffusione di questi dati, oltre a comportare una violazione della normativa, può rendere i minori facile preda di malintenzionati.

Un altro caso frequente riguarda la pubblicazione sui siti Internet degli istituti delle graduatorie di docenti e personale amministrativo tecnico e ausiliario (A.T.A.) per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste, giustamente accessibili a tutti, non devono però contenere, come in diversi casi segnalati al Garante, i numeri di telefono e gli indirizzi privati dei candidati. Questa illecita diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre i lavoratori a forme di *stalking* o a possibili furti di identità.

Anche **i moduli di iscrizione di bambini e studenti devono essere predisposti con cura da istituti scolastici, asili nido e Comuni, così da non chiedere alle famiglie informazioni personali eccedenti e non rilevanti**. Particolare attenzione deve essere posta sull'eventuale raccolta di dati sensibili, come quelli sulle condizioni di salute e sull'appartenenza etnica o religiosa. Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa, richiede infatti speciali cautele e può essere effettuato solo se i dati sensibili sono indispensabili per l'attività istituzionale svolta.

Quanto alle prestazioni di carattere economico, il Garante ricorda che **è illecito pubblicare sul sito della scuola il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della**

⁴⁷ Per l'art. 22 C.P. vedi *infra* nota n. 69, pag. 31.

retta o del servizio mensa⁴⁸. Lo stesso vale per gli studenti che usufruiscono gratuitamente del servizio in quanto appartenenti a famiglie con reddito minimo o a fasce deboli. Gli avvisi messi *on line* devono avere carattere generale, mentre alle singole persone ci si può rivolgere con comunicazioni di carattere individuale. Resta inteso che, a salvaguardia della trasparenza sulla gestione delle risorse scolastiche, restano ferme le regole sull'accesso ai documenti amministrativi da parte delle persone interessate.

- Nota M.I.U.R. n. 510 del 22 gennaio 2013 – Argomento: divieto di pubblicazione dei dati sensibili nelle graduatorie ad esaurimento, di circolo e di istituto

La nota in oggetto dà riscontro ad alcune segnalazioni pervenute all'Autorità Garante per la Protezione dei Dati Personali che denunciano la pubblicazione sui siti *web* istituzionali di istituti scolastici, nonché di altri uffici periferici di graduatorie relative al personale docente, nonché al personale A.T.A., recante oltre ai punteggi maturati, al nominativo e alla data di nascita degli interessati, anche dati ulteriori che non rispettano il requisito della "pertinenza, completezza e non eccedenza rispetto alle finalità" (quali il numero di codice fiscale, il numero di figli a carico, l'indirizzo di residenza, nonché recapiti telefonici e di posta elettronica).

Il Ministero pertanto precisa che in base alla normativa di cui al D.P.R. 445/2000, peraltro esplicitamente richiamata nei vari modelli di domanda di partecipazione alle procedure finalizzate alla produzione di elenchi e graduatorie, i dati richiesti al candidato sono acquisiti ai sensi dell'art. 16⁴⁹ del citato D.P.R. solo in quanto strettamente funzionali all'espletamento della procedura stessa ed assumono il carattere di riservatezza previsto dal d.lgs. 196/2003. Pertanto i dati forniti dal Sistema Informativo sono realizzati in duplice copia: l'una ai fini della pubblicazione (contenente soltanto i dati strettamente necessari all'individuazione del candidato, quali nome, cognome, punteggi e posizione in graduatoria) e l'altra, riservata ai soli uffici, in forma completa per tutti gli adempimenti procedurali. Il M.I.U.R. rivolge quindi un monito agli uffici e alle istituzioni scolastiche a voler prestare la massima attenzione nell'estrarre dal sistema il *file* con i dati da pubblicare.

- Provvedimento Garante n. 383 del 6 dicembre 2012 – Argomento: diffusione sul sito *web* istituzionale di una scuola di dati personali relativi agli studenti

Il provvedimento di cui trattasi sanziona un istituto scolastico per avere diffuso sul proprio sito *web* l'elenco degli studenti ammessi alle classi prime evidenziando con un diverso carattere i nomi e i cognomi di quelli ripetenti. Dal canto suo, il dirigente scolastico, invitato a fornire gli opportuni chiarimenti, evidenzia che vi sarebbe stato un assembramento di dati provenienti da diversi *file* che poteva aver causato la presenza di alcuni nominativi riportati con caratteri differenti ed, in secondo luogo, che in ogni caso, la lista era stata prontamente corretta. Il dirigente sottolinea poi che la pubblicazione degli elenchi degli iscritti alle prime classi del liceo rientra nelle finalità di trasparenza e pubblicità amministrative, atte ad indicare ufficialmente l'elenco degli studenti iscritti, la consistenza numerica delle classi e la divulgazione precoce degli inserimenti, al fine di snellire le procedure necessarie all'avvio dell'anno scolastico ed agevolarne il rispetto (acquisto libri di testo, conoscenza sede di allocazione delle classi, eventuale verifica di richiesta di desiderata, ecc...),

⁴⁸ Sul medesimo argomento vedi anche *infra* pag. 29, comunicato stampa del Garante del 27 ottobre 2010.

⁴⁹ In D.P.R. 445/2000 "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa", Capo II "Documentazione amministrativa", Sezione III "Trasmissione di documenti", art. 16 "Riservatezza dei dati personali contenuti nei documenti trasmessi": "Al fine di tutelare la riservatezza dei dati personali (...), i certificati ed i documenti trasmessi ad altre pubbliche amministrazioni possono contenere soltanto le informazioni relative a stati, fatti e qualità personali previste da legge o da regolamento e strettamente necessarie per il perseguimento delle finalità per le quali vengono acquisite".

considerato il numero dei destinatari, l'onerosità, la tempistica e la possibile inefficienza di una comunicazione personale.

Tali affermazioni non sono condivise dal Garante che, richiamando l'art. 19, comma 3 del Codice⁵⁰, evidenzia come **la pubblicazione della composizione delle varie classi non risulti essere autorizzata da alcuna norma di legge o di regolamento**. Il medesimo principio è espresso anche al punto 2.1⁵¹ delle "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web" adottate con provvedimento generale del 2 marzo 2011⁵². Il Garante evidenzia "(...) *lo scopo di definire un primo quadro unitario di misure e accorgimenti finalizzati a individuare opportune cautele che i soggetti pubblici sono tenuti ad applicare in relazione alle ipotesi in cui effettuano, in attuazione alle disposizioni normative vigenti, attività di comunicazione o diffusione di dati personali sui propri siti istituzionali per finalità di trasparenza, pubblicità dell'azione amministrativa, nonché di consultazione di atti su iniziativa di singoli soggetti*" (punto 1 delle Linee guida). Il richiamo va anche alle **diverse finalità per cui può essere effettuata la diffusione, ovvero la trasparenza e la pubblicità amministrativa: si tratta di finalità differenti, rispetto alle quali le pubbliche amministrazioni devono effettuare specifiche e differenziate valutazioni sia in relazione al rispetto dei principi di necessità e proporzionalità del trattamento dei dati personali, sia sugli strumenti e sui mezzi utilizzati per assicurarne la conoscibilità, affinché siano correttamente rispettati i diritti degli interessati** (punto 4 delle Linee Guida⁵³).

Tutto ciò premesso, il Garante, ritenuto illecito il trattamento dei dati effettuato dal liceo in questione, vieta ad esso di diffondere ulteriormente i nominativi dei propri studenti distinti per classe sul proprio sito Internet istituzionale, in assenza, appunto, di una norma di legge o di regolamento che ammetta tale operazione.

⁵⁰ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo II "Regole ulteriori per i soggetti pubblici", art. 19 C.P. "Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari", comma 3: "La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento". Per un caso analogo si veda anche *infra* pag. 29, **decisione del Garante su ricorso del 13 maggio 2010**.

⁵¹ Il **punto 2.1** delle citate **Linee Guida del 2011**, rubricato "Pubblicazione di dati personali sulla base di espressa previsioni normative", così dispone: "In relazione alle sole operazioni di comunicazione e di diffusione, le pubbliche amministrazioni, nel mettere a disposizione sui propri siti istituzionali dati personali, contenuti anche in atti e documenti amministrativi (in forma integrale, per estratto, ivi compresi gli allegati), devono preventivamente verificare che una norma di legge o di regolamento preveda tale possibilità (artt. 4, comma 1, lett. l) e m), 19, comma 3, 20 e 21, del Codice), fermo restando comunque il generale divieto di diffusione dei dati idonei a rivelare lo stato di salute dei singoli interessati (artt. 22, comma 8, 65, comma 5, 68, comma 3, del Codice)".

⁵² Si consideri che le Linee Guida adottate con provvedimento del 2 marzo 2011 devono ritenersi ormai sostituite dalle più recenti Linee Guida adottate con provvedimento del 15 maggio 2014. Ad ogni modo i principi contenute nelle prime Linee Guida e richiamati dal provvedimento 6 dicembre 2012 non devono ritenersi in contraddizione con quelli oggetto delle Linee guida più recenti.

⁵³ Il **punto 4** delle citate **Linee Guida del 2011**, rubricato "Trasparenza, pubblicità e consultabilità di atti e documenti: valutazione delle tre grandi finalità perseguibili mediante la pubblicazione on line" chiarisce che: "Le previsioni normative in materia di trasparenza, pubblicità e consultabilità degli atti, preordinate ad assicurare un certo grado di conoscenza dell'operato della pubblica amministrazione, non perseguono finalità analoghe. Le pubbliche amministrazioni, pertanto, sono tenute, in primo luogo, a valutare quali specifiche finalità sono rinvenibili dalle disposizioni legislative o regolamentari che prevedono un particolare regime di conoscibilità di informazioni, atti e documenti amministrativi. In particolare, occorre distinguere i casi in cui, in relazione alla attività di comunicazione o diffusione di dati personali attraverso la pubblicazione di atti e documenti amministrativi sui siti istituzionali, si perseguono finalità di: A Trasparenza; B Pubblicità; C Consultabilità. Tali valutazioni devono essere effettuate dalle amministrazioni pubbliche, nel rispetto dei principi di necessità e proporzionalità del trattamento dei dati personali (artt. 3 e 11 del Codice), in modo da garantire modalità differenziate di messa a disposizione di dati e documenti tenendo conto delle diverse finalità sopra evidenziate (...), delle tipologie di informazioni oggetto di divulgazione, nonché degli strumenti e dei mezzi utilizzati per assicurarne la conoscibilità, affinché siano correttamente rispettati i diritti degli interessati".

- **Provvedimento Garante n. 341 del 15 novembre 2012** – **Argomento: vietate le annotazioni di rettificazione di sesso su diplomi e certificazioni di laurea**

Nel caso di specie, l'università degli studi di "omissis" pone un interessante quesito al Garante. In particolare, chiede se, a seguito di una sentenza che accoglie la domanda di rettificazione di attribuzione di sesso, possa violare la riservatezza dell'individuo aggiungere un'annotazione in calce al diploma che riporta la sentenza e il nuovo nome dell'interessato, diploma che rimane comunque intestato alla persona con i precedenti dati anagrafici, ovvero se sia preferibile operare una ristampa del diploma con i nuovi dati anagrafici.

Il Garante risponde richiamando la legge n. 164/1982 recante "Norme in materia di rettificazione di attribuzione di sesso" ed in particolare l'art. 5 a mente del quale "Le attestazioni di stato civile riferite a persona della quale sia stata giudizialmente rettificata l'attribuzione di sesso sono rilasciate con la sola indicazione del nuovo sesso e nome", nonché il d.lgs. 150/2011 rubricato "Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione, ai sensi dell'articolo 54 della legge 18 giugno 2009, n. 69" ed, in particolare, l'art. 31, comma 5 dedicato alle "Controversie in materia di rettificazione di attribuzione di sesso" il quale prevede che "con la sentenza che accoglie la domanda di rettificazione di attribuzione di sesso il tribunale ordina all'ufficiale di stato civile del comune dove è stato compilato l'atto di nascita di effettuare la rettificazione nel relativo registro". L'Autorità, richiamando infine la speciale protezione relativa ai dati sensibili idonei a rivelare la vita sessuale, dispone di omettere l'annotazione della motivazione della ristampa dei diplomi di laurea richiesta dagli studenti per i quali sia intervenuta una sentenza del tribunale di rettificazione di attribuzione di sesso passata in giudicato, modalità ritenuta idonea a tutelare adeguatamente la dignità degli interessati e il diritto degli stessi a vedere correttamente rappresentata la propria identità sessuale a seguito della sua modificazione. Nel medesimo provvedimento il Garante prescrive alle università, ai sensi dell'art. 154, comma 1, lett. c), del Codice⁵⁴, che, sia **nelle certificazioni rilasciate in conformità alla legge**, sia nella predisposizione dell'ulteriore documentazione richiesta dall'interessato, ivi compresa la ristampa del diploma di laurea prevedano, nell'ambito dell'autonomia ad esse attribuita dall'ordinamento, **l'adozione di idonei accorgimenti e cautele**, anche similari a quelli sopra prospettati, **al fine di non riportare in tale documentazione elementi idonei a rivelare l'avvenuta rettificazione di attribuzione di sesso per effetto di una sentenza del tribunale passata in giudicato ed il nome originario dell'interessato**, a salvaguardia del suo futuro inserimento nei rapporti sociali e lavorativi, **fermi restando gli obblighi di conservazione, a norma di legge, dell'atto o del documento che contiene i dati personali dell'interessato con il sesso e il nome originario**.

- **Provvedimento Garante del 2 dicembre 2010** – **"Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica"**

Si ritiene opportuno inserire un cenno al provvedimento di cui in epigrafe stante l'ampia quantità di dati personali che emergono nell'ambito delle pronunce giurisdizionali per motivi di divulgazione giuridica. La diffusione dei provvedimenti giurisdizionali costituisce, infatti, fonte preziosa per lo studio e l'accrescimento della cultura giuridica, nonché strumento indispensabile di controllo da parte dei cittadini dell'esercizio del potere giurisdizionale: la conoscenza di tali provvedimenti è

⁵⁴ In Parte III "Tutela dell'interessato e sanzioni", Titolo II "L'Autorità", Capo I "Il Garante per la protezione dei dati personali", art. 154 C.P. "Compiti": "1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: (...) c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143 (...)".

realizzata in primo luogo dalla stessa Autorità giudiziaria “anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet” (art. 51, comma 2⁵⁵), osservando alcune cautele previste dallo stesso Codice Privacy (art. 52⁵⁶), volte alla tutela dei diritti e della dignità degli interessati. Alle cautele previste dal Codice rinvia anche l’art. 56, commi 2 e 2 bis⁵⁷ del d.lgs. 7 marzo 2005, n. 82 (Codice dell’amministrazione digitale) che, con riferimento alle sentenze e alle altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, ne prevede la pubblicazione anche sul sito istituzionale della rete Internet osservando le cautele previste dalla normativa in materia di tutela dei dati personali e stabilendone l’accessibilità ai sensi dell’articolo 51 del Codice Privacy.

⁵⁵ In Parte II “Disposizioni relative a specifici settori”, Titolo I “Trattamenti in ambito giudiziario”, Capo III “Informatica giuridica”, **art. 51 C.P.** “Principi generali”: “1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all’autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet. 2. Le sentenze e le altre decisioni dell’autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo”.

⁵⁶ In Parte II “Disposizioni relative a specifici settori”, Titolo I “Trattamenti in ambito giudiziario”, Capo III “Informatica giuridica”, **art. 52 C.P.** “Dati identificativi degli interessati”: “1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell’autorità giudiziaria di ogni ordine e grado, l’interessato può chiedere per motivi legittimi, con richiesta depositata nella cancelleria o segreteria dell’ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull’originale della sentenza o del provvedimento, un’annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l’indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento. 2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l’autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d’ufficio che sia apposta l’annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati. 3. Nei casi di cui ai commi 1 e 2, all’atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l’indicazione degli estremi del presente articolo: “In caso di diffusione omettere le generalità e gli altri dati identificativi di ...”. 4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l’annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l’indicazione delle generalità e degli altri dati identificativi dell’interessato. 5. Fermo restando quanto previsto dall’articolo 734-bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell’autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell’annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l’identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone. 6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell’articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l’annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell’articolo 32 della legge 11 febbraio 1994, n. 109, provvede in modo analogo in caso di richiesta di una parte. 7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali”.

La tutela in esame si aggiunge a quella prevista dall’**art. 734-bis c.p.** (“Divulgazione delle generalità o dell’immagine di persona offesa da atti di violenza sessuale”), che viene espressamente richiamato, il quale punisce chiunque divulghi, nell’ambito di determinati delitti a sfondo sessuale (soprattutto, ma non solo, relativi a minori), anche attraverso mezzi di comunicazione di massa, le generalità o l’immagine della persona offesa senza il suo consenso.

⁵⁷ Ai sensi dell’**art. 56 C.A.D.**, rubricato “Dati identificativi delle questioni pendenti dinanzi autorità giudiziaria di ogni ordine e grado”: “I dati identificativi delle questioni pendenti dinanzi al giudice amministrativo e contabile sono resi accessibili a chi vi abbia interesse mediante pubblicazione sul sistema informativo interno e sul sito istituzionale delle autorità emananti. 2. Le sentenze e le altre decisioni del giudice amministrativo e contabile, rese pubbliche mediante deposito in segreteria, sono contestualmente inserite nel sistema informativo interno e sul sito istituzionale, osservando le cautele previste dalla normativa in materia di tutela dei dati personali. 2-bis. I dati identificativi delle questioni pendenti, le sentenze e le altre decisioni depositate in cancelleria o segreteria dell’autorità giudiziaria di ogni ordine e grado sono, comunque, rese accessibili ai sensi dell’articolo 51 del codice in materia di protezione dei dati personali approvato con decreto legislativo n. 196 del 2003”.

La procedura prevista è quella della anonimizzazione, ovvero l'omissione - in caso di riproduzione del provvedimento - dei dati identificativi del soggetto citato nel provvedimento stesso.

Ciò può avvenire su richiesta dell'interessato (le parti di un giudizio civile, l'imputato in un processo penale o qualsiasi altro soggetto reso identificabile nel provvedimento stesso) esplicitandone i motivi legittimi oppure l'annotazione sul provvedimento può essere disposta d'ufficio dal magistrato il quale si fa carico di una specifica responsabilità nell'attenta valutazione dell'opportunità dell'anonimizzazione dei dati identificativi contenuti nei singoli provvedimenti, specie nei casi in cui emergano dati sensibili.

In merito, è opportuno rammentare il disposto di cui all'art. 26 C.P., comma 4 lett. c)⁵⁸ che prevede delle limitazioni che, proprio in ambito giudiziario, vengono poste alla difesa dei diritti in giudizio, laddove si richiede che il diritto alla riservatezza dei dati possa essere sacrificato solo ove il diritto azionato sia "di rango pari" a quello dell'interessato medesimo, *"ovvero consistente in un diritto o libertà fondamentale e inviolabile"*.

La salvaguardia dei diritti degli interessati attraverso un oscuramento delle loro generalità non pregiudica la finalità di informazione giuridica, sottesa alla diffusione del provvedimento, che il Codice intende salvaguardare, ma può risultare necessaria, nell'ottica di un corretto bilanciamento dei diversi interessi, rimesso alla responsabilità dell'Autorità giudiziaria procedente, per tutelare la sfera di riservatezza degli interessati.

Se la richiesta dell'interessato viene accolta (con decreto), spetta alla cancelleria o alla segreteria giudiziaria darvi esecuzione, apponendo sull'originale del provvedimento, all'atto del deposito da parte del magistrato, anche con un timbro, un'annotazione che riporti l'indicazione dell'art. 52 del Codice e la dizione: *"In caso di diffusione omettere le generalità e gli altri dati identificativi di ..."*.

Lo scopo è di escludere che il divieto possa essere esteso a ipotesi di diffusione diverse rispetto a quella della riproduzione del provvedimento per finalità di informazione giuridica. Spetta a chi riceve la copia provvedere all'omissione dei dati ove intenda riprodurla e diffonderla per finalità di informazione giuridica.

La prescrizione è rivolta in primo luogo all'Autorità Giudiziaria, ma anche a tutti gli altri soggetti, terzi rispetto ad essa, che svolgono attività di diffusione dei provvedimenti per finalità di informazione giuridica. Ci si riferisce, ad esempio, anche alla diffusione delle massime giuridiche estratte dai provvedimenti sull'originale dei quali sia apposta l'annotazione sull'omissione dei dati.

Il comma 5 dell'art. 52 del Codice pone, infine, uno specifico, ulteriore, divieto di diffusione dei dati dei minori e delle parti nei procedimenti giudiziari in materia di rapporti di famiglia e di stato

⁵⁸ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati" Capo III "Regole ulteriori per privati ed enti pubblici economici", art. 26 C.P. "Garanzie per i dati sensibili": "1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti. 2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.(...). 4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante: a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro (...) a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'ente (...); b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. (...); c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile; d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro (...). 5. I dati idonei a rivelare lo stato di salute non possono essere diffusi".

delle persone: si tratta di una tutela più ampia che impone di omettere, nei casi ivi considerati, non solo le generalità e gli altri dati identificativi dei soggetti tutelati, ma anche gli “*altri dati relativi a terzi dai quali può desumersi anche indirettamente l’identità*”.

In tali ipotesi l’obbligo opera “*in ogni caso*”, cioè anche qualora la sentenza o l’altro provvedimento giudiziale oggetto di diffusione non riporti l’annotazione di cui al comma 2 dell’art. 52; si tratta di un divieto assoluto: neppure il consenso dei soggetti interessati può determinare l’inapplicabilità dell’obbligo in esame.

I soggetti tutelati⁵⁹ sono i minori coinvolti in qualunque tipo di procedimento giudiziario e le parti, limitatamente ai procedimenti in materia di rapporti di famiglia e di stato civile delle persone di cui al Libro I del Codice Civile (quali, ad esempio: matrimonio e sue vicende, filiazione, adozione, ordini di protezione contro gli abusi familiari, azioni di stato, richieste di rettificazione di sesso). L’obbligo di omissione dei dati identificativi delle parti dei procedimenti in materia di famiglia e di status sussiste anche nei casi in cui la controversia attenga a rapporti di tipo patrimoniale o economico.

- Comunicato stampa Garante del 27 ottobre 2010 – Argomento: lista genitori morosi sul web

Coerentemente con i principi sopra esposti, il Garante è di recente intervenuto sulla questione della lista dei morosi pubblicata sul sito *web*⁶⁰ di un comune, aprendo un’apposita istruttoria sulla diffusione dei nomi di chi non è in regola con il pagamento della retta dell’asilo.

In una lettera rivolta all’amministrazione comunale si ricorda che più volte il Garante ha dichiarato **illecita la diffusione di dati personali mediante la pubblicazione di avvisi di mora o di sollecitazioni di pagamento. La diffusione di simili informazioni può contenere solo avvisi di carattere generale, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale.**

- Decisione Garante su ricorso del 13 maggio 2010 – Argomento: comunicazione di dati personali relativi agli allievi minorenni

Nel caso esaminato il Garante ha dichiarato **non lecito il trattamento dei dati personali di alunni minorenni da parte della scuola, che, volendo acquistare capi sportivi per gli studenti, aveva comunicato a un negozio di abbigliamento nomi e altri dati personali di questi, ritenendo violato l’art. 19 comma 3 del Codice privacy⁶¹, per mancanza di una norma di legge o di regolamento che prevedesse la necessità della suddetta comunicazione.**

Pur vertendo la decisione esclusivamente sui presupposti per la comunicazione dei dati personali a un soggetto privato, si può implicitamente rintracciare anche un’applicazione del principio di necessità nel trattamento dei dati, di cui all’art. 11, comma 1 lett. d) del Codice⁶². La legittima finalità perseguita dalla scuola (acquistare capi di abbigliamento sportivo adatti a ciascuno studente) non richiedeva, infatti, di comunicare all’esercizio commerciale nomi e altri dati personali degli studenti, potendo essere realizzata anche senza attivare il flusso di informazioni in questione.

⁵⁹ La tutela in esame si aggiunge a quella prevista dall’art. 734-bis c.p. (“*Divulgazione delle generalità o dell’immagine di persona offesa da atti di violenza sessuale*”), che viene espressamente richiamato, il quale punisce chiunque divulghi, nell’ambito di determinati delitti a sfondo sessuale (soprattutto, ma non solo, relativi a minori), anche attraverso mezzi di comunicazione di massa, le generalità o l’immagine della persona offesa senza il suo consenso.

⁶⁰ Sul medesimo argomento vedi anche *supra* pag. 23, comunicato stampa del Garante dell’11 settembre 2013.

⁶¹ L’art. 19 C.P. è richiamato in un caso analogo (vedi *supra* pag. 24, provvedimento del Garante n. 383 del 6 dicembre 2012 e nota n. 50, pag. 25).

⁶² In Parte I “*Disposizioni generali*”, Titolo III “*Regole generali per il trattamento dei dati*”, Capo I “*Regole per tutti i trattamenti*”, art. 11 C.P. “*Modalità del trattamento e requisiti dei dati*”: “1. I dati personali oggetto di trattamento sono: (...) d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati (...)”.

L'operazione di trattamento dei dati da parte della scuola è risultata, dunque, eccedente rispetto alle finalità e, pertanto, illecita.

Va osservato, altresì, che **il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali** (art. 18, comma 2 del Codice⁶³). Tuttavia, pare ragionevole estendere anche alla scuola, il principio, espresso dall'art. 3 del Codice⁶⁴ con riferimento ai sistemi informativi e programmi informatici, secondo cui **il trattamento dei dati personali va escluso quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità**. Il caso di specie rappresenta proprio uno di quei casi in cui la finalità perseguita dalla scuola (l'acquisto di abbigliamento) poteva essere comunque raggiunta senza la necessità di comunicare nomi e altri dati personali degli studenti.

- **Comunicato stampa Garante del 28 agosto 2008 – Argomento: pubblicità dei voti dell'esame di stato**

Il Garante per la protezione dei dati personali ribadisce che, come già precisato più volte, **nessun provvedimento dell'Autorità ha mai impedito la pubblicità dei voti dell'esame di stato**⁶⁵.

- **Provvedimento Garante del 28 febbraio 2008 – Argomento: blocco del trattamento dei dati personali relativi ad alunni beneficiari del contributo per l'acquisto dei libri di testo**

Con questo provvedimento il Garante ha bloccato il trattamento dei dati personali relativi alla lista con i nomi degli alunni delle scuole secondarie di I e II grado beneficiarie del contributo per l'acquisto dei libri di testo: tale lista era stata pubblicata sul sito *web* di un componente del consiglio comunale. Fra le informazioni personali pubblicate vi erano: i dati identificativi di alunni e genitori, l'ammontare del contributo economico erogato e in alcuni casi perfino le coordinate del conto corrente bancario. Il Garante, pur confermando il diritto del consigliere comunale di accedere ai documenti dell'amministrazione comunale, ha ritenuto tuttavia che **il trattamento dei dati personali (consistente in un'operazione di diffusione)** risultasse **effettuato in violazione dei principi di liceità, finalità e pertinenza e non eccedenza del trattamento** (art. 11, comma 1, lett. a), b) e d), del Codice⁶⁶). Disponeva quindi il blocco del trattamento dei dati personali ai sensi dell'art. 154, comma 1, lett. d) del Codice⁶⁷.

⁶³ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo II "Regole ulteriori per i soggetti pubblici", art. 18 C.P. "Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici", comma 2: "Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali".

⁶⁴ In Parte I "Disposizioni generali", Titolo I "Principi generali", art. 3 C.P. "Principio di necessità nel trattamento dei dati": "I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

⁶⁵ Si veda altresì *supra* pag. 17, quadro sintetico, parte relativa alle informazioni sul rendimento scolastico.

⁶⁶ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo I "Regole per tutti i trattamenti", art. 11 C.P. "Modalità del trattamento e requisiti dei dati": "1. I dati personali oggetto di trattamento sono: a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; (...) d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati (...)". Per il testo completo della norma vedi *supra*, nota n. 31, pag. 15.

⁶⁷ In Parte III "Tutela dell'interessato e sanzioni", Titolo II "L'Autorità", Capo I "Il Garante per la protezione dei dati personali", art. 154 C.P. "Compiti": "1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: (...) d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporre il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali; (...)".

- Decreto ministeriale M.I.U.R. 7 dicembre 2006, n. 305 (preceduto da parere del Garante del 16 marzo 2006 e newsletter n. 276 del 12 maggio 2006) – “Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del d.lgs. 196/2003, Codice in materia di protezione dei dati personali”- Argomento: dati sensibili e giudiziari trattati dalle istituzioni scolastiche

Si tratta di un provvedimento⁶⁸ importante, previsto dagli articoli 20 e 21 del d.lgs. 196/03 e più volte sollecitato dal Garante per la protezione della privacy, che specifica i tipi di dati che possono essere trattati dalla scuole, le operazioni che su di essi sono eseguibili e le finalità di rilevante interesse pubblico perseguite. In particolare, l'art. 20, secondo comma prevede che: “Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, **il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22**”⁶⁹, con atto di natura regolamentare adottato in conformità al parere espresso dal

⁶⁸ L'art. 1 del Regolamento (D.M. M.I.U.R. 305/2006) rubricato “Oggetto del Regolamento” dispone che: “Il presente regolamento, in attuazione degli articoli 20, comma 2, e 21, comma 2, del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali», di seguito denominato «codice», identifica nelle schede allegate, che ne formano parte integrante, le tipologie di dati sensibili e giudiziari e di operazioni indispensabili per la gestione del sistema dell'istruzione, nel perseguimento delle finalità di rilevante interesse pubblico individuate dal codice e dalle specifiche previsioni di legge”.

⁶⁹ In Parte I “Disposizioni generali”, Titolo III “Regole generali per il trattamento dei dati”, Capo II “Regole ulteriori per i soggetti pubblici”, art. 22 C.P. “Principi applicabili al trattamento di dati sensibili e giudiziari”:
“1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di

Garante ai sensi dell'articolo 154, comma 1, lettera g)⁷⁰, anche su schemi tipo". L'art. 21, secondo comma estende il disposto anche ai dati giudiziari stabilendo che: "Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari".

Il testo del Regolamento, molto snello ed essenziale, è suddiviso in 3 articoli nei quali si richiama il d.lgs. 196/03 e si sottolinea l'obbligo di trattare dati sensibili e giudiziari solo previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato (art. 2)⁷¹.

Sono parte integrante del Regolamento 7 schede⁷² (consultabili al link in nota), aggiornate con periodicità triennale, che individuano tutti i dati sensibili e giudiziari trattati dalle scuole, suddividendoli in ambiti. Ogni scheda consente alle scuole di individuare chiaramente i trattamenti consentiti, le finalità di rilevante interesse pubblico perseguite, le fonti normative, i soggetti esterni pubblici e privati a cui è possibile comunicare i dati, i tipi di dati trattati⁷³, la denominazione dei trattamenti. Le schede costituiscono una "guida obbligatoria" cui le scuole debbono attenersi, eventualmente anche rivedendo e modificando atti e procedimenti già adottati che non siano conformi con le prescrizioni in esse contenute.

Il suddetto regolamento è stato preceduto dal parere⁷⁴ favorevole (espresso in data 16 marzo 2006) e da una newsletter⁷⁵ del Garante (la n. 276 del 12 maggio 2006) nella quale viene sottolineato il

legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale".

⁷⁰ In Parte III "Tutela dell'interessato e sanzioni", Titolo II "L'Autorità", Capo I "Il Garante per la protezione dei dati personali", art. 154 C.P. "Compiti": "1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di: (...) g) esprimere pareri nei casi previsti".

⁷¹ In particolare, l'art. 2 del Regolamento (D.M. M.I.U.R. 305/2006) rubricato "Individuazione dei tipi di dati e di operazioni eseguibili" stabilisce che: "1. I dati sensibili e giudiziari individuati dal presente regolamento sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato. 2. Le operazioni di interconnessione e raffronto con banche di dati di altri titolari del trattamento e di comunicazione a terzi individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati e solo per il perseguimento delle rilevanti finalità di interesse pubblico specificate, le operazioni sopraindicate sono inoltre svolte nel rispetto delle disposizioni in materia di protezione dei dati personali e degli altri limiti stabiliti dalla legge e dai regolamenti. 3. I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie sono consentite soltanto previa verifica della loro stretta indispensabilità rispetto ai singoli casi e previa indicazione scritta dei motivi che ne giustificano l'effettuazione. Le operazioni effettuate utilizzando banche di dati di diversi titolari del trattamento e la diffusione di dati sensibili e giudiziari sono ammesse esclusivamente previa verifica della loro stretta indispensabilità in relazione ai singoli casi e nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono. 4. Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali".

⁷² E' possibile consultare le schede al seguente link:

www.normattiva.it/uri-res/N2Ls?urn:nir:ministero.pubblica.istruzione:decreto:2006-12-07;305!vig=.

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

⁷³ E' importante tenere presente il contesto in cui il trattamento si svolge: ad esempio per le operazioni propedeutiche di avvio dell'anno scolastico (scheda n. 4) non è consentito il trattamento dei dati relativi alle convinzioni filosofiche, che invece è consentito per la gestione del contenzioso e procedimenti disciplinari (scheda n. 2). O ancora: nella gestione del rapporto di lavoro (scheda n. 1), i dati idonei a rilevare l'adesione al sindacato possono essere trattati solo per operare la ritenuta sindacale e per l'esercizio dei diritti sindacali. Un trattamento per fini diversi sarebbe illegittimo.

⁷⁴ In particolare, nel **parere del 16 marzo 2006** il Garante evidenzia che il Ministero, le istituzioni scolastiche ed educative, gli istituti di alta formazione artistica, musicale e coreutica e gli istituti regionali di ricerca educativa, al pari degli altri soggetti pubblici, possono trattare i dati sensibili e giudiziari in base ad un'espressa disposizione di legge

particolare significato dell'adozione del regolamento stesso ai fini della tutela della riservatezza degli studenti: il Garante ha evidenziato come con questo atto vengano individuate e rese note informazioni riguardanti la salute, la sfera religiosa, quella politico-sindacale, l'origine razziale ed etnica che sono eventualmente trattate presso gli istituti scolastici e, soprattutto, per quali specifiche finalità. In base al Codice in materia di protezione dei dati personali per poter raccogliere, utilizzare e conservare per le loro attività istituzionali dati così delicati, le pubbliche amministrazioni devono adottare specifici atti regolamentari. Il regolamento del Ministero reca il **quadro generale di garanzie per la gestione scolastica dei dati che incidono in modo più significativo sulla sfera privata degli studenti**.

Nel regolamento viene chiarito, tra l'altro, che i dati sensibili degli studenti possono essere usati solo per specifiche finalità: i dati sulle origini etniche possono essere trattati solo per favorire l'inclusione degli alunni con cittadinanza non italiana; i dati relativi alle convinzioni religiose solo per garantire la libertà di credo religioso; i dati sulla salute solo per l'erogazione del sostegno agli alunni con disabilità, dell'insegnamento domiciliare e per il servizio di refezione; le informazioni sulle convinzioni politiche solo per la costituzione ed il funzionamento delle consulte e delle associazioni degli studenti e dei genitori; i dati di carattere giudiziario sono trattati solo per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione.

- Comunicato stampa Garante del 14 giugno 2005 - Argomento: tabelloni scolastici

In riferimento alla notizia relativa all'iniziativa di alcuni presidi degli istituti superiori di Cremona, dove sono stati affissi cartelli in cui si fa divieto di fotografare gli esiti finali degli allievi, l'ufficio stampa del Garante per la protezione dei dati personali precisa che **nessuna norma del Codice sulla protezione dei dati personali preclude la piena pubblicità degli scrutini scolastici, la possibilità di accesso ai luoghi dove essi sono esposti e di trarne notizia prendendo appunti per usi personali, eventualmente anche con foto**. Non si può utilizzare il Codice per precludere la piena pubblicità degli esiti finali: se poi vi fosse, a posteriori, un eventuale uso non corretto, questo sarebbe ovviamente verificabile. Inoltre, **i dati relativi agli esiti scolastici, per quanto riferiti a minori, non sono dati sensibili**, non riguardano cioè informazioni sullo stato di salute, le opinioni politiche, le appartenenze religiose, l'etnia o gli stili di vita, ma attengono esclusivamente al rendimento scolastico degli allievi.

- D.lgs. 76 del 15 aprile 2005 – “Definizione delle norme generali sul diritto-dovere all'istruzione e alla formazione, ai sensi dell'articolo 2, comma 1, lettera c) della legge 28 marzo 2003, n. 53” – Argomento: sistema nazionale delle anagrafi degli studenti

Per completezza espositiva e per le evidenti implicazioni che possono derivare rispetto alla normativa sulla privacy, nella presente trattazione, un cenno merita anche l'istituzione del **sistema nazionale delle anagrafi degli studenti**, previsto dal sopracitato decreto. Lo scopo di tale istituto è quello di una piena realizzazione del diritto-dovere all'istruzione e alla formazione attraverso la realizzazione di piani di intervento per l'orientamento, la prevenzione, il recupero degli abbandoni

nella quale siano specificati i tipi di dati, le operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite. In presenza di una disposizione primaria che si limiti a specificare solo la finalità di rilevante interesse pubblico, è necessario identificare e rendere pubblici, in un atto di natura regolamentare conforme al parere reso dal Garante, i tipi di dati sensibili o giudiziari, nonché le operazioni eseguibili in relazione alle finalità perseguite nei singoli casi, al fine di rendere legittimo il trattamento. A tale scopo, il Ministero è quindi tenuto ad adottare un atto di natura regolamentare conforme al parere reso dal Garante.

⁷⁵ Nella **newsletter del Garante n. 276 del 12 maggio 2006**, oltre a ribadire che le scuole devono avere la massima cura dei dati sensibili dei ragazzi e trattarli solo per scopi specifici, si rende noto che **le scuole devono anche dare riscontro alle richieste di accesso ai dati personali da parte delle famiglie**. Di recente il Garante ha infatti accolto il ricorso di due genitori che avevano chiesto di conoscere tutti i dati, propri e della figlia, contenuti nella documentazione in possesso dell'istituto scolastico frequentato dalla ragazza e ha imposto alla scuola di fornirli.

ed il contrasto alla dispersione scolastica e formativa. In particolare, all'art. 3⁷⁶ del decreto è stabilito che: *“(...) nel rispetto delle disposizioni del decreto legislativo 30 giugno 2003, n. 196, l'anagrafe nazionale degli studenti presso il Ministero dell'istruzione, dell'università e della ricerca opera il trattamento dei dati sui percorsi scolastici, formativi e in apprendistato dei singoli studenti a partire dal primo anno della scuola primaria, avvalendosi delle dotazioni umane e strumentali del medesimo Ministero”*. Ai sensi del successivo accordo integrativo è poi espressamente previsto all'art. 1 che: *“L'accesso ai dati personali dell'Anagrafe avvenga nel rispetto delle competenze attribuite dalla legge e dei principi di pertinenza, non eccedenza ed indispensabilità di cui al d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)”*.

- Comunicato stampa Garante del 3 dicembre 2004 - Argomento: falsità sulla privacy

Benché non recente, si ritiene opportuno richiamare nella presente trattazione il suddetto comunicato stampa contenente la secca smentita del Garante ad una serie di notizie del tutto infondate riguardanti la privacy nelle scuole. L'Autorità ribadisce che **non è vero che i voti scolastici devono restare segreti, non è vero che gli studenti devono “nascondere” la propria fede religiosa, non è vero che i risultati degli scrutini devono rimanere “clandestini”**. Trattasi di notizie che, nonostante le pronte e numerose precisazioni del Garante, sono spesso riportate anche da quotidiani a carattere nazionale, senza le necessarie verifiche.

In particolare, **non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe, delle interrogazioni o gli scrutini, né di consegnarli agli alunni in busta chiusa**. Mai, in nessun caso, un tale provvedimento è stato preso, né, tanto meno, esso è previsto dall'attuale legge in vigore, il Codice sulla privacy. **I risultati degli scrutini**, come già ricordato, **non sono, peraltro, dati sensibili, soggetti a speciali tutele**: devono essere al contrario pubblicati anche dopo l'avvento della normativa sulla privacy, essendo ciò previsto da una specifica disciplina in materia e rispondendo a principi di trasparenza. Anche i punteggi attribuiti come crediti scolastici a ciascun alunno sono pubblicati nell'albo degli istituti, unitamente ai voti conseguiti in sede di scrutinio finale. In ciascun albo va anche pubblicato l'esito degli esami, con la sola indicazione della dizione *non promosso* nel caso di esito negativo.

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

- Newsletter Garante del 15 aprile 2002 e decisione su ricorso del 10 aprile 2002 - Argomento: stop alla diffusione di dati relativi ad alunni disabili su internet

La newsletter richiama il provvedimento d'urgenza avente ad oggetto il blocco della diffusione di dati sanitari pubblicati sul sito *web* di un centro di documentazione didattica, che aveva sede presso la succursale di una scuola media statale. Alla segnalazione che lamentava, oltre la diffusione dei

⁷⁶ Ai sensi del 4° comma dell'art. 3 del d.lgs. 76/2005 è altresì previsto che: *“Con apposito accordo tra Ministero dell'istruzione, dell'università e della ricerca, Ministero del lavoro e delle politiche sociali, in sede di Conferenza unificata (...), è assicurata l'integrazione delle anagrafi di cui ai commi 1, 2 e 3 (ovvero anagrafe nazionale degli studenti, anagrafi regionali e anagrafi comunali) nel Sistema nazionale delle Anagrafi degli studenti”*. Successivamente, infatti, in sede di conferenza unificata del 16 dicembre 2010, viene adottato tale accordo (che coinvolge anche Regioni, Province e Comuni). Esso prevede, tra l'altro, per quanto di nostro interesse, che: *“(...) il Ministero è responsabile del processo di acquisizione dei dati relativi agli studenti del sistema nazionale di istruzione e della sua correttezza e completezza mentre le Regioni sono responsabili del processo di acquisizione dei dati degli studenti presenti nei percorsi di istruzione e formazione professionale e della sua correttezza e completezza”*.

nominativi degli alunni con disabilità, anche la descrizione dettagliata delle patologie sofferte da ciascuno di essi, ha fatto seguito l'accertamento preliminare eseguito dall'Ufficio del Garante. Dagli ulteriori accertamenti effettuati poi in sede di ispezione è emerso che, consultando la pagina Internet, accessibile attraverso il sito di un centro di documentazione scolastico, erano conoscibili, da chiunque, varie patologie di persone individuate nominativamente o appartenenti a classi, che venivano citate, di istituti scolastici. Nel provvedimento collegiale del 10 aprile 2002 che ha disposto il blocco dei dati, il Garante ha evidenziato la possibile violazione di diverse disposizioni della legge sulla privacy, ed in particolare dell'art. 23⁷⁷ che vieta la diffusione di informazioni sullo stato di salute degli interessati quando non sia necessaria per finalità di prevenzione, accertamento e repressione dei reati. Ritenendo, inoltre, necessario intervenire con urgenza, vista la particolare natura dei dati sanitari rilevati ed il concreto rischio che la permanenza sul sito di informazioni dettagliate potesse produrre un pregiudizio rilevante per gli alunni disabili, l'Autorità ha ordinato anche l'immediata rimozione dei dati dalla pagina web.

PARTE III

Cyberbullismo

Quadro sintetico

La rapida diffusione delle nuove tecnologie ha portato con sé nuove occasioni di incontro e interazione, oltre che stravolto le modalità di comunicazione, gli stili di vita, il modo di pensare, la divulgazione del sapere e della cultura. Tuttavia, accanto a queste opportunità di crescita e arricchimento culturale, i nuovi mezzi di comunicazione di massa portano con sé anche **rischi e pericoli** e i giovani, purtroppo, sono spesso volte i primi a dover fare i conti con l'aspetto maligno della grande Rete, della telefonia mobile, dei videogiochi.

Il pericolo più recente che si nasconde dietro uno schermo è il **cyberbullismo, o bullismo elettronico**, termine che indica un atto aggressivo, intenzionale, condotto da un individuo o un gruppo di individui usando varie forme di contatto elettronico, contro una vittima che non può facilmente difendersi. Sono considerati atti di bullismo elettronico l'invio di messaggi scortesi, offensivi, insultanti attraverso e-mail, sms, messaggi, telefonate sgradite o talvolta mute; la diffusione o pubblicazione *online* di materiale altamente offensivo e denigratorio, come, per esempio, immagini alterate o fotomontaggi della vittima; l'esclusione intenzionale di un coetaneo da un gruppo *online*, da una *chat*, da un *game* interattivo e da altri ambienti protetti da *password*, con lo scopo di determinarne una riduzione di collegamenti amicali, popolarità e quindi "potere"; l'ormai famoso fenomeno dell'*happy slapping*, in cui un ragazzo o un gruppo di ragazzi picchiano

⁷⁷ In Parte I "Disposizioni generali", Titolo III "Regole generali per il trattamento dei dati", Capo III "Regole ulteriori per privati ed enti pubblici economici", art. 23 C.P. "Consenso": "1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. 2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. 3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13. 4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili".

un coetaneo mentre altri riprendono con il videofonino l'aggressione, che verrà poi pubblicata in Internet, diventando, così, occasione di condivisione e derisione *online*⁷⁸.

Non c'è ancora in Italia una legge specifica per il bullismo, né per il cyberbullismo. Tuttavia è stato approvato all'unanimità il **disegno di legge 1261** rubricato "*Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo*"⁷⁹ comunicato alla Presidenza il 27 gennaio 2014 ed ora solo in attesa di essere discusso in aula.

⁷⁸ Nancy Willard, direttrice del Centro americano per l'utilizzo sicuro e responsabile di Internet (*Center for Safe and Responsible Internet Use*), ha individuato le seguenti tipologie di cyberbullismo: **flaming**, ovvero l'invio di messaggi *online* violenti e volgari mirati a suscitare battaglie verbali in un forum; **harassment (molestie)**, cioè la spedizione ripetuta di messaggi insultanti mirati a ferire qualcuno; **denigrazione** consistente nello sparlare di qualcuno per danneggiare gratuitamente e con cattiveria la sua reputazione, via e-mail, messaggistica istantanea, ecc...; **impersonation (sostituzione di persona)** consistente nel farsi passare per un'altra persona per spedire messaggi o pubblicare testi repressibili; **exposure (rivelazioni)**, cioè informazioni private e/o imbarazzanti su un'altra persona; **trickery (inganno)** consistente nell'ottenere la fiducia di qualcuno con l'inganno per poi pubblicare o condividere con altri le informazioni confidate via mezzi elettronici; **esclusione** di una persona da un gruppo *online* per provocare in essa un sentimento di emarginazione; **cyberstalking (cyber-persecuzione)**, ovvero le molestie e denigrazioni ripetute e minacciose, mirate a incutere paura.

Gli studi pubblicati sul fenomeno dimostrano che i cyberbulli credono di potersi nascondere dietro all'anonimato, pensano di essere invisibili, non identificabili, e per tale motivo di rimanere impuniti. Al contempo, nelle giovani vittime è molto radicata l'omertà, in quanto (pur essendo elevato il numero di bambini ed adolescenti che dichiara di essersi trovato coinvolto in episodi di bullismo online) è altamente improbabile che essi trovino il coraggio di parlarne con qualcuno. I giovani internauti hanno paura che, confidando l'accaduto, i genitori gli vietino l'accesso al web e, soprattutto, si sentono deboli, incapaci di difendersi, alimentando in loro un pericolosissimo senso di vergogna e d'inadeguatezza. Le conseguenze del cyberbullismo sono analoghe – se non maggiormente gravose a causa dell'elevato numero di persone coinvolte e della forza mediatica della pubblicazione di messaggi e foto sul web – a quelle del bullismo tradizionale. Tra gli effetti, più o meno gravi, la nascita di stati di depressione, ansie, paure, frustrazioni, bassa autostima, problemi scolastici e, nei casi più estremi, idee suicide. La loro pericolosità è da mettere in relazione non solo alla natura stessa degli attacchi, bensì alla possibile illimitata frequenza e permanenza in rete.

In tutti i casi di cyberbullismo, qualora si tratti di fatti illeciti commessi da minori capaci di intendere e di volere, la norma civilistica a cui bisogna fare riferimento è, senza alcun dubbio, l'**art. 2048 c. c.** (vedi nota n. 12 pag. 8). Come è noto, la norma stabilisce una presunzione di colpa dei genitori (o dei soggetti ivi indicati). La presunzione di responsabilità, posta a carico del genitore, per i danni causati dal figlio minore può, infatti, essere vinta solo con la prova di aver adempiuto tutti i doveri ed esercitato tutti i poteri idonei ad impedire l'illecita condotta del figlio. Al riguardo, la giurisprudenza è assolutamente costante nell'affermare che non basta dimostrare che il genitore non abbia potuto materialmente impedire il fatto, perché commesso fuori della sua sfera di azione; occorre infatti che egli dimostri di aver svolto nei riguardi del minore una vigilanza adeguata alla sua età, al suo carattere, alla sua indole e di avergli impartito un'educazione idonea in relazione alla sua personalità. In definitiva la responsabilità del genitore viene esclusa soltanto allorché lo stesso provi l'inevitabilità del fatto o l'esistenza di tutte le precauzioni (con riferimento alle circostanze concrete, compresa l'età e la personalità del minore) volte a impedire che il fatto potesse accadere. La responsabilità dei genitori *ex art. 2048 cod. civ.* si aggiunge a quella del figlio minore capace di intendere e di volere ma non la sostituisce trattandosi di responsabilità solidali tra loro.

⁷⁹ Si ritiene opportuno riportare le disposizioni del **d.d.l. 1261** – approvato all'unanimità ed in attesa di essere discusso in aula - rubricato "*Disposizioni a tutela dei minori per la prevenzione e il contrasto del fenomeno del cyberbullismo*": **art. 1:** "*Finalità e definizioni*": 1. La presente legge si pone l'obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione e tutela ai minori coinvolti, sia nella posizione di vittime sia in quella di responsabili di illeciti.

2. Ai fini della presente legge, per «cyberbullismo» si intende qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione e si intende altresì qualunque forma di furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica;

art. 2: "*Tutela della dignità del minore*": 1. Ciascun genitore o, comunque, il soggetto esercente la responsabilità del minore che abbia subito taluno degli atti di cui all'articolo 1, comma 2, della presente legge, può inoltrare al titolare del trattamento, una istanza per l'oscuramento, la rimozione o il blocco di qualsiasi altro dato personale del minore, diffuso nella rete internet, previa conservazione dei dati originali, anche qualora le condotte di cui all'articolo 1, comma 2, della presente legge, non integrino le fattispecie previste dall'articolo 167 del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, ovvero da altre norme incriminatrici.

Inoltre diverse norme di legge nel codice civile, penale e nella Costituzione puniscono i comportamenti dei bulli.

Tali condotte comportano *in primis* una **violazione dei principi costituzionali**⁸⁰ di uguaglianza, di libertà dell'insegnamento e di diritto all'istruzione, principi connessi al compito dello Stato di promuovere e favorire il pieno sviluppo della persona umana.

2. Qualora, entro le ventiquattro ore successive al ricevimento dell'istanza di cui al comma 1, il soggetto richiesto non abbia provveduto, o comunque nel caso in cui non sia possibile identificare il titolare del trattamento, l'interessato può rivolgere analoga richiesta, mediante segnalazione o reclamo, al Garante per la protezione dei dati personali, il quale, entro quarantotto ore dal ricevimento dell'atto, provvede ai sensi degli articoli 143 e 144 del citato codice di cui al decreto legislativo 30 giugno 2003, n. 196;

art. 3: "Piano di azione integrato": 1. Con decreto del Presidente del Consiglio dei ministri, da emanare entro trenta giorni dalla data di entrata in vigore della presente legge, è istituito presso la Presidenza del Consiglio dei ministri, senza nuovi o maggiori oneri per la finanza pubblica, il tavolo tecnico per la prevenzione e il contrasto del cyberbullismo, del quale fanno parte: rappresentanti del Ministero dell'interno, del Ministero dell'istruzione, dell'università e della ricerca, del Ministero del lavoro e delle politiche sociali, del Ministero della giustizia, del Ministero dello sviluppo economico, del Garante per l'infanzia e l'adolescenza, del Comitato di applicazione del codice di autoregolamentazione media e minori, del Garante per la protezione dei dati personali e delle organizzazioni non governative già coinvolte nel programma nazionale del Safer internet center.

2. Il tavolo tecnico di cui al comma 1 redige, entro sessanta giorni dal suo insediamento, un piano di azione integrato per il contrasto e la prevenzione del cyberbullismo, nel rispetto delle direttive europee in materia e nell'ambito del programma pluriennale dell'Unione europea di cui alla decisione 1351/2008/CE del Parlamento europeo e del Consiglio del 16 dicembre 2008.

3. Il piano di cui al comma 2 è integrato con il codice di autoregolamentazione per la prevenzione e il contrasto del cyberbullismo, rivolto agli operatori che forniscono servizi di social networking e agli altri operatori della rete. Detto codice prevede l'istituzione di un comitato di monitoraggio al quale è assegnato il compito di adottare un marchio di qualità in favore dei fornitori di servizi di comunicazione elettronica e comunque produttori di dispositivi elettronici aderenti ai progetti elaborati dallo stesso tavolo tecnico, secondo modalità disciplinate con il decreto di cui al comma 1 del presente articolo.

4. Il piano di cui al comma 2 stabilisce, altresì, le iniziative di informazione e di prevenzione del fenomeno del cyberbullismo, rivolte ai cittadini;

art. 4: "Linee guida per la prevenzione e il contrasto in ambito scolastico": 1. Per l'attuazione delle finalità di cui all'articolo 1, comma 1, il Ministero dell'istruzione, dell'università e della ricerca, emana entro trenta giorni dalla data di entrata in vigore della presente legge, linee guida per la formazione, la prevenzione e il contrasto del fenomeno del cyberbullismo nelle scuole, prevedendo che i corsi di formazione del personale scolastico, ai quali ogni autonomia scolastica assicura la partecipazione di un proprio referente, garantiscano l'acquisizione di idonee competenze teoriche e pratiche, anche per il sostegno ai minori vittime del cyberbullismo.

2. Gli uffici scolastici regionali garantiscono la promulgazione di bandi per il finanziamento di progetti di particolare interesse elaborati da reti di scuole in collaborazione con enti locali, servizi territoriali, Forze dell'ordine nonché associazioni ed enti per promuovere sul territorio azioni integrate di contrasto al cyberbullismo.

3. L'educazione all'uso consapevole della rete assume carattere di continuità curricolare tra i diversi ordini di scuola e in modo particolare tra la secondaria di primo grado e la secondaria di secondo grado, secondo quanto previsto dal decreto di cui al comma 1;

art. 5: "Rifinanziamento del fondo di cui all'articolo 12 della legge 18 marzo 2008, n. 48": 1. La Polizia postale e delle comunicazioni relaziona con cadenza semestrale al tavolo tecnico di cui all'articolo 3, comma 1, sugli esiti delle misure di contrasto al fenomeno del cyberbullismo con specifiche verifiche dei sistemi di segnalazione di cui all'articolo 2.

2. Per le esigenze connesse allo svolgimento delle attività di formazione in ambito scolastico e territoriale finalizzate alla sicurezza dell'utilizzo della rete e prevenzione e contrasto al cyberbullismo sono stanziati ulteriori risorse (...);

art. 6: "Ammonimento": 1. Fino a quando non è stata proposta querela o non è presentata denuncia per taluno dei reati di cui agli articoli 594, 595 e 612 del codice penale o 167 del codice di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196, commessi, mediante la rete internet, da minorenni di età superiore agli anni quattordici nei confronti di altro minorenne, è applicabile la procedura di ammonimento di cui all'articolo 8 del decreto-legge 23 febbraio 2009, n. 11, convertito, con modificazioni, dalla legge 23 aprile 2009, n. 38, e successive modificazioni".

⁸⁰ Il riferimento è, in particolare, all'**art. 3 della Costituzione** a mente del quale: "Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'uguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese";

Sono ravvisabili anche molteplici **reati penali**⁸¹ a seconda di come si manifesti il comportamento del bullo: percosse (art. 581 c.p.), lesioni (art. 582 c.p.), danneggiamento alle cose (art. 635 c.p.), ingiuria (art. 594 c.p.), diffamazione (art. 595 c.p.), molestia o disturbo alle persone (art. 660 c.p.), minaccia (art. 612 c.p.), atti persecutori o *stalking* (art. 612 bis c.p.), interferenze nella vita privata

all'art. 33 Cost., commi 1 e 2: “L'arte e la scienza sono libere e libero ne è l'insegnamento. La Repubblica detta le norme generali sull'istruzione ed istituisce scuole statali per tutti gli ordini e gradi” e all'art. 34 Cost., commi 1, 2 e 3: “La scuola è aperta a tutti. L'istruzione inferiore, impartita per almeno otto anni, è obbligatoria e gratuita. I capaci e meritevoli, anche se privi di mezzi, hanno diritto di raggiungere i gradi più alti degli studi”.

⁸¹ Il riferimento è ai seguenti reati: **percosse (art. 581 c.p.)**: “Chiunque percuote taluno, se dal fatto non deriva una malattia nel corpo o nella mente, è punito, a querela della persona offesa, con la reclusione fino a sei mesi o con la multa fino a euro 309. Tale disposizione non si applica quando la legge considera la violenza come elemento costitutivo o come circostanza aggravante di un altro reato”; **lesione personale (art. 582 c.p.)**: “Chiunque cagiona ad alcuno una lesione personale, dalla quale deriva una malattia nel corpo o nella mente, è punito con la reclusione da tre mesi a tre anni. Se la malattia ha una durata non superiore ai venti giorni e non concorre alcuna delle circostanze aggravanti previste negli articoli 583 e 585, ad eccezione di quelle indicate nel numero 1 e nell'ultima parte dell'articolo 577, il delitto è punibile a querela della persona offesa”; **danneggiamento (art. 635 c.p.)**: “Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui, è punito, a querela della persona offesa, con la reclusione fino a un anno o con la multa fino a euro 309 (...)”; **ingiuria (art. 594 c.p.)**: “Chiunque offende l'onore o il decoro di una persona presente è punito con la reclusione fino a sei mesi o con la multa fino a euro 516. Alla stessa pena soggiace chi commette il fatto mediante comunicazione telegrafica o telefonica, o con scritti o disegni, diretti alla persona offesa. La pena è della reclusione fino a un anno o della multa fino a euro 1.032 se l'offesa consiste nell'attribuzione di un fatto determinato. Le pene sono aumentate qualora l'offesa sia commessa in presenza di più persone”; **diffamazione (art. 595 c.p.)**: “Chiunque, fuori dei casi indicati nell'articolo precedente, comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a euro 2.065. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza o ad una autorità costituita in collegio, le pene sono aumentate”; **molestia o disturbo alle persone (art. 660 c.p.)**: “Chiunque, in un luogo pubblico o aperto al pubblico, ovvero col mezzo del telefono, per petulanza o per altro biasimevole motivo, reca a taluno molestia o disturbo è punito con l'arresto fino a sei mesi o con l'ammenda fino a euro 516”; **minaccia (art. 612 c.p.)**: “Chiunque minaccia ad altri un ingiusto danno è punito, a querela della persona offesa, con la multa fino a euro 1.032. Se la minaccia è grave o è fatta in uno dei modi indicati nell'articolo 339, la pena è della reclusione fino a un anno e si procede d'ufficio”; **atti persecutori (art. 612 bis c.p. inserito dal D.L. 23 febbraio 2009 n. 11)**: “Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a cinque anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita. La pena è aumentata se il fatto è commesso dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se il fatto è commesso attraverso strumenti informatici o telematici. La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona travisata. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale. La querela è comunque irrevocabile se il fatto è stato commesso mediante minacce reiterate nei modi di cui all'articolo 612, secondo comma. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio”; **interferenze nella vita privata (art. 615 c.p.)**: “Chiunque mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde, mediante qualsiasi mezzo di informazione al pubblico, le notizie o le immagini ottenute nei modi indicati nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa; tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato”; **sostituzione di persona (art. 494 c.p.)**: “Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica con la reclusione fino a un anno”.

(art. 615 c.p.), sostituzione di persona (art. 494 c.p.). Per attivare i rimedi previsti dalla legge penale è sufficiente, se il reato è perseguibile d'ufficio, sporgere denuncia ad un organo di polizia o all'autorità giudiziaria (questura, carabinieri, ecc...). Nella maggior parte dei casi, però, tali reati sono perseguibili a querela, ovvero con la richiesta da parte della vittima di procedere penalmente contro l'autore del reato. Il processo penale potrà concludersi con la condanna del colpevole alla reclusione o al pagamento di una pena pecuniaria o anche con altre sanzioni tra cui, in casi rari, l'ordine al colpevole di compiere determinate attività socialmente utili.

Quanto all'imputabilità del bullo minorenne occorre distinguere tra il minore di anni quattordici che non è mai imputabile penalmente, ma solo assoggettabile a misure di sicurezza (quali libertà vigilata o ricovero in riformatorio) se riconosciuto "socialmente pericoloso" ed il minore ultraquattordicenne che è imputabile se, secondo il giudizio del giudice che si avvale di consulenti professionali, viene ritenuto capace di intendere e di volere. Dal punto di vista civilistico, ai fini risarcitori, trova applicazione anche l'art. 2046 del c.c. che sancisce in tema di *"Imputabilità del fatto dannoso"* che: *"Non risponde delle conseguenze del fatto dannoso chi non aveva la capacità d'intendere o di volere al momento in cui lo ha commesso, a meno che lo stato d'incapacità derivi da sua colpa"*. Anche il minore pertanto, se ritenuto capace di intendere e volere, può essere ritenuto responsabile degli atti di bullismo insieme ai genitori ed alla scuola.

Nell'ipotesi di reati di bullismo compiuti a scuola è inoltre configurabile la responsabilità dell'insegnante il quale, nello svolgimento della sua attività professionale, ricopre la carica di pubblico ufficiale *ex art. 357 c.p.*⁸² ed è tenuto a denunciare all'Autorità Giudiziaria i reati di cui ha avuto notizia nell'esercizio o a causa delle sue funzioni (art. 361 c.p.⁸³).

Quanto, infine, alla **normativa civilistica**, il riferimento è all'art. 2043 c.c.: *"qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto obbliga colui che ha commesso il fatto a risarcire il danno"*. La vittima del bullismo, infatti, subisce un danno ingiusto (anche se non volontario) alla propria persona e/o alle proprie cose e pertanto tale danno è certamente risarcibile. In particolare, può essere risarcito: il danno morale (danno riguardante le sofferenze fisiche e morali, il dolore ed il turbamento dello stato d'animo della vittima); il danno biologico (danno riguardante la salute e l'integrità fisica e psichica della persona tutelati dalla Costituzione italiana all'art. 32); il danno esistenziale (danno riguardante la qualità della vita e la vita di relazione quantificato dal giudice in via equitativa).

In questi casi è ravvisabile anche la *culpa in educando e in vigilando*⁸⁴ dei genitori: il non esercitare una vigilanza adeguata all'età e indirizzata a correggere comportamenti inadeguati è, infatti, alla

⁸² L'art. 357 c.p. rubricato *"Nozione del pubblico ufficiale"* dispone che *"Agli effetti della legge penale, sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi"*.

⁸³ L'art. 361 c.p. rubricato *"Omessa denuncia di reato da parte del pubblico ufficiale"* statuisce che: *"Il pubblico ufficiale, il quale omette o ritarda di denunciare all'autorità giudiziaria, o ad un'altra autorità che a quella abbia obbligo di riferirne, un reato di cui ha avuto notizia nell'esercizio o a causa delle sue funzioni, è punito con la multa da euro 30 a euro 516 (...)"*.

⁸⁴ La giurisprudenza identifica la colpa del genitore non tanto nell'impedire il fatto ma nel comportamento antecedente allo stesso ovvero nella violazione dei doveri concernenti l'esercizio della potestà sanciti dall'art. 147 c.c.; quindi è il genitore che deve fornire la prova positiva di aver dato al figlio una buona educazione in conformità alle condizioni sociali, familiari, all'età, al carattere e all'indole del minore. Inoltre, la colpa del genitore non coabitante non esclude la responsabilità del genitore stesso laddove sia dimostrata la carenza di educazione del genitore e di rapporti non costanti con il discendente.

Ai sensi dell'art. 147 c.c. rubricato *"Doveri verso i figli"*: *"Il matrimonio impone ad ambedue i coniugi l'obbligo di mantenere, istruire, educare e assistere moralmente i figli, nel rispetto delle loro capacità, inclinazioni naturali e aspirazioni, secondo quanto previsto dall'articolo 315-bis"*. Secondo l'art. 315 bis c.c. rubricato *"Diritti e doveri del figlio"*: *"Il figlio ha diritto di essere mantenuto, educato, istruito e assistito moralmente dai genitori, nel rispetto delle sue capacità, delle sue inclinazioni naturali e delle sue aspirazioni. Il figlio ha diritto di crescere in famiglia e di mantenere rapporti significativi con i parenti. Il figlio minore che abbia compiuto gli anni dodici, e anche di età*

base della responsabilità civile dei genitori per gli atti illeciti commessi dal figlio minore che sia capace di intendere e di volere. Di tali atti non può, per legge, rispondere il minore, in quanto non ha autonomia patrimoniale. Pertanto, se i genitori del minore non dimostrino di non aver potuto impedire il fatto, saranno *ex art. 2048⁸⁵ c.c.*, primo comma, oggettivamente responsabili.

Infine, anche la *culpa in vigilando* della scuola⁸⁶ è da prendere in esame, sia ai sensi dell'art. 28 Cost⁸⁷, sia *ex art. 2048⁸⁸ c.c.*, secondo comma. Anche in tal caso a carico dei docenti è configurabile una responsabilità aggravata in quanto la presunzione di colpa può essere superata solamente laddove si dimostri di aver adeguatamente vigilato ovvero si dia la prova del caso fortuito.

Nella successiva parte di approfondimento verranno presi in esame i plurimi interventi del Presidente dell'Autorità Garante della Privacy Antonello Soro diretti ad una sensibilizzazione sul tema del cyberbullismo, nonché le più recenti pronunce giurisprudenziali in merito.

Approfondimento: casi pratici e normativa di riferimento

- Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali del 13 febbraio 2014 – Argomento: educazione digitale contro i cyberbulli

Il Garante evidenzia come in poco più di un decennio i *social network* abbiano trasformato radicalmente le relazioni ed il modo di comunicare, sottolinea come i giovani debbano essere consapevoli che non c'è differenza tra vita reale e mondo *on line* e che le nostre azioni in rete possono produrre effetti negativi anche per un tempo infinito: *“troppi ragazzi, insultati, discriminati, vittime di cyberbulli, soffrono, sono costretti a cambiare scuola o, nei casi più tragici, arrivano al suicidio. E quelli che oggi sembrano spavaldi sul web, un domani potrebbero fare i conti con un datore di lavoro che li selezioni sulla base del loro profilo facebook”*.

inferiore ove capace di discernimento, ha diritto di essere ascoltato in tutte le questioni e le procedure che lo riguardano. Il figlio deve rispettare i genitori e deve contribuire, in relazione alle proprie capacità, alle proprie sostanze e al proprio reddito, al mantenimento della famiglia finché convive con essa”.

⁸⁵ Vedi *supra* nota n. 14, pag. 9.

⁸⁶ Al riguardo si segnala la **sentenza n. 8081 del 7 giugno 2013 del Tribunale di Milano, sez. X civile**, che si colloca nella linea interpretativa della giurisprudenza italiana che sancisce la responsabilità del Ministero dell'Istruzione, Università e Ricerca, per culpa in vigilando, a causa delle lesioni patite nella scuola da un minore vittima di episodi di bullismo avvenuti durante l'orario scolastico. La sentenza in questione evidenzia come non sia affatto sufficiente per gli operatori della scuola “vigilare sul comportamento” dei ragazzi al fine di scongiurare episodi di violenza, perché il particolare rapporto che si crea con l'affidare alla scuola un minore concretizza l'evento regolato dall'art. 2048 c.c. per cui, in caso di danno al minore stesso, la responsabilità risarcitoria sarà piena ogni volta, e potrà essere esclusa solo dalla dimostrazione di aver adottato misure preventive tali da poter considerare l'evento occorso come un elemento “straordinario” che ha superato la stessa “prevenzione”. La sentenza sarà approfondita *infra* a pag. 46.

Come evidenziato dalla giurisprudenza costante della Cassazione, ed in particolare dalla **sentenza n. 2657 del 21 febbraio 2003, sez. III Cassazione**, per superare la presunzione, la scuola dovrebbe dimostrare di adottare “misure preventive” atte a scongiurare situazioni anti-giuridiche: l'organo giudicante sancisce, infatti, come “non sia sufficiente la sola dimostrazione di non essere stati in grado di spiegare un intervento correttivo o repressivo, ma è necessario anche dimostrare di aver adottato, in via preventiva tutte le misure disciplinari od organizzative idonee ad evitare il sorgere di situazioni pericolose”. Nel caso di specie, un alunno delle scuole elementari di Roma, durante le ore di lezione, subiva lesioni al dito indice della mano destra. La madre del minore, conveniva pertanto in giudizio, per il risarcimento, il M.I.U.R., che il Tribunale di Roma condannava al pagamento di L. 17.000.000, oltre agli interessi, a titolo di danno biologico. La Corte d'Appello rigettava il gravame e la Cassazione respingeva il ricorso del Ministero evidenziando, tra l'altro, che il dovere di vigilanza dell'insegnante debba essere commisurato all'età e al grado di maturazione raggiunto dagli allievi in relazione alle circostanze del caso concreto.

⁸⁷ L'art. 28 Cost. dispone che: *“I funzionari ed i dipendenti dello Stato e degli enti pubblici sono direttamente responsabili, secondo le leggi penali, civili ed amministrative, degli atti compiuti in violazione di diritti. In tali casi la responsabilità civile si estende allo Stato ed agli enti pubblici”*.

⁸⁸ Vedi *supra* nota n. 14, pag. 9.

Alla domanda se *web* e tutela della riservatezza possano procedere insieme per creare una società migliore, Soro risponde: *“lo sforzo del Garante va proprio in questa direzione. Quest’anno in occasione della Giornata europea della protezione dati abbiamo proposto di introdurre come materia di insegnamento nelle scuole di base l’educazione digitale, una sorta di rinnovata ed evoluta educazione civica che sensibilizzi i giovani ad un uso consapevole dei social network e, soprattutto, all’importanza del rispetto degli altri: è un obiettivo ambizioso ma necessario. Lo sforzo per proteggere la “persona digitale” deve riguardare tutti: le istituzioni, gli educatori e gli operatori sono chiamati a misurarsi insieme con le sfide poste da questa complessa fase di evoluzione sociale e tecnologica e a dare risposte adeguate”*.

- **Giornata europea della protezione dei dati personali del 29 gennaio 2014⁸⁹ – Argomento: educare alla rete. L’alfabeto della nuova cittadinanza nella società digitale**

Trattasi di una iniziativa promossa dal Consiglio d’Europa con il sostegno della Commissione Ue e di tutte le Autorità europee per la protezione dei dati personali. L’obiettivo della Giornata europea è stato quello di sensibilizzare i cittadini sui diritti legati alla tutela della riservatezza, della dignità della persona e delle libertà fondamentali, promuovendo “l’educazione della persona digitale”, una sorta di nuova educazione civica, rivolta a tutti i cittadini, agli operatori, agli utenti della Rete senza distinzione di età o di ruoli. L’esigenza di assicurare un uso legittimo dei dati che circolano nella rete e l’impegno a favorire e diffondere una piena consapevolezza delle potenzialità ma anche dei rischi nell’utilizzo dei moderni strumenti di comunicazione rappresentano - come sottolinea il Presidente della Camera dei Deputati Laura Boldrini - i due profili su cui le istituzioni preposte e i soggetti operanti nel settore devono necessariamente trovare un punto di incontro e di sintesi.

Passando all’intervento del Garante per la Privacy, Antonello Soro evidenzia come ormai *“la nostra vita ha trovato nelle tecnologie digitali strumenti per esprimere nuove esigenze alle quali è impossibile ed irrealistico rinunciare. La materialità delle cose si è ridotta: la maggior parte delle attività – dalle amicizie, allo scambio di semplici pensieri, agli spostamenti – si è smaterializzata dando luogo ad una produzione massiccia di dati che circolano, in modo incessante, attraverso la Rete. La rivoluzione digitale che trasforma in dati parti sempre più rilevanti delle nostre vite private propone problemi nuovi per le nostre libertà. Perché nello spazio digitale si possono violare le nostre persone, si possono negare i diritti, si possono manipolare o perfino rubare informazioni che riguardano strettamente aspetti fondamentali della nostra esistenza, che coincidono con la nostra vita”*. Il Garante prosegue sottolineando che *“se un’esperienza millenaria ci ha trasmesso ed insegnato la necessità di proteggere e tutelare i beni materiali, dobbiamo riconoscere che siamo ancora inesperti e privi di adeguate capacità di fronte ai lati oscuri dello spazio digitale. Gli hacker che, attraverso virus o codici, forzano i sistemi di sicurezza per accedere alle banche dati o ai siti protetti sono ladri esattamente come coloro che utilizzano il grimaldello per aprire la porta blindata. Il furto dell’identità digitale o di un profilo Facebook reca alla vittima un danno anche maggiore rispetto alla sottrazione del portafoglio o di un’agenda personale. Ed ancora: forme di monitoraggio continuo in Rete non sono semplicemente un fastidio e una inammissibile invadenza, ma armi puntate contro di noi; i dati digitali tracciati, controllati,*

⁸⁹ La “Giornata europea della protezione dei dati personali” è un’iniziativa promossa dal Consiglio d’Europa con il sostegno della Commissione europea e di tutte le Autorità europee per la protezione dei dati personali e che, a partire dal 2007, si celebra in tutta Europa il 28 gennaio. Nel corso della medesima giornata organizzata per l’anno precedente (2013), il Garante per la protezione dei dati personali aveva già deciso di affrontare il delicatissimo problema del cyberbullismo, chiamando a discuterne insieme il mondo della scuola e quello dei *social network*. Il tema era stato trattato nell’ambito della trasmissione “Uno Mattina” della Rai con la partecipazione del Presidente dell’Autorità Garante Antonello Soro, dell’allora Ministro della Pubblica Istruzione, Università e Ricerca Francesco Profumo e di un responsabile di Google per l’Italia.

archiviati possono al momento opportuno essere utilizzati per danneggiarci. Occorre trovare nuove forme per tutelare la persona nella sua unicità tra vita fisica e vita digitale. Così come nutriamo una legittima aspettativa di integrità e sicurezza quando ci muoviamo nello spazio fisico, dove esistono regole, leggi, consuetudini, mezzi di tutela per prevenire situazioni di pericolo e rimuovere ostacoli al libero dispiegarsi della nostra personalità, allo stesso modo deve essere presidiato lo spazio digitale, nel quale si svolge una parte rilevante delle nostre vite e che, dunque, non può essere affidato all'arbitrio di chi quello spazio conquista. Proteggere il flusso di dati con i quali comunichiamo, e dunque, "viviamo", significa proteggere noi stessi e le nostre esistenze".

Il Garante conclude evidenziando le implicazioni giuridiche del progresso tecnologico: *"la rivoluzione digitale attacca e scompagina le tradizionali categorie giuridiche. Ma non possiamo permettere che gli eventi ci soverchino e che inerzia e situazioni di fatto favoriscano l'oblio del diritto. Dobbiamo sfuggire due tentazioni estreme e opposte: da una parte quella di una inutile e stupida tecnofobia, la fuga dall'innovazione, l'idea apocalittica che attribuisce alla Rete la colpa di tutti i mali della modernità e, dall'altra, la rinuncia rassegnata a contrastare le distorsioni del sistema, a ricercare una qualche regolazione dei processi globali che presiedono alla comunicazione elettronica e più in generale a vivere responsabilmente il nostro tempo".*

"La risposta va trovata, auspicabilmente in una dimensione sovranazionale. Per questo è di estrema importanza la Risoluzione approvata nel novembre 2013 dall'ONU proprio sul tema della "Privacy nell'era digitale" con la quale si invitano gli Stati membri ad operare per prevenire le violazioni del "diritto umano alla privacy" e si sottolinea la necessità che nel mondo online i diritti debbano godere della identica tutela offerta loro nel mondo reale. Nella stessa prospettiva, anche le Autorità garanti per la protezione dei dati del mondo, riunite nella 35ma Conferenza internazionale di Varsavia, hanno adottato una specifica Risoluzione proprio sulla promozione dell'educazione digitale. L'obiettivo è quello di impegnare i Governi affinché venga assicurata particolare protezione ai minori e garantita una formazione permanente degli educatori sui rischi della tecnologia, che deve sempre promuovere il rispetto degli utenti. Un'adeguata protezione dei dati si pone dunque come garanzia ineludibile per scongiurare il pericolo che le nuove tecnologie, indispensabili nel semplificare l'attività dei singoli individui, agevolare lo scambio di informazioni e conoscenza, migliorare la vita di relazione, si traducano in strumenti perversi e potenzialmente lesivi".

- Codice di autoregolamentazione per la prevenzione ed il contrasto del cyberbullismo dell'8 gennaio 2014 - Argomento: cyberbullismo

Si ritiene opportuno proseguire il presente approfondimento esaminando anche questo atto, ancora in fase di elaborazione. Proprio per prevenire e contrastare le nuove forme di bullismo, che possono avere un impatto fortissimo su vittime spesso molto giovani, è stata approvata l'8 gennaio 2014 la prima bozza del Codice di Autoregolamentazione sul cyberbullismo, alla cui stesura hanno collaborato Ministero dello Sviluppo Economico, Autorità per le garanzie nelle comunicazioni, Polizia postale e delle comunicazioni, Direzione Centrale della Polizia Criminale, Autorità per la privacy, Garante per l'infanzia e Comitato media e minori, Associazioni (Confindustria digitale, Assoprovider) e operatori (Google, Microsoft). Nella bozza, il cyberbullismo viene definito come l'insieme di atti di bullismo e di molestia effettuati tramite mezzi elettronici come l'e-mail, la messaggistica istantanea, i blog, i telefoni cellulari e/o i siti web posti in essere da un minore, singolo o in gruppo, che colpiscono o danneggiano un proprio coetaneo incapace di difendersi.

Nell'articolo 1, gli operatori che forniscono servizi di *social networking*, i fornitori di servizi *on line*, di contenuti, di piattaforme e *social network* che aderiscono al Codice, si impegnano ad attivare appositi meccanismi di segnalazione di episodi di cyberbullismo, al fine di prevenire e contrastare il proliferare del fenomeno. La bozza del Codice è stata di recente messa a consultazione pubblica per ottenere ulteriori suggerimenti dagli utenti del *web*.

Il caso riguarda un video immesso per la successiva diffusione a mezzo Internet sul sito www.video.google.it, raffigurante un soggetto con sindrome di Down che viene preso in giro con frasi offensive e azioni vessatorie riferite alla sua sindrome da parte di altri soggetti minorenni.

La condotta contestata consiste, in particolare, nell'aver omesso un'informativa sulla privacy, visualizzabile in italiano dalla pagina iniziale del servizio Google video, in sede di attivazione del relativo *account*, al fine di porre in essere l'*upload* di *file*, in ordine a quanto prescritto dal comma 1 dell'art. 13 C.P. e, per esso, del valido consenso di cui all'art. 23, comma 3 C.P.⁹⁰. La violazione ipotizzata investe anche l'art. 26 C.P.⁹¹, riguardando dati idonei a rivelare lo stato di salute della persona inquadrata nel video e l'art. 17 C.P.⁹², per i rischi specifici insiti nel tipo di trattamento omesso, anche in relazione alle concrete misure organizzative da prestare.

Con sentenza del 21 dicembre 2012, la Corte d'Appello di Milano ha riformato, per la parte che qui rileva, la sentenza impugnata, evidenziando che l'art. 167 C.P.⁹³, non richiamando il precedente art. 13, non impone all'Internet *provider* di rendere edotto l'utente circa l'esistenza e i contenuti della legislazione sulla privacy. Infatti, l'eventuale violazione del citato art. 13, consistente nell'omessa o inidonea informativa all'interessato, viene punita non dall'art. 167, bensì dal precedente art. 161⁹⁴, che prevede una sanzione amministrativa. Nella stessa sentenza si esclude, inoltre, la configurabilità di un concorso omissivo nel reato contestato. Si esclude, altresì, la sussistenza del dolo specifico richiesto dalla disposizione incriminatrice, sul rilievo che gli imputati non erano preventivamente a conoscenza del filmato e dell'immissione del dato personale illecitamente trattato e sull'ulteriore rilievo della incompatibilità giuridica di detto dolo specifico col dolo eventuale individuato dal Tribunale in capo agli imputati.

Quest'ultima sentenza è stata impugnata, con ricorso per cassazione, dal Procuratore generale della Repubblica presso la Corte d'Appello di Milano, rilevando l'erronea applicazione dell'art. 26 C.P. e della normativa sul commercio elettronico *ex d.lgs. 70/2003*, nonché l'inosservanza degli artt. 167, 13, 23 e 4, del d.lgs. n. 196 del 2003, oltre alla mancanza e alla manifesta illogicità della motivazione.

La Corte di Cassazione respinge il ricorso rilevando la complessità e la novità delle questioni trattate e fissando alcuni punti fermi sul reato di trattamento illecito dei dati. In particolare, evidenzia che, essendo il concetto di trattamento assai ampio - configurandosi in qualunque operazione di utilizzazione e diffusione dei dati - esso può consistere anche in una rappresentazione fotografica o in una ripresa video. In punto responsabilità, la Cassazione precisa che essa ricade unicamente su chi ha realizzato e caricato in rete il video, in violazione del divieto di diffusione dei dati idonei a rivelare lo stato di salute (dato sensibile) di un persona; nessuna

⁹⁰ L'art. 23 C.P. "Consenso" è già stato riportato *supra* nella nota n. 77, pag. 35 e l'art. 13 C.P. "Informativa" nella nota n. 7, pag. 5.

⁹¹ Per l'art. 26 C.P. "Garanzie per i dati sensibili" si veda la nota n. 58, pag. 28.

⁹² Per l'art. 17 C.P. "Trattamento che presenta rischi specifici" si veda la nota n. 13, pag. 8.

⁹³ In Parte III "Tutela dell'interessato e sanzioni", Titolo III "Sanzioni", Capo II "Illeciti penali", art. 167 C.P. "Trattamento illecito di dati": "1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi. 2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".

⁹⁴ In Parte III "Tutela dell'interessato e sanzioni", Titolo III "Sanzioni", Capo I "Violazioni amministrative", art. 161 C.P. "Omessa o inidonea informativa all'interessato": "1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da seimila euro a trentaseimila euro. Si veda anche la nota n. 22, pag. 11.

responsabilità invece è configurabile a carico del fornitore di servizi (*host provider*: nel caso in oggetto la piattaforma Google Video, che si è limitata ad “ospitare” il filmato), a meno che, essendo venuto a conoscenza del dato sensibile contenuto nel video caricato dagli utenti, non abbia immediatamente provveduto a rimuovere le informazioni o disabilitarne l'accesso su comunicazione delle autorità competenti.

La Cassazione, nel ricostruire il quadro normativo applicabile al caso di specie, richiama il decreto legislativo 70/2003⁹⁵, per il quale **il prestatore di un servizio di hosting (servizio che consiste nel memorizzare informazioni fornite da altri) non è tenuto ad un obbligo generale di sorveglianza sulle informazioni che trasmette** (artt. 16 e 17)⁹⁶, né sui dati immessi da terzi sul sito da lui gestito. Neppure sussiste in capo al *provider* alcun obbligo sanzionato penalmente di informare il soggetto che ha immesso i dati dell'esistenza e della necessità di fare applicazione della normativa relativa al trattamento dei dati stessi.

Sulla base di queste considerazioni, i manager di Google Italia sono stati quindi scagionati da ogni accusa relativa al reato di trattamento illecito dei dati. **La persona che può essere chiamata a rispondere delle violazioni delle norme sulla protezione dei dati è, infatti, sempre il titolare del trattamento e non il mero hosting provider: gli unici titolari del trattamento dei dati sensibili eventualmente contenuti nei video caricati su un sito sono quindi gli stessi utenti che li hanno caricati, ai quali soli possono essere applicate le sanzioni, amministrative e penali, previste per il titolare del trattamento dal Codice Privacy.**

- Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali del 17 settembre 2013 e dichiarazione del 14 settembre 2013 – Argomento: smartphone, tablet, minorenni suicidi a causa del cyberbullismo

Il Garante, intervistato sulle classi 2.0, annuncia nuove norme contro il cyberbullismo e per l'uso consapevole del *web*, auspicando che possa diventare una materia di studio. In particolare, alla domanda se *tablet* e *smartphone* a scuola possano costituire più un'opportunità o un rischio per la privacy, risponde che: **“nuove tecnologie e web rappresentano ormai una realtà con cui fare i conti anche nell'ambito dell'attività scolastica. Smartphone e tablet sono utili, ad esempio, per registrare**

⁹⁵ Trattasi del **d.lgs. 9 aprile 2003, n. 70** “Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico”.

⁹⁶ L'**art. 16** del **d.lgs. 70/2003** prevede che: “1. Nella prestazione di un servizio della società dell'informazione, consistente nella memorizzazione di informazioni fornite da un destinatario del servizio, il prestatore non è responsabile delle informazioni memorizzate a richiesta di un destinatario del servizio, a condizione che detto prestatore: a) non sia effettivamente a conoscenza del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illiceità dell'attività o dell'informazione; b) non appena a conoscenza di tali fatti, su comunicazione delle autorità competenti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso. 2. Le disposizioni di cui al comma 1 non si applicano se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore. 3. L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse”.

Il successivo **art. 17** rubricato “Assenza dell'obbligo generale di sorveglianza” dispone che: “Nella prestazione dei servizi di cui agli articoli 14, 15 e 16, il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite. 2. Fatte salve le disposizioni di cui agli articoli 14, 15 e 16, il prestatore è comunque tenuto: a) ad informare senza indugio l'autorità giudiziaria o quella amministrativa avente funzioni di vigilanza, qualora sia a conoscenza di presunte attività o informazioni illecite riguardanti un suo destinatario del servizio della società dell'informazione; b) a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite. 3. Il prestatore è civilmente responsabile del contenuto di tali servizi nel caso in cui, richiesto dall'autorità giudiziaria o amministrativa avente funzioni di vigilanza, non ha agito prontamente per impedire l'accesso a detto contenuto, ovvero se, avendo avuto conoscenza del carattere illecito o pregiudizievole per un terzo del contenuto di un servizio al quale assicura l'accesso, non ha provveduto ad informarne l'autorità competente”.

le lezioni o per fare ricerche. Ma non devono trasformarsi in strumenti di offesa usandoli per diffondere sulla rete video e foto che possono ledere la dignità di compagni o insegnanti". In ogni caso: "spetta agli istituti scolastici decidere nella loro autonomia come regolamentare l'uso di questi dispositivi".

Alla richiesta su quale ruolo possa svolgere la scuola per aiutare i ragazzi a non correre rischi in rete, il Garante risponde che: "esiste una "vita digitale" dei nostri giovani che richiede oramai una educazione specifica. L'educazione digitale dovrebbe diventare una materia di studio fin dalle elementari. La scuola si trova di fronte ad un compito fondamentale: quello di promuovere, insieme a famiglie e istituzioni, la conoscenza delle opportunità e dei pericoli che si corrono in rete e dei danni che si possono provocare. E' una sfida alla quale nessuno può sottrarsi. Il Garante privacy, da parte sua, ha realizzato una campagna di informazione rivolta ai giovani per sensibilizzarli ad un uso consapevole del web, a partire dai social network. E sta lavorando ad iniziative sul tema del cyberbullismo, anche in collaborazione con il M.I.U.R."

Interpellato, infine, sui casi di minorenni suicidi a causa del cyberbullismo, evidenzia che "il cyberbullismo è un fenomeno gravissimo e per certi versi aberrante contro il quale dobbiamo impegnare tutte le nostre forze. E' necessario lavorare per rafforzare la cultura del rispetto dell'altro, far capire ai nostri ragazzi che le offese, gli insulti, le derisioni e le minacce in rete sono molto più gravi ed hanno effetti molto più devastanti di quelli portati per strada. Una violenza non soltanto "virtuale", spesso favorita dall'anonimato consentito da alcuni social network. Occorre far capire ai giovani che i nuovi rivoluzionari strumenti di comunicazione in rete, così popolari tra loro, non possono trasformarsi in vere e proprie armi". "Armi - continua il Garante privacy - che hanno un potenziale offensivo terribile e da cui non tutti sono in grado di difendersi. Basti pensare che l'ultimo gravissimo caso di suicidio di una ragazzina inglese è avvenuto proprio dopo gli insulti su un social network".

- Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali del 22 marzo 2013 – Argomento: uso responsabile dei social network, episodio di omofobia

Antonello Soro prende spunto dal cyber-blitz al liceo classico "Omissis" per rilanciare una battaglia di civiltà: sulla pagina Facebook "Spotted" gli studenti del liceo di "Omissis" schedavano e insultavano gli studenti omosessuali della propria scuola. Nomi, cognomi, dettagli sulle frequentazioni, parentele e insinuazioni: l'ennesimo episodio di omofobia.

Interpellato in merito, il Garante, evidenzia che: "dobbiamo aiutare i ragazzi a un uso responsabile del web con la leva delle famiglie e della scuola, con nuove leggi di tutela, col sostegno dei media, con un confronto che assicuri più protezioni collettive ma non limiti la libertà". Ricorda quanto sia importante per tutti, in particolare per le nuove generazioni, servirsi dei social network senza ingerenze nella sfera privata. E da presidente dell'Autorità di garanzia sulla protezione dei dati personali indica gli strumenti che giudica più opportuni per raggiungere maggiori consapevolezze: "i giovani devono poter frequentare le piazze mediatiche in maniera da non nuocere a se stessi e agli altri. Vanno abituati a conoscere davvero gli strumenti che abitualmente usano ma di cui spesso ignorano i pericoli. Si può raggiungere il traguardo unendo gli sforzi per assicurare rispetto in una terra incognita quale si rivela spesso internet. E dato che la fragilità dei ragazzi è accentuata dalle sfide tecnologiche che stanno cambiando il nostro modo di essere, sono diversi i campi d'azione possibili. Partiamo dalla vicenda di "Omissis". Intanto è stato evidente come la componente omofoba sia stata subito isolata dall'opinione pubblica e dagli stessi studenti". La reazione della scuola, infatti, preside compreso, non si era fatta attendere: indignati, studenti e docenti avevano condannato immediatamente quanto successo e indetto tempestivamente un'assemblea straordinaria.

"Ma contro il bullismo elettronico" - prosegue Soro - "crescente e più pericoloso di quello che conoscevano sino a qualche anno fa, bisognerà che i genitori si facciano coinvolgere di più. Controllando l'attività su internet dei figli, soprattutto nella fascia d'età tra i 7 e i 12 anni. Allo

stesso tempo mi pare necessario che le istituzioni scolastiche si attivino a fondo mettendo in guardia tutti dai rischi di un utilizzo sbagliato della rete (...). A essere esposti infatti sono soprattutto i giovanissimi, spesso lasciati soli davanti al computer da padri e madri, disinformati e inconsapevoli dei pericoli che si possono trovare sul web”.

Alla richiesta se il cyberbullismo debba essere considerato più devastante di quello tradizionale, Antonello Soro risponde: *“il linguaggio in rete, generato di frequente dagli adulti, è di per sé tutt’altro che sereno. Appare spesso aggressivo, liquidatorio. E anche col bullismo elettronico si crea sul web una memoria estesa delle cose che si scrivono, sempre visibili a distanza di anni. Inoltre, l’assenza di contatti personali produce un discredito privo di freni inibitori. La vittima tutte le volte che usa il suo tablet può rileggere all’infinito le frasi con le quali è stata colpita. Questo fenomeno può provocare in qualche caso gesti estremi. Insomma, siamo in presenza di una violenza incommensurabilmente maggiore del bullismo tradizionale”.*

- Sentenza n. 8081 del 7 giugno 2013 – Tribunale di Milano, Sez. X Civile – Argomento: episodi di bullismo avvenuti durante l’orario scolastico e culpa in vigilando del docente

Poco attinente al tema della privacy, ma interessante sotto il profilo del bullismo è la sentenza citata che evidenzia la rilevanza della responsabilità per *culpa in vigilando* del docente qualora si verificano a carico di un minore lesioni derivanti da episodi di bullismo perpetratisi durante l’orario scolastico. Nel caso di specie, il Tribunale di Milano ha condannato il M.I.U.R. a risarcire 10.000 euro per danni morali patiti da un adolescente vittima di bullismo a scuola.

L’organo giudicante ribadisce che la scuola e la pubblica amministrazione sono responsabili nel “tempo” dell’affidamento dell’allievo al precettore (*ex art. 2048 c.c.*) e, se si verifica un evento che causi un danno al primo, sorgerà una responsabilità risarcitoria a carico del docente. La sentenza in questione evidenzia come non sia affatto sufficiente per gli operatori della scuola “vigilare sul comportamento” dei ragazzi al fine di scongiurare episodi di violenza, perché il particolare rapporto che si crea con l’affidare alla scuola un minore concretizza l’evento regolato dall’art. 2048 c.c. per cui, in caso di danno al minore stesso, la responsabilità risarcitoria sarà piena ogni volta, e potrà essere esclusa solo dalla dimostrazione di aver adottato misure preventive tali da poter considerare l’evento occorso come un elemento “straordinario” che ha superato la stessa “prevenzione”⁹⁷.

⁹⁷ Altra pronuncia interessante in tema di responsabilità dei docenti e dell’istituzione scolastica è la **sentenza n. 1769 del 17 gennaio 2012, Corte di Cassazione, sez. III civile**. Nel caso di specie la Suprema Corte doveva, in particolare, stabilire le eventuali responsabilità per un danno subito da una minore sedicenne che, durante una gita scolastica, dopo avere scavalcato un parapetto, cadeva dalla terrazza, priva di protezioni, posta a livello del balcone della stanza al secondo piano dell’albergo, in cui alloggiava con altri compagni. Precedentemente la **Corte d’Appello di Trieste con sentenza n. 375/2009** aveva escluso la responsabilità del docente statuendo che: *“la sorveglianza del docente non doveva spingersi ad invadere la “privacy” dei ragazzi e la sua diligenza al controllo del non possesso di spinelli o alla verifica dell’astratta sicurezza delle strutture ospitanti, aperte al largo pubblico e nella fattispecie utilizzate da una scolaresca di ragazzi prossimi alla maggiore età e presumibilmente dotati di un senso del pericolo”*. Tre anni dopo, tale assunto veniva rimesso in discussione dalla Cassazione con la sentenza sopracitata. Con riferimento alla posizione dell’istituto scolastico, i giudici della Suprema Corte, infatti, stabiliscono che **“la responsabilità dell’istituto scolastico e dell’insegnante non ha natura extracontrattuale, bensì contrattuale, atteso che – quanto all’istituto scolastico – l’accoglimento della domanda di iscrizione, con la conseguente ammissione dell’allievo a scuola, determina l’instaurazione di un vincolo negoziale, dal quale sorge l’obbligazione di vigilare sulla sicurezza e l’incolumità dell’allievo nel tempo in cui questi fruisce della prestazione scolastica in tutte le sue espressioni** (Cass. 15 febbraio 2011, n. 3680) **ed è onere della scuola dimostrare in concreto, benché anche solo per presunzioni, che le lesioni sono state conseguenza di una sequenza causale ad essa non imputabile (tra le ultime Cass. 3 marzo 2010, n. 5067; Cass. 3 febbraio 2011, n. 2559; Cass. 20 aprile 2011, n. 9325), se non anche (come si esprime Cass. 9542 del 2009) quella di aver adottato, in via preventiva, le misure organizzative e disciplinari idonee ad evitare prevedibili situazioni di pericolo favorevoli all’insorgere della serie causale sfociante nella produzione del danno.** Tali principi vanno applicati alla particolare fattispecie dello svolgimento di una gita scolastica o viaggio di istruzione: la prestazione di vigilanza dell’istituto, come in concreto espletata dai professori accompagnatori, assume connotati particolari: di certo, il carattere continuo del contatto con gli studenti durante l’intera giornata, comprendente quindi le normali attività quotidiane e proprie della sfera di riservatezza più intima dell’individuo, impone di limitare l’entità e le stesse

Trattandosi di docenti di una scuola pubblica, precisa il Tribunale - la responsabilità si estende alla pubblica amministrazione in virtù del principio organico ai sensi dell'art. 28 della Costituzione che da una parte ravvisa la responsabilità *in proprio* dei pubblici dipendenti che agiscono quali organi della pubblica amministrazione, dall'altra afferma la responsabilità della stessa pubblica amministrazione per gli atti illeciti da loro commessi che ha natura *diretta* in virtù del cosiddetto rapporto organico che immedesima l'attività degli organi con quella dell'ente pubblico.

- **Sentenza n. 13010 del 6 febbraio/28 maggio 2013 – Corte di Cassazione, Sez. V Penale – Argomento: cyberbullismo e diritto di querela; prevalenza della volontà del genitore di sporgere querela rispetto alla volontà del minore**

Degna di nota risulta tale pronuncia. Essa evidenzia come anche in tema di cyberbullismo occorra attribuire in ogni caso rilievo alla volontà di sporgere querela, provenga o meno essa dal minore. In particolare, nel caso di specie una minorenni era stata vittima di un episodio di diffamazione *online* (art. 595 c.p.⁹⁸): nel *blog* a lei registrato, accessibile a chiunque, erano state inserite dall'imputata ultraquattordicenne fotografie che la ritraevano con commenti e conversazioni in *chat* denigratori ed immagini allusive ad un rapporto sessuale. La Corte d'Appello-sezione minorenni di Bologna aveva confermato la sentenza del 5 ottobre 2011 con la quale il Tribunale per i minorenni di quella stessa città aveva dichiarato non doversi procedere in ordine al reato di diffamazione nei confronti dell'imputata minorenni per concessione del perdono giudiziale⁹⁹, respingendo altresì tutte le

*modalità della vigilanza, affinché non violino oltre il necessario la sfera suddetta; ed un'attività di ispezione continua e prolungata è in radice esclusa, oltre che francamente impossibile, soprattutto quanto alle ampie frazioni di giornata che il singolo alunno trascorre comunque nell'intimità della propria stanza di albergo; (...) per dimostrare la carenza di colpa non deve però ritenersi sufficiente quanto appena indicato; proprio perché il rischio che, lasciati in balia di se stessi, i minori possano compiere atti incontrollati e potenzialmente autolesivi, **all'istituzione è imposto un obbligo di diligenza per così dire preventivo, consistente, quanto alla gita scolastica, nella scelta di vettori e di strutture alberghiere che non possano, né al momento della loro scelta, né al momento della loro concreta fruizione, presentare rischi o pericoli per l'incolumità degli alunni**; anche in questo caso con una valutazione da farsi caso per caso in relazione alle circostanze della concreta fattispecie, allora, **incombe all'istituzione scolastica la dimostrazione di avere compiuto tali controlli preventivi e di avere impartito le conseguenti istruzioni agli allievi affidati alla sua cura e alla sua vigilanza (...)**".*

⁹⁸ L'art. 595 c.p. rubricato "Diffamazione" dispone che: "Chiunque, fuori dei casi indicati nell'articolo precedente (riferito al reato di "ingiuria"), comunicando con più persone, offende l'altrui reputazione, è punito con la reclusione fino a un anno o con la multa fino a euro 1.032. Se l'offesa consiste nell'attribuzione di un fatto determinato, la pena è della reclusione fino a due anni, ovvero della multa fino a euro 2.065. Se l'offesa è recata col mezzo della stampa o con qualsiasi altro mezzo di pubblicità, ovvero in atto pubblico, la pena è della reclusione da sei mesi a tre anni o della multa non inferiore a euro 516. Se l'offesa è recata a un Corpo politico, amministrativo o giudiziario, o ad una sua rappresentanza o ad una autorità costituita in collegio, le pene sono aumentate".

⁹⁹ Ai sensi dell'art. 169 c.p. rubricato "Perdono giudiziale per i minori degli anni diciotto": "Se, per il reato commesso dal minore degli anni diciotto la legge stabilisce una pena restrittiva della libertà personale non superiore nel massimo a due anni, ovvero una pena pecuniaria non superiore nel massimo a euro 5 anche se congiunta a detta pena, il giudice può astenersi dal pronunciare il rinvio al giudizio, quando, avuto riguardo alle circostanze indicate nell'articolo 133, presume che il colpevole si asterrà dal commettere ulteriori reati. Qualora si proceda al giudizio, il giudice, può, nella sentenza, per gli stessi motivi, astenersi dal pronunciare condanna. (...). Il perdono giudiziale non può essere concesso più di una volta".

La norma richiama l'istituto del perdono giudiziale, un provvedimento irrevocabile con cui il giudice può decidere per l'estinzione del reato, solo però se questo è stato commesso da minorenni e al ricorrere dei requisiti previsti. Deve considerarsi minorenni il soggetto che all'epoca in cui ha commesso il fatto non aveva superato il diciottesimo anno d'età, ma aveva comunque già compiuto gli anni quattordici, dal momento che questa è la soglia minima prevista per l'imputabilità. Il perdono giudiziale può poi applicarsi se il minore abbia commesso un reato la cui pena non sia superiore nel massimo a due anni, ovvero, se pena pecuniaria, non superiore nel massimo a cinque euro. Si tratta di limiti che non vanno determinati con riferimento al massimo della pena stabilita dalla legge per il reato commesso dal minore, bensì con riferimento alla sanzione che in concreto il giudice ritenga si debba applicare. Infine, condizione essenziale per l'applicazione del perdono giudiziale è la ragionevole presunzione, da parte del giudice, che la mancata irrogazione della pena contribuisca al recupero del minore, lasciando presupporre, quindi, una sua buona condotta per il

censure sollevate da parte ricorrente in merito all'improcedibilità dell'azione penale per invalidità della querela sporta dai genitori della minorenni diffamata. La Corte di Cassazione conferma, in merito al diritto di querela, l'orientamento della Corte d'Appello. Il richiamo è in particolare all'art. 120 c.p., comma 3 ai sensi del quale: *"i minori che hanno compiuto gli anni quattordici e gli inabilitati possono esercitare il diritto di querela, e possono altresì, in loro vece, esercitarlo il genitore ovvero il tutore o il curatore, nonostante ogni contraria dichiarazione di volontà, espressa o tacita, del minore o dell'inabilitato"*. Dal tenore letterale della norma si evince il diritto di sporgere querela in capo al minore ultraquattordicenne; se però questi resta inerte o non intende proporla, la scelta se presentarla o no è attribuita in via sussidiaria ai genitori, anche nell'ipotesi in cui – come nel caso *de quo* - il minore non sia mai venuto a conoscenza del fatto ritenuto lesivo nei suoi confronti. La Corte ben argomenta che in caso di minore-persona offesa che abbia compiuto gli anni quattordici, il legislatore ha previsto una doppia legittimazione: in capo allo stesso minore ed all'esercente la potestà genitoriale. Il conferimento della doppia titolarità del diritto di querela comporta, nondimeno, la necessità di superare possibili situazioni conflittuali nascenti da eventuale volontà contraria di uno dei due soggetti abilitati. In ipotesi di dissenso del genitore - evidenzia la Corte - la norma nulla dice, lasciando, implicitamente, ritenere che, in tal caso, debba prevalere la volontà del minore, siccome portatore dell'interesse giuridico direttamente leso dal fatto illecito da altri commesso nei suoi confronti, anche in ragione del fine di politica criminale di favorire quanto più possibile il perseguimento di azioni delittuose. Viceversa, nell'ipotesi in cui la volontà contraria, tacita od espressa, sia, invece, manifestata dallo stesso minore, il legislatore mantiene la legittimazione in capo al suo genitore. Tale potere surrogatorio trova agevole spiegazione nella ridotta capacità di determinazione e di agire del minore ultraquattordicenne e nella conseguente semipiena capacità, da parte sua, di apprezzare le conseguenze lesive di un fatto-reato nella sfera giuridica dei suoi interessi, in tutti i possibili riflessi patrimoniali o morali. Tale disposto normativo, unitamente alla menzionata *ratio legis*, induce a ritenere che il mantenimento della legittimazione all'esercizio del diritto di querela in capo al genitore del minore dissenziente costituisca fattispecie giuridica che ricomprenda necessariamente - come il più comprende il meno - anche l'ipotesi in cui il minore non sia venuto a conoscenza (magari per responsabile scelta del di lui genitore o comunque delle persone a lui vicine, come pare essersi verificato nel caso di specie) della condotta delittuosa in suo danno. Ne segue che in entrambi i casi, sia il minore infra o ultraquattordicenne, non ha rilievo giuridico alcuno che il minore sia o meno a conoscenza del fatto illecito in suo danno, giacché in nessun caso la sua contraria volontà potrebbe prevalere sulla volontà del genitore orientata all'esercizio del diritto di querela.

Nel caso *de quo* l'Organo giudicante ha altresì ravvisato i presupposti della comunicazione con più persone, tipici del reato di diffamazione, riferendosi alle modalità di accesso al sito, sulla base delle quali, con insindacabile apprezzamento di merito, ha ritenuto che quanto pubblicato, costituente deprecabile esempio di cyberbullismo, fosse venuto a conoscenza di una pluralità di persone.

- Intervista ad Antonello Soro, Presidente del Garante per la protezione dei dati personali del 29 gennaio 2013 – Argomento: i social network un rischio per un giovane su quattro

Antonello Soro, presidente dell'Ufficio del Garante della privacy, valuta la situazione italiana all'indomani della Giornata europea della protezione dei dati personali, evidenziando come: "i giovani non hanno la reale percezione del potere della rete. Di come la vita privata, nell'era dei social network, acquisti un altro peso e i rapporti tutta un'altra platea: sempre più vasta, sempre più sconosciuta".

futuro. Pertanto, il perdono giudiziale non può essere concesso al minore già condannato in precedenza per un delitto doloso, colposo, tentato o consumato.

Alla richiesta se siano aumentati i casi di cyberbullismo, Soro risponde che: *“i dati parlano di un ragazzo su quattro che ne è vittima o autore. Lo testimoniano gli episodi di adolescenti disperati per foto pubblicate a loro insaputa e presi in giro sui social network e che hanno deciso di togliersi la vita”*. Gli si chiede come difendere la propria vita privata¹⁰⁰ e il Garante risponde: *“siamo noi stessi i nostri migliori difensori. Il problema è che i ragazzi non si rendono conto che quando scrivono o mettono immagini on line, a vedere quei contenuti non sono solo i loro amici di sempre. Ma amici di amici di amici, fino ad arrivare a gente che non conoscono. E soprattutto non pensano che quello che mettono in rete oggi sarà visibile per sempre. I comportamenti di oggi rischiano di cambiare il loro domani. Se a 16 anni è divertente pubblicare la foto di una bella bevuta, bisogna ricordarsi che le aziende, quando devono assumere qualcuno, cercano informazioni in rete, anche su Facebook (...). Il 23,6 per cento dei giovani ha trovato falsità e pettegolezzi sul proprio conto e il 20,5 proprie foto imbarazzanti”*.

- **Sentenza n. 18 del 16 gennaio 2012 – Tribunale di Teramo - Argomento: cyberbullismo, formazione di gruppi su Facebook e responsabilità genitoriale**

Il caso sottoposto all'attenzione del Tribunale di Teramo riguardava la formazione su *Facebook* del gruppo denominato *“Per tutti quelli che odiano L.C.”*. In pratica, degli adolescenti avevano creato tale gruppo sul noto *Social Network* ove pubblicavano quotidianamente una serie di frasi ingiuriose e minacciose nei confronti di una loro compagna di scuola minorenni di cui venivano citate espressamente le generalità. Nel corso del giudizio emergeva che la stessa vittima aveva innescato il meccanismo di offese avendo pubblicato precedentemente sulla propria bacheca di *Facebook* una frase offensiva.

Nel caso di specie, il Giudice ha ritenuto di dover condividere l'impostazione interpretativa più rigorosa ed esigente in relazione ai compiti, al ruolo ed alle connesse responsabilità genitoriali, in forza della quale i genitori dei minori capaci di intendere e di volere, per andare esenti dalla responsabilità di cui all'art. 2048 cod. civ., devono positivamente dimostrare: 1) di aver adempiuto all'onere educativo sancito dall'art. 147 cod. civ.; 2) di aver poi effettivamente e concretamente controllato che i figli abbiano assimilato l'educazione a loro impartita esercitando una vigilanza adeguata all'età.

L'Autorità giudiziaria teramense chiarisce, contestualmente alla sentenza, che l'onere educativo consiste nel fornire alla prole gli strumenti indispensabili alla costruzione di relazioni umane effettivamente significative per la migliore realizzazione della loro personalità. Inoltre, consolidata giurisprudenza di Cassazione sostiene che la responsabilità genitoriale non scema con l'avvicinarsi

¹⁰⁰ Tra gli strumenti proposti, il Garante per la Privacy segnala anche un **video su YouTube** con una sorta di decalogo in forma di domande, dal titolo: *“Voglio veramente che tutti sappiano cosa penso di qualcuno, dove sono, quando e con chi?”*. Degna di nota è anche la **lettera del 9 gennaio 2013** che il Antonello Soro presidente dell'Autorità Garante per la Privacy ha indirizzato all'allora Ministro dell'Istruzione, Università e Ricerca Francesco Profumo sottolineando la necessità di affrontare il tema dell'uso responsabile dei *social network* in relazione agli ultimi terribili casi di giovanissimi che hanno deciso di porre fine alla loro vita per essersi sentiti violati nella loro dignità da insulti e offese diffusi *on line* così laceranti per loro da indurli a questo gesto estremo. *“Lo sviluppo tecnologico”*, dice il Garante della privacy, *“è sempre connotato dall'endiadi “opportunità-rischi”, ma mai come con l'avvento della Rete questa doppia faccia si mostra in tutta la sua evidenza. Non si vuole certo demonizzare i social network, ma evidenziare il bisogno di usarli senza nuocere a se stessi e agli altri. Non si tratta solo dei pericoli legati all'autoesposizione, al divulgare senza remore anche gli aspetti più intimi, al “postare” foto e video di cui soprattutto i giovani potrebbero pentirsi in futuro. I rischi riguardano l'enorme potenziale di danno che, come nel caso del cyberbullismo, i nuovi strumenti di comunicazione, proprio per la loro stessa primaria qualità di raggiungere con un click un numero elevatissimo di persone, portano con sé. È con questa preoccupazione”* conclude Soro, *“che so pienamente condivisa, che mi rivolgo a Lei, Signor Ministro, e a tutta la realtà della scuola, affinché il tema della tutela della riservatezza e della dignità delle persone nel mondo on line venga assunto come momento imprescindibile di formazione dei nostri giovani. È aiutandoli a conoscere realmente gli strumenti che abitualmente usano, ma di cui spesso ignorano i pericoli, che potremo garantire loro un'autentica capacità di costruire se stessi, di sviluppare in libertà e armonia la loro identità”*.

dell'adolescente alla maggiore età, avendo questi ultimi ancora “una fragile e indefinita personalità essendo dunque incapaci di controllare i propri istinti”.

Il fatto che il comportamento ingiurioso e minaccioso sia proseguito nel *web* per ben 3 giorni, a parere del Tribunale di Teramo, comprova che i genitori dei minori convenuti non avevano posto in essere le necessarie attività di verifica e di controllo sull'effettiva acquisizione dei valori educativi da parte dei figli. Il Giudice di prime cure ha quindi ritenuto ampiamente raggiunta la prova positiva dell'inadempimento da parte dei genitori degli stessi minori a quel dovere di verifica dell'assimilazione effettiva dell'educazione pure eventualmente impartita¹⁰¹.

Nel caso di specie, tuttavia, il Tribunale ha liquidato esclusivamente il danno patrimoniale e non anche il danno morale soggettivo invocato dai genitori della parte attrice riconoscendo in favore dei convenuti l'attenuante della provocazione.

PARTE IV

Accesso agli atti

Quadro sintetico

Occorre innanzi tutto precisare **che l'accesso agli atti amministrativi non è regolato dal Codice della privacy, né vigilato dal Garante** per la protezione dei dati personali. Come indicato nella legge n. 241 del 1990 (e successive modifiche) rubricata “*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*” **spetta alla singola amministrazione valutare se esistono i presupposti normativi che permettono di prendere visione e di estrarre copia di documenti amministrativi** ai soggetti con un “interesse diretto, concreto e attuale” alla conoscibilità degli atti.

La legge sul procedimento amministrativo non esaurisce l'esame del tema dell'accesso agli atti¹⁰². La materia è ulteriormente approfondita, sotto i profili attuativi, in altre disposizioni normative. Si vedano, in particolare, il D.P.R. 184/2006 “*Regolamento recante disciplina in materia di accesso ai documenti amministrativi*” e il D.P.R. 352/1992 “*Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della legge 7 agosto 1990, n. 24, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*”.

La presente trattazione, nella parte di approfondimento, è dedicata in modo particolare ai numerosi casi in cui occorre effettuare un ponderato **bilanciamento tra le esigenze di accesso agli atti - talvolta connesse ad eventuali azioni difensive e risarcitorie - e le esigenze di tutela della riservatezza dei soggetti coinvolti o citati negli atti e documenti di cui si chiede l'ostensione**.

Approfondimento: casi pratici e normativa di riferimento

- **Sentenza n. 1251 del 20 novembre 2014 – Tar Lombardia, Brescia, Sez. II – Argomento: diritto di accesso ad esposti e denunce da parte del soggetto che subisce un procedimento di controllo – ricognizione dei principi positivi a fondamento**

¹⁰¹ Sul tema della responsabilità genitoriale si segnalano le seguenti pronunce: Cass. Civ., Sez. III, 17 settembre 2013, n. 21168; Cass. Civ., Sez. III, 6 dicembre 2011 n. 26200; Cass. Civ., Sez. III, 22 aprile 2009 n. 9556; Cass. Civ., Sez. III, 13 febbraio/14 marzo 2008 n. 7050; Cass. Civ., Sez. III, 20 ottobre 2005, n. 20322.

¹⁰² Si ricorda altresì la **L. 15/2005** “*Modifiche ed integrazioni alla legge 7 agosto 1990, n. 241, concernenti norme generali sull'azione amministrativa*” che, unitamente alle più recenti **L. 116/2014** e **L. 164/2014**, ha apportato sostanziali modifiche al testo della L. 241/90.

Si ritiene opportuno iniziare la trattazione del delicatissimo tema dell'accesso prendendo in esame la presente pronuncia che, oltre ad essere tra le più recenti, raccoglie e sintetizza, meglio di altre, tutti i principi che nel corso degli ultimi anni sono stati posti a fondamento della prevalenza del diritto di accesso rispetto alle esigenze di privacy. Tale orientamento si può ormai pacificamente definire maggioritario, risultando prevalenti le esigenze di riservatezza solo in alcune ipotesi del tutto residuali (che verranno esaminate nel prosieguo della trattazione) connesse prevalentemente al rischio di ritorsioni, all'attività ispettiva per incompatibilità ambientale o al coinvolgimento di soggetti "deboli".

Venendo al caso in esame, esso riguarda una richiesta di accesso agli atti avanzata nei confronti di un'A.s.l. ed avente ad oggetto un esposto a seguito del quale il richiedente era stato sottoposto ad un procedimento di controllo.

Il Consiglio di Stato nella decisione evidenzia i seguenti principi ormai consolidati e applicabili anche in casi di richieste di accesso agli atti avanzate in ambito scolastico:

- "che il diritto di accesso è ormai pacificamente riconosciuto come diritto soggettivo ad un'informazione qualificata, a fronte del quale l'amministrazione pone in essere un'attività materiale vincolata;

- che l'istanza del richiedente deve essere sorretta da un interesse giuridicamente rilevante, così inteso come un qualsiasi interesse che sia serio, effettivo, autonomo, non emulativo, non riducibile a mera curiosità e ricollegabile all'istante da uno specifico nesso;

- che il diritto alla trasparenza dell'azione amministrativa costituisce una situazione giuridica attiva meritevole di autonoma protezione, da garantire qualora sia funzionale a qualunque forma di tutela, sia giudiziale che stragiudiziale, anche prima e indipendentemente dall'effettivo esercizio di un'azione giudiziale;

- che il privato che subisce un procedimento di controllo vanta un interesse qualificato a conoscere tutti i documenti utilizzati per l'esercizio del potere – inclusi, di regola, gli esposti e le denunce che hanno attivato l'azione dell'autorità – suscettibili per il loro particolare contenuto probatorio di concorrere all'accertamento di fatti pregiudizievoli per il denunciato (Consiglio di Stato, sez. V – 19/5/2009 n. 3081¹⁰³; sez. VI – 25/6/2007 n. 3601¹⁰⁴);

- che l'esposto, una volta pervenuto nella sfera di conoscenza dell'amministrazione, costituisce un documento che assume rilievo procedimentale come presupposto di un'attività ispettiva o di un intervento in autotutela, e di conseguenza il denunciante perde il controllo sulla propria segnalazione la quale diventa un elemento nella disponibilità dell'amministrazione;

- che la sua divulgazione non è preclusa da esigenze di tutela della riservatezza, giacché il predetto diritto non assume un'estensione tale da includere il diritto all'anonimato di colui che rende una dichiarazione a carico di terzi (T.A.R. Veneto, sez. III – 3/2/2012 n. 116¹⁰⁵);

- che la tolleranza verso denunce segrete e/o anonime è un valore estraneo al nostro ordinamento giuridico (si veda la sentenza di questo T.A.R. 29/10/2008 n. 1469¹⁰⁶), e gli autori degli esposti sono tutelati dagli strumenti predisposti dall'ordinamento contro ogni forma di ritorsione o vendetta privata;

- che non può pertanto seriamente dubitarsi che la conoscenza integrale dell'esposto rappresenti uno strumento indispensabile per la tutela degli interessi giuridici dell'istante, essendo intuitivo che solo in questo modo egli potrebbe proporre (eventualmente) contro-denunce a tutela della propria immagine verso l'esterno;

- che detto rilievo rende privi di qualsiasi fondamento giuridico i dubbi sull'uso strumentale e ritorsivo della conoscenza dell'esposto che ha dato luogo ai procedimenti a carico del ricorrente,

¹⁰³ Per la trattazione della sentenza n. 3081 del 19 maggio 2009 del Consiglio di Stato, sez. V si veda *infra* la nota n. 142, pag. 63.

¹⁰⁴ Per la trattazione della sentenza n. 3601 del 25 giugno 2007 del Consiglio di Stato, sez. VI si veda *infra* pag. 75.

¹⁰⁵ Per la trattazione della sentenza n. 116 del 3 febbraio 2012 del Tar Veneto, sez. III si veda *infra* pag. 67.

¹⁰⁶ Per la trattazione della sentenza n. 1469 del 29 ottobre 2008 del Tar Lombardia, Brescia, sez. I si veda *infra* pag. 71.

non potendo ammettersi che pretese esigenze di riservatezza possano determinare un vulnus intollerabile ad un diritto fondamentale della persona, quale quello dell'onore (Consiglio di Stato, sez. V – 28/9/2012 n. 5132¹⁰⁷);

- che il principio di trasparenza dell'attività amministrativa vale sia per il denunciato nei confronti del denunciante sia in senso inverso, in quanto la posizione di denunciante legittima l'accesso agli atti della procedura che ha preso origine dall'esposto;

- che infatti, specularmente, la qualità di autore di un esposto che abbia dato luogo a un procedimento lato sensu sanzionatorio è circostanza idonea a radicare la titolarità di una situazione giuridicamente rilevante di accesso agli atti della pubblica amministrazione (T.A.R. Toscana, sez. III – 16/10/2014 n. 1569 e la giurisprudenza ivi richiamata¹⁰⁸);

- che è pur vero che, in un caso particolare sul quale si è confrontata la giurisprudenza – ossia quello dell'accesso ai verbali redatti dalle autorità amministrative (INPS e INAIL), titolari delle funzioni di vigilanza sui rapporti di lavoro – è stata affermata una stringente esigenza di tutela dei lavoratori che hanno reso le dichiarazioni agli organi ispettivi, per il possibile rischio di condotte ritorsive provenienti dalla parte “forte” del rapporto contrattuale;

- che è stato tuttavia affermato che le suesposte necessità appaiono in ogni caso recessive, rispetto alle esigenze difensive del datore, ove il rapporto d'impiego sia cessato (cfr. T.A.R. Umbria – 21/1/2013 n. 31¹⁰⁹).

Per tutte le ragioni suesposte, nel caso di specie il Tar accoglie quindi il ricorso, riconoscendo al ricorrente “un evidente interesse diretto alla conoscenza integrale dell'esposto” depositato presso l'A.s.l., “che permetterà all'interessato di valutare eventuali future azioni da compiere”.

- **Sentenza n. 5515 del 20 novembre 2013 – Consiglio di Stato, Sez. VI – Argomento: accesso negato per finalità di controllo sull'operato dell'amministrazione, differenza tra accesso civico ed accesso ordinario**

La sentenza in esame risulta particolarmente interessante per il richiamo alla normativa di cui al d.lgs. 33/2013 nonché alle differenze tra l'accesso civico e quello ordinario.

Nel caso di specie, l'università appellante contestava la sentenza del Tar per la Lombardia con la quale era stato in parte accolto il ricorso proposto dal dott. X, per l'accesso ai documenti richiesti alla citata università con istanza a norma degli articoli 22¹¹⁰ e seguenti della legge n. 241/1990. In

¹⁰⁷ Per la trattazione della **sentenza n. 5132 del 28 settembre 2012 del Consiglio di Stato, sez. V** si veda *infra* pag. 63.

¹⁰⁸ Si veda in merito l'interessantissima **sentenza n. 1569 del 14 ottobre 2014 del Tar Toscana, sez. II** che afferma il principio secondo cui in materia di accesso agli atti, la legittimazione a chiedere visione e copia è attribuita anche all'autore di un esposto che abbia dato luogo ad un procedimento disciplinare, circostanza che, insieme ad altre, si ritiene idonea a radicare nell'autore dell'esposto la titolarità di una situazione giuridicamente rilevante di accesso agli atti della P.A. (cfr. Cons. St., A.P., 20 maggio 2006, n. 7; TAR Lombardia, Milano, Sez. III, 22 marzo 2013 n. 763; TAR Piemonte, Sez. I, 6 febbraio 2013, n. 166).

¹⁰⁹ Interessante è il caso trattato nella **sentenza n. 31 del 21 gennaio 2013 del Tar Umbria, sez. I** in cui il Collegio evidenzia che: “le eventuali esigenze di riservatezza del lavoratore controinteressato appaiono in ogni caso recessive rispetto alle esigenze difensive (ex multis Consiglio di Stato sez. VI, 19 giugno 2008, n. 3803) anche in considerazione della cessazione del rapporto di lavoro con l'odierno ricorrente; per questo verso, anzi, le dichiarazioni dell'(ex) dipendente del ricorrente sarebbero al di fuori dell'ambito applicativo del D.M. n. 757/1994 - e dunque i documenti che le contengono non potrebbero essere sottratti all'accesso - poiché l'art. 3, comma 1, lett. c) del citato decreto ministeriale stabilisce che per i documenti in discorso la sottrazione all'accesso permane finché perdura il rapporto di lavoro”. Degno di interesse anche un altro passaggio che si riporta: “l'interesse all'accesso ai documenti va valutato in astratto, senza che possa essere operata, con riferimento al caso specifico, alcun apprezzamento in ordine alla fondatezza o ammissibilità della domanda giudiziale che gli interessati potrebbero eventualmente proporre sulla base dei documenti acquisiti mediante l'accesso e quindi la legittimazione all'accesso non può essere valutata alla stessa stregua di una legittimazione alla pretesa sostanziale sottostante (ex multis Consiglio Stato sez. V, 10 gennaio 2007, n. 55)”.

¹¹⁰ In **L. 241/1990** “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, Capo V “Accesso ai documenti amministrativi”, **art. 22** “Definizioni e principi in materia di accesso”:

particolare, il ricorrente, escluso da un corso di dottorato di ricerca, chiedeva ulteriormente l'ostensione del decreto rettorale, nonché di tutti gli atti delle procedure di valutazione di tutti i dottorandi di ricerca. L'amministrazione universitaria inviava copia del citato decreto rettorale, ma dichiarava inammissibile l'ulteriore richiesta, *"in quanto preordinata al controllo generalizzato dell'operato della scrivente"*.

Nella sentenza appellata le ragioni del ricorrente erano ritenute fondate, limitatamente alla documentazione riferita ai dottorati di ricerca nelle materie giuridiche, svoltisi a partire dall'anno 2009 (in coincidenza col decreto rettorale, approvativo del regolamento dei corsi di dottorato di cui trattasi). Nella pronuncia si sottolineava come l'interesse perseguito riguardasse il rilascio del titolo di dottore di ricerca anche nei casi in cui – come avvenuto per il ricorrente – i Commissari non avessero espresso alcun voto, positivo o negativo, a sostegno della proposta di rilascio del titolo.

A tale riguardo, veniva segnalata *"un'evoluzione sempre più a favore della trasparenza, pur con contemperamenti"*, indirizzati a *"proteggere il più possibile la divulgazione di dati personali"*: quanto sopra, in attuazione delle norme nazionali e comunitarie che – al fine di combattere la corruzione – hanno imposto la più ampia divulgazione delle informazioni, relative ai procedimenti amministrativi, fino all'approvazione del d.lgs. 33/2013¹¹¹, che riordina in un *corpus* unitario la disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione delle informazioni da parte delle pubbliche amministrazioni ed introduce il cosiddetto **diritto di accesso civico, in caso di omessa pubblicazione di dati, di cui sia resa obbligatoria la divulgazione.**

In considerazione, tuttavia, della notevole mole di documentazione richiesta dall'interessato, l'accesso era limitato al periodo successivo all'anno 2009 (e non 2005 come richiesto), tenuto conto della data di approvazione del regolamento dei corsi di dottorato presso l'università.

In sede di appello, la citata università contesta l'applicabilità – nel procedimento speciale di cui agli articoli 22 e seguenti della legge n. 241/1990 – della successiva legislazione in materia di trasparenza. Il Collegio ritiene che l'appello sia meritevole di accoglimento e al riguardo sottolinea che le nuove disposizioni, dettate con d.lgs. 33/2013 in materia di pubblicità, trasparenza e

"1. Ai fini del presente capo si intende: a) per "diritto di accesso", il diritto degli interessati di prendere visione e di estrarre copia di documenti amministrativi; b) per "interessati", tutti i soggetti privati, compresi quelli portatori di interessi pubblici o diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso; c) per "controinteressati", tutti i soggetti, individuati o facilmente individuabili in base alla natura del documento richiesto, che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza; d) per "documento amministrativo", ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attività di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale; e) per "pubblica amministrazione", tutti i soggetti di diritto pubblico e i soggetti di diritto privato limitatamente alla loro attività di pubblico interesse disciplinata dal diritto nazionale o comunitario.

2. L'accesso ai documenti amministrativi, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza.

3. Tutti i documenti amministrativi sono accessibili, ad eccezione di quelli indicati all'articolo 24, commi 1, 2, 3, 5 e 6.

4. Non sono accessibili le informazioni in possesso di una pubblica amministrazione che non abbiano forma di documento amministrativo, salvo quanto previsto dal decreto legislativo 30 giugno 2003, n. 196, in materia di accesso a dati personali da parte della persona cui i dati si riferiscono.

5. L'acquisizione di documenti amministrativi da parte di soggetti pubblici, ove non rientrante nella previsione dell'articolo 43, comma 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, si informa al principio di leale cooperazione istituzionale.

6. Il diritto di accesso è esercitabile fino a quando la pubblica amministrazione ha l'obbligo di detenere i documenti amministrativi ai quali si chiede di accedere".

Si consideri altresì l'**art. 23** *"Ambito di applicazione del diritto di accesso"*: *"Il diritto di accesso di cui all'articolo 22 si esercita nei confronti delle pubbliche amministrazioni, delle aziende autonome e speciali, degli enti pubblici e dei gestori di pubblici servizi. Il diritto di accesso nei confronti delle Autorità di garanzia e di vigilanza si esercita nell'ambito dei rispettivi ordinamenti, secondo quanto previsto dall'articolo 24"*.

¹¹¹ Il d.lgs. 33/2013 è esaminato anche *supra* a pagg. 18 e 21.

diffusione di informazioni da parte delle pubbliche amministrazioni disciplinano situazioni, non ampliative né sovrapponibili a quelle che consentono l'accesso ai documenti amministrativi, ai sensi degli articoli 22 e seguenti della legge 241/90, come successivamente modificata ed integrata. Col citato d.lgs. 33/2013, infatti, si intende procedere al riordino della disciplina, intesa ad assicurare a tutti i cittadini la più ampia accessibilità alle informazioni, concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, al fine di attuare *“il principio democratico e i principi costituzionali di eguaglianza, imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche”*, quale integrazione del diritto *“ad una buona amministrazione”*, nonché per la *“realizzazione di un'amministrazione aperta, al servizio del cittadino”*. Detta normativa – avente finalità dichiarate di contrasto della corruzione e della cattiva amministrazione – intende anche attuare la funzione di *“coordinamento informativo, statistico e informatico dei dati dell'amministrazione statale, regionale e locale”*: quanto sopra, tramite pubblicazione obbligatoria di una serie di documenti nei siti istituzionali delle medesime, con diritto di chiunque di accedere a tali siti *“direttamente ed immediatamente, senza autenticazione ed identificazione”*; **solo in caso di omessa pubblicazione può essere esercitato**, ai sensi dell'art. 5¹¹² del citato d.lgs., **il cosiddetto**

¹¹² L'art. 5 del d.lgs. 33/2013 rubricato “Accesso civico” prevede che:

“1. L'obbligo previsto dalla normativa vigente in capo alle pubbliche amministrazioni di pubblicare documenti, informazioni o dati comporta il diritto di chiunque di richiedere i medesimi, nei casi in cui sia stata omessa la loro pubblicazione.

2. La richiesta di accesso civico non è sottoposta ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente, non deve essere motivata, è gratuita e va presentata al responsabile della trasparenza dell'amministrazione obbligata alla pubblicazione di cui al comma 1, che si pronuncia sulla stessa.

3. L'amministrazione, entro trenta giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, l'amministrazione indica al richiedente il relativo collegamento ipertestuale.

4. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo di cui all'articolo 2, comma 9-bis della legge 7 agosto 1990, n. 241, e successive modificazioni, che, verificata la sussistenza dell'obbligo di pubblicazione, nei termini di cui al comma 9-ter del medesimo articolo, provvede ai sensi del comma 3.

5. La tutela del diritto di accesso civico è disciplinata dalle disposizioni di cui al decreto legislativo 2 luglio 2010, n. 104, così come modificato dal presente decreto.

6. La richiesta di accesso civico comporta, da parte del Responsabile della trasparenza, l'obbligo di segnalazione di cui all'articolo 43, comma 5”.

Si segnalano altresì i richiamati commi 9 bis e 9 ter dell'art. 2 L. 241/1990: 9-bis. “L'organo di governo individua, nell'ambito delle figure apicali dell'amministrazione, il soggetto cui attribuire il potere sostitutivo in caso di inerzia. Nell'ipotesi di omessa individuazione il potere sostitutivo si considera attribuito al dirigente generale o, in mancanza, al dirigente preposto all'ufficio o in mancanza al funzionario di più elevato livello presente nell'amministrazione. Per ciascun procedimento, sul sito internet istituzionale dell'amministrazione è pubblicata, in formato tabellare e con collegamento ben visibile nella homepage, l'indicazione del soggetto a cui è attribuito il potere sostitutivo e a cui l'interessato può rivolgersi ai sensi e per gli effetti del comma 9-ter. Tale soggetto, in caso di ritardo, comunica senza indugio il nominativo del responsabile, ai fini della valutazione dell'avvio del procedimento disciplinare, secondo le disposizioni del proprio ordinamento e dei contratti collettivi nazionali di lavoro, e, in caso di mancata ottemperanza alle disposizioni del presente comma, assume la sua medesima responsabilità oltre a quella propria.

9-ter. Decorso inutilmente il termine per la conclusione del procedimento o quello superiore di cui al comma 7, il privato può rivolgersi al responsabile di cui al comma 9-bis perché, entro un termine pari alla metà di quello originariamente previsto, concluda il procedimento attraverso le strutture competenti o con la nomina di un commissario”.

Infine è utile riportare il testo del citato art. 43 d.lgs. 33/2013 rubricato “Responsabile della trasparenza”:

“1. All'interno di ogni amministrazione il responsabile per la prevenzione della corruzione, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, svolge, di norma, le funzioni di Responsabile per la trasparenza, di seguito “Responsabile”, e il suo nominativo è indicato nel Programma triennale per la trasparenza e l'integrità. Il responsabile svolge stabilmente un'attività di controllo sull'adempimento da parte dell'amministrazione degli obblighi di pubblicazione previsti dalla normativa vigente, assicurando la completezza, la chiarezza e l'aggiornamento delle informazioni pubblicate, nonché segnalando all'organo di indirizzo politico, all'Organismo indipendente di valutazione (OIV), all'Autorità nazionale anticorruzione e, nei casi più gravi, all'ufficio di disciplina i casi di mancato o ritardato adempimento degli obblighi di pubblicazione.

“accesso civico”, consistente in una richiesta – che non deve essere motivata – di effettuare tale adempimento, con possibilità, in caso di conclusiva inadempienza all’obbligo in questione, di ricorrere al giudice amministrativo, secondo le disposizioni contenute nel relativo codice sul processo (d.lgs. 2.7.2010, n. 104¹¹³).

L’accesso ai documenti amministrativi, disciplinato dagli articoli 22 e seguenti della legge 241/90¹¹⁴ è riferito, invece, al “diritto degli interessati di prendere visione ed estrarre copia di documenti amministrativi”, intendendosi per “interessati tutti i soggetti (...) che abbiano un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l’accesso”; in funzione di tale interesse la domanda di accesso deve essere opportunamente motivata.

Benché sommarie, le indicazioni sopra fornite appaiono sufficienti per evidenziare la diversificazione di finalità e di disciplina dell’accesso agli atti, rispetto al cosiddetto accesso civico, pur nella comune ispirazione al principio di trasparenza, che si vuole affermare con sempre maggiore ampiezza nell’ambito dell’amministrazione pubblica.

Per quanto riguarda la documentazione richiesta nel caso di specie – concernente tutti gli atti delle procedure di valutazione di tutti i dottorandi di ricerca – deve ritenersi evidente, secondo il Consiglio di Stato, che la procedura attivata sia da ricondurre in via esclusiva alla citata legge n. 241/1990, come del resto formalmente enunciato nell’istanza: una così ampia diffusione degli atti interni di qualsiasi procedura valutativa non appare imposta, infatti, dal ricordato d.lgs. n. 33/2013, né – se pure lo fosse – potrebbe intendersi riferita anche a procedure antecedenti all’emanazione del medesimo d.lgs., entrato in vigore il 20 aprile 2013.

Per esaminare l’istanza in questione, pertanto, deve farsi riferimento all’art. 24, comma 7, della legge n. 241/1991¹¹⁵, in base al quale *“deve essere garantito ai richiedenti l’accesso ai documenti*

2. Il responsabile provvede all’aggiornamento del Programma triennale per la trasparenza e l’integrità, all’interno del quale sono previste specifiche misure di monitoraggio sull’attuazione degli obblighi di trasparenza e ulteriori misure e iniziative di promozione della trasparenza in rapporto con il Piano anticorruzione.

3. I dirigenti responsabili degli uffici dell’amministrazione garantiscono il tempestivo e regolare flusso delle informazioni da pubblicare ai fini del rispetto dei termini stabiliti dalla legge.

4. Il responsabile controlla e assicura la regolare attuazione dell’accesso civico sulla base di quanto stabilito dal presente decreto.

5. In relazione alla loro gravità, il responsabile segnala i casi di inadempimento o di adempimento parziale degli obblighi in materia di pubblicazione previsti dalla normativa vigente, all’ufficio di disciplina, ai fini dell’eventuale attivazione del procedimento disciplinare. Il responsabile segnala altresì gli inadempimenti al vertice politico dell’amministrazione, all’OIV ai fini dell’attivazione delle altre forme di responsabilità”.

¹¹³ Si tratta del **d.lgs. 104/2010** ovvero **Codice del processo amministrativo**, rubricato *“Attuazione dell’articolo 44 della legge 18 giugno 2009, n. 69, recante delega al governo per il riordino del processo amministrativo”*.

¹¹⁴ Per l’**art. 22 L. 241/1990** vedi *supra* nota n. 110, pag. 52.

¹¹⁵ Si ritiene opportuno riportare per intero il testo dell’**art. 24 L. 241/1990** rubricato *“Esclusione dal diritto di accesso”* a mente del quale:

“1. Il diritto di accesso è escluso: a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo; b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano; c) nei confronti dell’attività della pubblica amministrazione diretta all’emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione; d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psico-attitudinale relativi a terzi.

2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all’accesso ai sensi del comma 1.

3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell’operato delle pubbliche amministrazioni.

4. L’accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

amministrativi, la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici”; nel caso di “documenti contenenti dati sensibili e giudiziari”, però, la medesima norma precisa che l’accesso è consentito solo “nei limiti in cui sia strettamente indispensabile” (in esito ad un sostanziale bilanciamento di interessi, operato già a livello legislativo). Il tenore letterale e la ratio della disposizione legislativa in questione impongono un’attenta valutazione – da effettuare caso per caso – circa la stretta funzionalità dell’accesso alla salvaguardia di posizioni soggettive protette, che si assumano lese, con ulteriore salvaguardia, attraverso i limiti così imposti, degli altri interessi coinvolti, talvolta rispondenti a principi di pari rango costituzionale rispetto al diritto di difesa.

Se l’accesso ai documenti amministrativi, inoltre, costituisce “principio generale dell’attività amministrativa, al fine di favorire la partecipazione e di assicurarne l’imparzialità e la trasparenza”, è anche vero che si richiede per l’accesso un “interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l’accesso” e che “non sono ammissibili istanze di accesso, preordinate ad un controllo generalizzato dell’operato delle pubbliche amministrazioni”, essendo tale controllo estraneo alle finalità, perseguite attraverso l’istituto di cui trattasi (artt. 22, comma 1 lettera b)¹¹⁶ e 24, comma 3 L. 241/90¹¹⁷).

Il cospicuo numero delle istanze di accesso – argomenta il Consiglio di Stato - appare già, di per sé, non conforme alle finalità della normativa in esame, che consente di conoscere tutta la documentazione, che in base ad un apprezzamento preventivo di probabilità l’interessato può, ragionevolmente, ritenere utile per le proprie esigenze di accertamento di fatti che lo riguardano e delle relative, possibili ragioni difensive; può anche riconoscersi che, dalla conoscenza di alcuni atti, possa dimostratamente scaturire l’esigenza di ulteriori acquisizioni documentali; non può invece ritenersi giustificato un ricorso frazionato e protratto nel tempo del diritto di accesso, senza che risultino plausibili ragioni per una omessa acquisizione originaria di tutta la documentazione ritenuta utile e con sostanziale trasformazione dell’accesso in indagine sull’attività amministrativa, alla mera ricerca di nuovi elementi utilizzabili.

Premesso quanto sopra, il Collegio ritiene che le ragioni difensive dell’università appellante siano nella fattispecie condivisibili. Come già in altre decisioni rilevato, infatti (cfr. in particolare, per il

5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell’ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l’eventuale periodo di tempo per il quale essi sono sottratti all’accesso.

6. Con regolamento, adottato ai sensi dell’articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all’accesso di documenti amministrativi: a) quando, al di fuori delle ipotesi disciplinate dall’articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all’esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione; b) quando l’accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria; c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell’ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all’attività di polizia giudiziaria e di conduzione delle indagini; d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all’amministrazione dagli stessi soggetti cui si riferiscono; e) quando i documenti riguardino l’attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all’espletamento del relativo mandato.

7. Deve comunque essere garantito ai richiedenti l’accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l’accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall’articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale”.

¹¹⁶ Per l’art. 22 L. 241/1990 si veda *supra* la nota n. 110, pag. 52.

¹¹⁷ Per l’art. 24 L. 241/1990 si veda subito *supra* la nota n. 115, pag. 55.

principio, Cons. St., sez. VI, n. 1842 del 22.4.2008¹¹⁸), le disposizioni in materia di diritto di accesso mirano a coniugare la ratio dell'istituto, quale fattore di trasparenza e garanzia di imparzialità dell'Amministrazione – nei termini di cui all'art. 22 della citata legge n. 241/90 – con il bilanciamento da effettuare rispetto ad interessi contrapposti, inerenti non solo alla riservatezza di altri soggetti coinvolti, ma anche alle esigenze di buon andamento dell'amministrazione, che appare da salvaguardare in presenza di richieste pretestuose e defatiganti, ovvero introduttive di forme atipiche di controllo.

E' vero che, in via generale, le necessità difensive – riconducibili ai principi tutelati dall'art. 24 della Costituzione¹¹⁹ – sono ritenute prioritarie ed in tal senso il dettato normativo richiede che l'accesso sia garantito “comunque” a chi debba acquisire la conoscenza di determinati atti per la cura dei propri interessi giuridicamente protetti (art. 24, comma 7, L. n. 241/90¹²⁰); la medesima norma tuttavia – come successivamente modificata tra il 2001 e il 2005 – specifica con molta chiarezza come non bastino esigenze di difesa genericamente enunciate per garantire l'accesso, dovendo quest'ultimo corrispondere ad una effettiva necessità di tutela di interessi che si assumano lesi ed ammettendosi solo nei limiti in cui sia “strettamente indispensabile” la conoscenza di documenti, contenenti “dati sensibili e giudiziari”¹²¹.

Nel caso di specie, le esigenze difensive del richiedente l'accesso apparivano più che generiche, in quanto emergeva un contrasto fra lo stesso e gli organi universitari circa l'avvenuta valutazione, o meno, della tesi presentata al termine dei corsi di dottorato di ricerca e l'obbligo, o meno, di rilasciare il titolo relativo, non richiedente “valutazione o punteggio”, o quanto meno non richiedendo motivazione il voto positivo. Le modalità procedurali, attraverso cui l'università può addivenire al rilascio del titolo di dottore di ricerca sono dunque, evidentemente, vincolate, mentre ampiamente discrezionale non può non essere il contenuto della valutazione di merito da esprimere. Pertanto, la comparazione con precedenti procedure non poteva giovare alla difesa del richiedente l'accesso, non risultando prospettabile il vizio di eccesso di potere per disparità di trattamento in rapporto ad atti vincolati e non essendo censurabili nel merito gli apprezzamenti discrezionali delle commissioni giudicatrici.

Il Consiglio di Stato accoglieva quindi l'appello, non potendosi non ravvisare – in richieste non adeguatamente motivate e impicanti sia ricerche che produzioni documentali ponderose – proprio quella forma di atipico controllo sull'operato dell'amministrazione e/o di organi tecnici alla stessa riconducibili non consentita nel contesto normativo di riferimento.

- Sentenza n. 4035 del 31 luglio 2013 – Consiglio di Stato, Sez. VI e circolare n. 43 dell'8 novembre 2013 del Ministero del Lavoro e delle Politiche sociali - Argomento: diniego alla richiesta di accesso alle dichiarazioni rilasciate dai lavoratori in sede ispettiva

La sentenza in oggetto affronta la tematica della legittimità del provvedimento di diniego ad una richiesta di accesso alle dichiarazioni rese dai lavoratori nel corso di una verifica ispettiva. La materia non è prettamente scolastica, ma la vicenda processuale è degna di nota in quanto si inserisce in un quadro giurisprudenziale connotato da orientamenti contrastanti ed oscillanti nel tempo che, nel corso degli anni ed in relazione alla tematica cui afferisce l'accesso, hanno visto ora l'affermazione della prevalenza del diritto di difesa sancito dall'art. 24 Cost.¹²², ora il riconoscimento della legittimità dei dinieghi di accesso agli atti motivati dalle esigenze di tutela

¹¹⁸ Per un esame approfondito della **sentenza n. 1842 del 22 aprile 2008 del Consiglio di Stato, sez. VI** si veda *infra* pag. 73.

¹¹⁹ Ai sensi dell'**art. 24 Cost.**: “Tutti possono agire in giudizio per la tutela dei propri diritti e interessi legittimi. La difesa è diritto inviolabile in ogni stato e grado del procedimento (...)”.

¹²⁰ Per l'**art. 24 L. 241/1990** vedi *supra* nota n. 115, pag. 55.

¹²¹ Il medesimo assunto è stato espresso anche in passato nella **sentenza n. 5153 del 28 settembre 2012 del Consiglio di Stato, sez. VI** esaminata *infra* a pag. 64.

¹²² Per l'**art. 24 Cost.** vedi subito *supra* nota n. 119.

della riservatezza dei lavoratori unitamente a quella di preservazione della pubblica funzione di vigilanza. In effetti, nel recente passato, si sono succedute diverse pronunce che ritenevano ammissibile l'accesso alle dichiarazioni rese dai lavoratori in sede di verifica ispettiva sul presupposto che l'esigenza di riservatezza e di protezione dei lavoratori intervistati fosse recessiva di fronte al diritto esercitato dal richiedente per la difesa di un interesse giuridico, nei limiti in cui esso risultasse necessario alla difesa di quell'interesse. Le predette sentenze¹²³, in alcuni casi, fondavano le decisioni di accoglimento anche in base alla possibilità da parte dell'Amministrazione di intervenire con opportuni accorgimenti (cancellature o *omissis* attraverso cui ottenere l'espunzione dei nominativi dei dipendenti interessati) in modo da consentire il giusto contemperamento tra gli opposti interessi in gioco.

Il citato orientamento contrasta con altre pronunce (es. Consiglio di Stato, sez. VI, n. 1842/2008¹²⁴) che, in materia di accesso alle dichiarazioni rese dai lavoratori in sede di verifica ispettiva, hanno ritenuto legittimo il diniego opposto dall'Amministrazione sulla scorta degli articoli 2 e 3 del D.M. 757/1994¹²⁵ *“a motivo della salvaguardia di possibili azioni pregiudizievoli, recriminatorie o di pressione nei confronti dei lavoratori o collaboratori della società”*. In tali decisioni, il Consiglio di Stato, al fine di coniugare l'esigenza di trasparenza ed imparzialità dell'Amministrazione, esplicitata dall'art. 22 L. 241/90¹²⁶, rispetto ad altri interessi contrapposti, fra cui quelli dei soggetti *“individuati o facilmente individuabili”* che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza (art. 22, comma 1, lett. c)), prende in esame anche il successivo art.

¹²³ Tra queste si segnala la **sentenza n. 3798 del 29 luglio 2008 del Consiglio di Stato, sez. VI** in cui si evidenzia la necessità di una valutazione “caso per caso” che potrebbe talvolta consentire di ritenere prevalenti le esigenze difensive e che, nel caso di specie, ammette l'accesso al contenuto delle dichiarazioni di lavoratori agli ispettori del lavoro, ma con modalità che escludano l'identificazione degli autori delle medesime.

¹²⁴ Per un esame approfondito della **sentenza n. 1842 del 22 aprile 2008 del Consiglio di Stato, sez. VI** si veda *infra* a pag. 73.

¹²⁵ In **D.M. 757/1994** *“Regolamento concernente le categorie di documenti formati o stabilmente detenuti dal Ministero del lavoro e della previdenza sociale sottratti al diritto d'accesso, ai sensi dell'art. 24, comma 4, della legge 7 agosto 1990, n. 241”*, **art. 2** *“Categorie di atti sottratti al diritto di accesso”*: *“1. Sono sottratte al diritto di accesso le seguenti categorie di atti in relazione alla esigenza di salvaguardare la vita privata e la riservatezza di persone fisiche, di persone giuridiche, di gruppi, imprese e associazioni: a) documenti contenenti notizie sulla programmazione dell'attività di vigilanza, nonché sulle modalità ed i tempi di svolgimento di essa; b) documenti contenenti le richieste di intervento dell'Ispettorato del lavoro; c) documenti contenenti notizie acquisite nel corso delle attività ispettive, quando dalla loro divulgazione possano derivare azioni discriminatorie o indebite pressioni o pregiudizi a carico di lavoratori o di terzi; d) documenti contenenti notizie riguardanti le aziende pubbliche o private quando la loro divulgazione possa portare effettivo pregiudizio al diritto alla riservatezza o provocare concretamente una indebita concorrenza; e) relazioni ispettive presso gli enti previdenziali ed assistenziali; f) verbali di ispezione alle società cooperative; g) documenti riguardanti il lavoratore e contenenti notizie sulla sua situazione familiare, sanitaria, professionale, finanziaria, sindacale o di altra natura, sempreché dalla loro conoscenza possa derivare effettivo pregiudizio al diritto alla riservatezza; h) documenti riguardanti il dipendente dell'amministrazione e contenenti notizie sulla sua situazione familiare, sanitaria, professionale, finanziaria, sindacale o di altra natura, sempreché dalla loro conoscenza possa derivare effettivo pregiudizio al diritto alla riservatezza.*

2. Le notizie contenute nei documenti indicati alle categorie g) ed h), del comma 1 del presente articolo, cessano di essere escluse dall'accesso quando costituiscono rispettivamente titoli per l'avviamento al lavoro o la partecipazione a pubblici concorsi”.

Art. 3 *“Durata del divieto di accesso”*: *“1. Le categorie di documenti indicati nell'articolo precedente sono sottratti all'accesso rispettivamente per il periodo sottoindicato, che decorre dalla data del provvedimento che chiude il procedimento di cui essi fanno parte: a) cinque anni; b) cinque anni, o finché perduri il rapporto di lavoro nella ipotesi che la richiesta di intervento provenga da un lavoratore o abbia comunque ad oggetto un rapporto di lavoro; c) finché perduri il rapporto di lavoro, salvo che le notizie contenute nei documenti di tale categoria risultino a quella data sottoposti al segreto istruttorio penale; d) fino a quando sussista il titolare del diritto alla riservatezza; e) cinque anni, salvo che le notizie contenute nei documenti di tale categoria risultino a quella data sottoposti al segreto istruttorio penale; f) cinque anni, salvo che le notizie contenute nei documenti di tale categoria risultino a quella data sottoposti al segreto istruttorio penale; g) finché è in vita il titolare del diritto alla riservatezza; h) finché è in vita il titolare del diritto alla riservatezza”.*

¹²⁶ Per l'**art. 22 L. 241/1990** vedi *supra* nota n. 110, pag. 52.

24¹²⁷ della medesima legge che disciplina i casi di esclusione al diritto in questione. Quest'ultimo, al comma 6, tra i casi di possibile sottrazione all'accesso da stabilirsi in via regolamentare, prevede al punto d) quelli relativi *“a documenti che riguardano la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'Amministrazione dagli stessi soggetti a cui si riferiscono”*. In tale ottica, osserva il Consiglio di Stato, *“correttamente il D.M. n. 757/1994 inserisce fra tali categorie all'art. 2 lett. b) e c) i documenti contenenti richieste di intervento dell'Ispettorato del Lavoro nonché i documenti contenenti notizie acquisite nel corso delle attività ispettive, quando dalla loro divulgazione possano derivare azioni discriminatorie o indebite pressioni o pregiudizi a carico di lavoratori o di terzi”*. Il Consiglio di Stato rileva che la giurisprudenza¹²⁸ ha più volte confermato la sottrazione al diritto di accesso di documentazione acquisita dagli ispettori del lavoro nell'ambito dell'attività di controllo loro affidata, essendo necessario salvaguardare l'esigenza di riservatezza di chi abbia reso dichiarazioni, riguardanti se stessi o altri soggetti, senza autorizzarne la divulgazione, non attenendo la sfera di interessi in questione alla sola tutela delle posizioni del lavoratore ed essendo queste ultime, comunque, rilevanti “anche in rapporto all'ambiente professionale di appartenenza, più largamente inteso”. In tali statuizioni detto Organo sottolinea la **prevalenza dell'interesse pubblico all'acquisizione di ogni possibile informazione, a tutela della sicurezza e regolarità dei rapporti di lavoro rispetto al diritto di difesa delle società o imprese sottoposte ad ispezione**: il primo infatti non potrebbe non essere compromesso dalla comprensibile reticenza di lavoratori, cui non si accordasse la tutela di cui si discute, mentre il secondo risulta comunque garantito dall'obbligo di motivazione per eventuali contestazioni e dalla documentazione che ogni datore di lavoro è tenuto a possedere¹²⁹.

In merito poi agli eventuali accorgimenti (cancellature, *omissis*) che, in sede di ostensione dei dati, l'Amministrazione potrebbe adottare, il Ministero del Lavoro nella **nota n. 43 dell'8 novembre 2013** osserva come tali cautele risultino del tutto insufficienti a tutelare la riservatezza dei dichiaranti laddove, soprattutto in ipotesi di imprese di piccole dimensioni, il semplice contenuto delle dichiarazioni possa far risalire alla persona che le ha rilasciate, facilmente individuabile attraverso, per esempio, l'individuazione delle mansioni ricoperte oppure la puntuale indicazione dell'orario di lavoro osservato, ovvero l'indicazione degli altri colleghi appartenenti al medesimo reparto.

A supporto della interpretazione operata dal Consiglio di Stato sembra muoversi anche la Corte di Cassazione che, in alcune pronunce, ribadisce come, ai fini dell'esigenza di tutela del destinatario di provvedimenti ispettivi, è sufficiente la possibilità per lo stesso di proporre davanti al Giudice le censure o contestazioni in merito alla documentazione che l'Amministrazione, in quella sede, è tenuta ad esibire ai fini processuali. Pertanto, in tale sede, sarà sempre possibile al datore di lavoro azionare le proprie difese anche in relazione a tali fonti di prova esibite in giudizio.

Da ultimo, coerente con tale orientamento, si colloca la citata sentenza n. 4035 del 31 luglio 2013 che interviene in controtendenza **dopo un biennio di giurisprudenza favorevole all'accesso, riaffermando, pur entro certi limiti e previa valutazione motivata caso per caso, la legittimità per le Direzioni territoriali del Ministero del Lavoro di sottrarre all'accesso le dichiarazioni dei lavoratori rese durante l'accesso ispettivo**. In particolare, la sentenza in questione, oltre a richiamare alcune valutazioni già espresse nelle conformi menzionate pronunce, chiarisce con nettezza che **“ferma restando, dunque, una possibilità di valutazione caso per caso, che potrebbe talvolta consentire di ritenere prevalenti le esigenze difensive in questione (cfr. Consiglio di Stato,**

¹²⁷ Per l'art. 24 L. 241/1990 vedi *supra* nota n. 115, pag. 55.

¹²⁸ In tal senso: C.d.S., n. 736/2009; C.d.S., sez. VI, n. 1842 del 22.4.2008; C.d.S., sez. VI, n. 65 del 27.1.1999 e C.d.S., sez. VI, n. 1604 del 19.1.1996.

¹²⁹ Il medesimo orientamento emerge nella meno recente **sentenza n. 1842 del 22 aprile 2008 del Consiglio di Stato, sez. VI** trattata *infra* a pag. 73.

sez. VI, n. 3798/2008 del 29.7.08¹³⁰, che ammette l'accesso al contenuto delle dichiarazioni di lavoratori agli ispettori del lavoro, ma con modalità che escludano l'identificazione degli autori delle medesime), non può però affermarsi in modo aprioristico una generalizzata recessività dell'interesse pubblico all'acquisizione di ogni possibile informazione, per finalità di controllo della regolare gestione dei rapporti di lavoro (a cui sono connessi valori, a loro volta, costituzionalmente garantiti), rispetto al diritto di difesa delle società o imprese sottoposte ad ispezione¹³¹(...)". La sentenza in parola risolve, inoltre, anche la *vexata quaestio* della posizione dei lavoratori in ordine alle richieste di accesso alle dichiarazioni dagli stessi rilasciate in sede ispettiva, chiarendo come vada loro attribuita la qualifica di "controinteressati" con il conseguente riconoscimento, anche dal punto di vista del procedimento amministrativo, di tutti i diritti inerenti a tale qualificazione, spettanti anche nei confronti di eventuali obbligati solidali diversi dal datore di lavoro.

- **Provvedimento del Garante privacy del 18 luglio 2013 – Argomento: accesso ex artt. 7 e 8 Codice Privacy ed accesso ordinario ex L. 241/90**

Nel caso in esame, il Garante provvede sul ricorso presentato da una docente, la quale aveva presentato istanza ai sensi degli artt. 7¹³² e 8¹³³ d.lgs. 196/2003 alla propria direzione didattica di appartenenza ai fini di ottenere la comunicazione in forma intelligibile di tutti i dati personali che la riguardavano (con particolare riferimento ad una riunione nel corso della quale erano state rese dichiarazioni sul suo conto).

Il ricorso è parzialmente accolto, con conseguente ordine alla direzione didattica di provvedere, ma il Garante coglie l'occasione per sottolineare la differenza di questo tipo di accesso rispetto all'ordinario accesso agli atti previsto dagli artt. 22¹³⁴ ss. l. 241/1990. In particolare, chiarisce che **l'accesso previsto dalla l. 241/1990 prevede un diritto di accedere ad atti e documenti nei confronti dei quali l'istante vanta un interesse qualificato, a fronte di una motivazione contingente. La tutela del controinteressato in questi casi è offerta tramite l'obliterazione dei dati sensibili e l'avviso ai sensi dell'art. 3 D.P.R. 184/2006¹³⁵. L'accesso previsto dall'art. 7 d.lgs. 196/2003 è invece "volto a consentire agli interessati di ottenere, ai sensi dell'art. 10 del predetto Codice¹³⁶, la comunicazione in forma intelligibile dei dati personali effettivamente**

¹³⁰ Per la **sentenza n. 3798 del 29 luglio 2008 del Consiglio di Stato, sez. VI** vedi *supra* nota n. 123, pag. 58.

¹³¹ Il medesimo assunto è stato espresso anche in passato nella **sentenza n. 5153 del 28 settembre 2012 del Consiglio di Stato, sez. VI** esaminata *infra* a pag. 64.

¹³² In merito all'**art. 7 C.P.** si veda *supra* la nota n. 21, pag. 11.

¹³³ In Parte I "**Disposizioni generali**", Titolo II "**Diritti dell'interessato**", **art. 8 C.P.** "**Esercizio dei diritti**" : "**1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo. (...) 4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento**".

¹³⁴ Per l'**art. 22 L. 241/1990** vedi *supra* nota n. 110, pag. 52.

¹³⁵ In **D.P.R. 184/2006** "**Regolamento recante disciplina in materia di accesso ai documenti amministrativi**" **art. 3** "**Notifica ai controinteressati**": "**1. Fermo quanto previsto dall'articolo 5, la pubblica amministrazione cui è indirizzata la richiesta di accesso, se individua soggetti controinteressati, di cui all'articolo 22, comma 1, lettera c), della legge, è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione. I soggetti controinteressati sono individuati tenuto anche conto del contenuto degli atti connessi, di cui all'articolo 7, comma 2. 2. Entro dieci giorni dalla ricezione della comunicazione di cui al comma 1, i controinteressati possono presentare una motivata opposizione, anche per via telematica, alla richiesta di accesso. Decorso tale termine, la pubblica amministrazione provvede sulla richiesta, accertata la ricezione della comunicazione di cui al comma 1**".

¹³⁶ In Parte I "**Disposizioni generali**", Titolo II "**Diritti dell'interessato**", **art. 10 C.P.** "**Riscontro all'interessato**" : "**1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare: a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che**

detenuti dal titolare del trattamento, estrapolati dai documenti che li contengono". La tutela del controinteressato è offerta, come nel provvedimento in commento, dall'oscuramento di tutti i dati riferiti a terzi.

La differenza di fondo è pertanto riferita al tipo di accesso e all'oggetto del medesimo: la l. 241/1990 nasce per consentire l'accesso ai documenti in possesso della Pubblica Amministrazione, mentre il Codice Privacy riguarda indifferentemente pubblico e privato e, pertanto, prescinde parzialmente dalle logiche pubblicistiche che governano l'accesso previsto dall'art. 22 l. 241/1990. Nel caso specifico, la mole del fascicolo rendeva eccessivamente onerosa l'estrapolazione dei dati: conseguentemente, il Garante autorizza l'esibizione e la consegna in copia dei documenti integrali ai sensi del comma 4° dell'art. 10 C.P. Provvede pertanto all'ordine *"di comunicare alla ricorrente, secondo le modalità di cui all'art. 10 del Codice, i dati personali che la riguardano contenuti nel verbale del 21.4.2008 e nelle altre dichiarazioni rese dai genitori al dirigente scolastico, previo oscuramento dei dati riferiti a terzi"*.

- Sentenza n. 2423 del 6 maggio 2013 – Consiglio di Stato, Sez. VI - Argomento: diritto di accesso ai verbali del Collegio docenti

Il componente di un organo collegiale della scuola ha diritto a richiedere copia degli atti e dei verbali inerenti all'attività del collegio stesso e pertanto è illegittimo il diniego dell'amministrazione scolastica all'estrazione di copia dei suddetti documenti.

Lo ha stabilito il Consiglio di Stato, con la pronuncia in esame, decidendo sul ricorso di quattro professoresse per la riforma della sentenza con la quale il Tribunale amministrativo per la Campania, sezione di Salerno, ha dichiarato inammissibile il loro ricorso per l'accesso. La vicenda è scaturita a causa del rifiuto, da parte del dirigente scolastico di una scuola campana, di fornire copia dei verbali di due sedute del collegio dei docenti, atteso che – secondo le ricorrenti - non si

riguardano singoli interessati identificati o identificabili; b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro".

era provveduto alla lettura ed approvazione dei relativi verbali. Della questione si era occupata la Commissione per l'accesso agli atti presso la Presidenza del Consiglio dei ministri, la quale aveva invitato l'amministrazione a riesaminare la vicenda. A causa del rifiuto, le docenti si erano rivolte al Tar, che aveva però rigettato il ricorso, ritenendo che non era stato dedotto *"un interesse giuridicamente tutelabile all'esibizione della documentazione richiesta"*.

Il Consiglio di Stato ha però riformato la sentenza, assumendo che *"tale valutazione di insussistenza del loro interesse all'accesso ai predetti documenti non può essere condivisa, trattandosi di un caso in cui l'interesse è in re ipsa, inerendo alla funzione di componente del collegio dei docenti, che giustifica l'esigenza di conservare e poter disporre della documentazione dell'attività svolta"*. Infatti, **"il componente di un organo collegiale dell'amministrazione ha un interesse concreto e diretto, oltre che qualificato, a disporre di copia degli atti e dei verbali inerenti all'attività del collegio stesso, per verifica, approfondimento, memoria dell'iter di formazione della volontà collegiale, disponibilità che non può essere circoscritta solo all'occasione delle riunioni cui egli partecipa o della apposizione della firma ai verbali ad esse relativi"**. Proprio alla qualità di componente di organo collegiale dell'istituzione scolastica si riconnette l'interesse, cui la disponibilità della documentazione può essere funzionale, ad ogni utile iniziativa sul piano propositivo e deliberativo per il miglior perseguimento degli interessi di rilievo pubblico che fanno capo all'istituzione stessa. Rimane, quindi, escluso che all'istanza delle odierne appellanti (...) possa attribuirsi un carattere eminentemente esplorativo, mentre pretestuoso, in relazione ad atti formati con la loro presenza, appare il richiamo a posizioni di terzi soggetti potenziali controinteressati, peraltro tutelabili da parte dell'amministrazione con le forme a ciò previste".

- **Sentenza n. 393 del 19 marzo 2013 – Tar Toscana, Sez. I - Argomento: diritto di accesso del docente al verbale della Polizia di Stato per poter tutelare la sua posizione giuridica**

Nel caso in esame una docente in servizio presso un istituto tecnico era stata coinvolta, in occasione degli esami di riparazione, in un episodio che aveva dato luogo all'intervento di personale della Polizia di Stato e che successivamente era stato causa dell'applicazione di una sanzione disciplinare nei suoi confronti. In particolare, una pattuglia dell'Ufficio "Volanti" della Questura era intervenuta presso l'istituto scolastico in cui prestava servizio la ricorrente a seguito di una richiesta di intervento circa la sua asserita irreperibilità in occasione degli esami di riparazione: dopo aver identificato le parti, il personale intervenuto aveva redatto una relazione di servizio al dirigente dell'ufficio. La professoressa aveva quindi chiesto al Questore, ai sensi dell'art. 22 l. 241/90¹³⁷, il rilascio del verbale redatto dagli agenti relativamente all'intervento e la registrazione della telefonata richiedente l'intervento o, in alternativa, la dichiarazione sul contenuto della telefonata.

Non avendo ottenuto favorevole riscontro ostandovi, secondo la P.A. adita, il disposto di cui all'art. 3 del D.M. 415/1994¹³⁸, la docente aveva proposto ricorso alla Commissione per l'accesso ai documenti amministrativi presso la Presidenza del Consiglio dei ministri, che parimenti aveva respinto il gravame. L'interessata agiva quindi in sede giurisdizionale. I giudici accoglievano il ricorso: secondo il Collegio, infatti, **"sussiste il presupposto per l'accesso consistente (art. 22 comma 1 lett. b) della legge n. 241/1990) nell'essere titolare di "un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso"**. **Non si può infatti negare che un insegnante definito "irreperibile" nell'istituto in cui presta servizio durante l'orario di svolgimento di esami di riparazione e quindi**

¹³⁷ Per l'art. 22 L. 241/1990 vedi *supra* nota n. 110, pag. 52.

¹³⁸ Nel D.M. 415/1994 "Regolamento per la disciplina delle categorie di documenti sottratti al diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 4, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" l'art. 3 riguarda le "Categorie di documenti inaccessibili per motivi di ordine e sicurezza pubblica ovvero ai fini di prevenzione e repressione della criminalità".

identificato da personale della Polizia di Stato, intervenuto su chiamata, abbia titolo per difendere la propria professionalità in ogni sede ritenuta opportuna”.

Inoltre – precisa la sentenza – ai sensi dell’art. 8, comma 5, lettera c) del D.P.R. 352/1992¹³⁹, le relazioni di servizio sono sottratte all’accesso in relazione all’esigenza di salvaguardare l’ordine pubblico e la prevenzione e repressione della criminalità, ipotesi non ricorrenti nel caso di specie “tenuto conto che i concetti di “tutela dell’ordine e della sicurezza pubblica” e di “prevenzione e repressione della criminalità” vanno calati nella realtà della singola fattispecie, anche per evitare il rischio di una sottrazione pressoché generalizzata all’accesso dei documenti formati dall’Amministrazione dell’Interno”.

- **Sentenza n. 5132 del 28 settembre 2012 – Consiglio di Stato, Sez. V- Argomento: diritto di accesso da parte del soggetto che subisce il procedimento disciplinare ad esposti e denunce che hanno determinato l’esercizio del potere di vigilanza dell’amministrazione**

La pronuncia in esame, pur non prettamente scolastica, è degna di nota in quanto si colloca nell’ambito del consolidato filone giurisprudenziale che – salvo casi particolari - riconosce la prevalenza del diritto di difesa rispetto alle esigenze di riservatezza¹⁴⁰.

Nel caso in esame, il Tar Lazio accoglieva il ricorso proposto dal sig. X ordinando all’intimata amministrazione comunale l’accesso documentale richiesto mediante consegna della copia dell’esposto (che dava luogo al provvedimento disciplinare in danno del ricorrente), nella sua forma completa e priva di cancellature o mascherature.

Con atto di appello il Comune chiedeva la riforma di tale sentenza, ma il Consiglio di Stato rigettava l’istanza rilevando che “secondo un consolidato indirizzo giurisprudenziale, dal quale non vi è motivo per discostarsi, **il soggetto che subisce un procedimento di controllo o ispettivo ha un interesse qualificato a conoscere integralmente tutti i documenti utilizzati dall’amministrazione nell’esercizio del potere di vigilanza, compresi gli esposti e le denunce che hanno determinato l’attivazione di tale potere** (C.d.S., sez. IV, 19 gennaio 2012, n. 231¹⁴¹; sez. V, 19 maggio 2009, n. 3081¹⁴²), **non ostandovi neppure il diritto alla riservatezza che non può essere invocato quando la**

¹³⁹ In D.P.R. 352/92 “Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell’art. 24, comma 2, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”, l’ **art. 8** rubricato “Disciplina dei casi di esclusione”, al comma 5 così dispone: “(...) i documenti amministrativi possono essere sottratti all’accesso: (...) c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell’ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, nonché all’attività di polizia giudiziaria e di conduzione delle indagini; (...)”.

¹⁴⁰ Nello stesso senso si veda *infra* a pag. 71 la meno recente **sentenza n. 1469 del 29 ottobre 2008 del Tar Lombardia, Brescia, sez. I.**

¹⁴¹ La **sentenza n. 231 del 19 gennaio 2012 del Consiglio di Stato, sez. IV** richiamata, riguardante il diritto di accesso nell’ambito di un’ispezione tributaria, pur non avendo ad oggetto la materia scolastica, risulta particolarmente interessante per il principio di diritto in essa espresso, coerente con quello richiamato nella pronuncia di cui trattasi e, più in generale, con l’orientamento giurisprudenziale ad oggi prevalente. In particolare, il Consiglio di Stato statuisce che: “(...) i documenti chiesti in visione, tenuto conto della loro natura e funzione (denunce e/o segnalazioni) appaiono (...) oggettivamente non pregiudizievoli rispetto ai “superiori” interessi tutelati dalla normativa in questione e cioè a quelli sottesi alla sicurezza, all’ordine pubblico e alla prevenzione e repressione della criminalità”. Inoltre “(...) secondo un preciso orientamento giurisprudenziale, dal quale non si ha motivo di discostarsi (...) gli atti interni, le denunce, gli atti di iniziativa, gli esposti (categorie nelle quali possono farsi rientrare i documenti chiesti in visione) sono ostensibili ai soggetti legittimati a richiederli (...). In definitiva, non sono assumibili nella specie ragioni ostative all’accoglimento della richiesta di accesso, (...) a fronte di una istanza di accesso formulata espressamente ai fini di difesa e tutela giudiziaria (cosiddetto “accesso difensivo”), circostanza in relazione alla quale il legislatore, all’art. 24, comma 7 della legge 241/90 (...), ha approntato una indubbia prevalenza sugli altri interessi coinvolti (...)”.

¹⁴² La **sentenza n. 3081 del 19 maggio 2009 del Consiglio di Stato, sez. V**, analoga alla precedente e non avente ad oggetto la materia scolastica, riguardava la richiesta da parte dell’appellante di una copia dell’esposto - al quale non era stato dato seguito - completa del nominativo dell’esponente. Il Consiglio di Stato, accogliendo l’appello e riformando la

richiesta di accesso ha ad oggetto il nome di coloro che hanno reso denunce o rapporti informativi nell'ambito di un procedimento ispettivo, giacché al predetto diritto alla riservatezza non può riconoscersi un'estensione tale da includere il diritto all'anonimato di colui che rende una dichiarazione a carico di terzi, tanto più che l'ordinamento non attribuisce valore giuridico positivo all'anonimato (C.d.S., sez. VI, 25 giugno 2007, n. 3601¹⁴³). Non può pertanto seriamente dubitarsi che la conoscenza integrale dell'esposto rappresenti uno strumento indispensabile per la tutela degli interessi giuridici dell'appellato, essendo intuitivo che solo in questo modo egli potrebbe proporre eventualmente denuncia per calunnia a tutela della propria onorabilità: il che rende del tutto privi di qualsiasi fondamento giuridico i dubbi sull'uso asseritamente strumentale e ritorsivo della conoscenza dell'esposto che ha dato luogo al procedimento disciplinare in danno del ricorrente, non potendo ammettersi che pretese esigenze di riservatezza possano determinare un vulnus intollerabile ad un diritto fondamentale della persona, quale quello dell'onore".

- Sentenza n. 5153 del 28 settembre 2012 – Consiglio di Stato, Sez. VI - Argomento: limiti al diritto di accesso e modalità di esercizio dello stesso relativamente alla documentazione acquisita dagli ispettori in materia scolastica per il rischio di pressioni o azioni pregiudizievoli da parte del destinatario delle dichiarazioni

Nel caso in esame, peraltro pronunciandosi nello stesso giorno, il Consiglio di Stato (in altra sezione, la VI) statuisce in modo diametralmente opposto rispetto alla sentenza precedente. Nel merito, la docente ricorrente contesta la sentenza del Tar Puglia che aveva acconsentito all'accesso agli atti del procedimento relativo al trasferimento per incompatibilità ambientale, ma con svariati *omissis*, tutti relativi - a suo dire - a circostanze rilevanti per la sua difesa, poiché riconducibili alla individuazione delle date degli episodi decisivi per l'avvio del procedimento stesso e dei nominativi delle persone che sono state ascoltate dall'ispettore nel corso del procedimento, nonché senza gli

sentenza del Tar, definisce la posizione soggettiva del ricorrente "giuridicamente rilevante e qualificata dall'ordinamento come meritevole di tutela", stabilendo che "la volontà di difendersi manifestata dal ricorrente non poteva essere ritenuta pretestuosa ed immotivata". Riconosce altresì che: "la formula utilizzata dal richiedente si sostanzia non già in una mera clausola di stile inidonea a sorreggere la richiesta di conoscere il nominativo dell'esponente, bensì in un'allegazione sufficiente a far apprezzare l'esistenza della situazione legittimante e la funzionalità del documento richiesto alla tutela della medesima. D'altro canto, il fatto che non sia stata indicata la specifica azione da proporre davanti al giudice ordinario non priva di rilievo detta manifestazione di volontà, tenuto conto, per un verso, che la conoscenza del nominativo del soggetto da convenire in giudizio è indispensabile quale che sia l'azione da instaurare e, per altro verso, tale indicazione non avrebbe consentito al Comune di valutare la portata dell'azione, i presupposti e, in ultima analisi, la possibilità di utile esperimento, atteso che detta valutazione, com'è noto, non compete alla pubblica amministrazione". Rileva inoltre che: "sotto altro ma concorrente aspetto va notata l'irrelevanza del fatto che il sopralluogo non abbia condotto ad un procedimento sanzionatorio. La giurisprudenza più recente di questo Consiglio di Stato, da cui la Sezione non ha motivo di dissentire, ha infatti osservato che "il nostro ordinamento non tollera le denunce segrete" e come "colui il quale subisce un procedimento di controllo o ispettivo abbia un interesse qualificato a conoscere integralmente tutti i documenti amministrativi utilizzati nell'esercizio del potere di vigilanza, a cominciare dagli atti d'iniziativa e di preiniziativa, quali, appunto, denunce o esposti", per concludere nel senso che "non si può escludere che l'immediata comunicazione del nominativo del denunciante potrebbe riflettersi negativamente sullo sviluppo dell'istruttoria. Ma ciò può, a tutto concedere, giustificare un breve differimento del diritto di accesso. Non consente, invece, il diniego del diritto alla conoscenza degli atti quando ormai (come accade nella fattispecie) il procedimento ispettivo-disciplinare si è definitivamente concluso" (cfr. Sez. VI, 25 giugno 2007 n. 3601).

¹⁴³ I principi espressi nelle sentenze richiamate erano già stati affermati nella meno recente **sentenza n. 3601 del 25 giugno 2007 del Consiglio di Stato, sez. VI**. Il caso riguardava una professoressa che richiedeva al dirigente scolastico il fascicolo dei rapporti informativi resi da studenti minorenni, genitori e docenti relativi a fatti a seguito dei quali vi era stata un'ispezione del M.I.U.R. nei suoi confronti. La sentenza verrà trattata *infra* a pag. 75. Qui se ne riporta la massima: "ogni soggetto deve poter conoscere con precisione i contenuti e gli autori di esposti o denunce che, fondatamente o meno, possano costituire le basi per l'avvio di un procedimento ispettivo o sanzionatorio, non potendo la p.a. procedente opporre all'interessato esigenze di riservatezza, foss'anche per coprire o difendere il denunciante da eventuali reazioni da parte del denunciato, le quali, comunque, non sfuggirebbero al controllo dell'autorità giudiziaria".

allegati, costituenti parte integrante della relazione. In sede di appello, il M.I.U.R. sottolinea la “mancanza di un interesse concreto ed attuale, che possa ritenersi prevalente rispetto all’esigenza di preservare l’identità di coloro che hanno reso dichiarazioni sul comportamento della docente e che potrebbero essere oggetto di possibili ritorsioni”, in quanto “(...) in contatto, quotidianamente, con la professoressa e con il potere disciplinare a quest’ultima riconosciuto dalla legge”. Il Collegio condivide le argomentazioni del M.I.U.R. circa le dichiarazioni rese da altri insegnanti e dai genitori di alcuni allievi, di cui è stato reso noto all’interessata l’integrale contenuto, ma senza indicazione dei dati anagrafici dei soggetti dichiaranti e delle date in cui i singoli incontri si sono svolti, al fine di evitare la automatica individuazione dei nominativi dei soggetti interessati. Il diniego dell’Amministrazione, infatti, deve essere valutato ai sensi degli articoli 24, comma 6, lettera d), della L. 241/1990¹⁴⁴, nonché 2 e 3 del D.M. 757/1994¹⁴⁵, che esplicitamente precludono l’accesso ai documenti, la cui conoscenza possa essere causa di violazione della privacy, ma anche di pressioni o azioni pregiudizievoli da parte del destinatario delle dichiarazioni.

Il Consiglio di Stato argomenta che “in rapporto a tale quadro normativo, anche al fine di salvaguardare la genuinità delle dichiarazioni da verbalizzare in sede amministrativa, anche la giurisprudenza ha più volte confermato la sottrazione al diritto di accesso della documentazione acquisita, ad esempio, dagli ispettori del lavoro nell’ambito dell’attività di controllo loro affidata. A non diverse conclusioni si presta, ad avviso del Collegio, l’attività degli ispettori in materia scolastica, tenuto anche conto delle peculiari esigenze di tutela di soggetti minori, di cui sia stata segnalata la già compromessa serenità di rapporti con uno o più docenti, ancora in servizio nell’Istituto.

È vero che, in via generale, le necessità difensive - riconducibili ai principi tutelati dall’art. 24 della Costituzione - sono ritenute prioritarie rispetto alla riservatezza di soggetti terzi (cfr. in tal senso Cons. St., Ad Plen. 4 febbraio 1997¹⁴⁶) ed in tal senso il dettato normativo richiede che l’accesso sia garantito “comunque” a chi debba acquisire la conoscenza di determinati atti per la cura dei propri interessi giuridicamente protetti (art. 24, comma 7, L. n. 241/90 cit.); la medesima norma tuttavia - come successivamente modificata tra il 2001 e il 2005 (...) - specifica con molta chiarezza come non bastino esigenze di difesa genericamente enunciate per garantire l’accesso, dovendo quest’ultimo corrispondere ad una effettiva necessità di tutela di interessi che si assumano lesi ed ammettendosi solo nei limiti in cui sia “strettamente indispensabile” la conoscenza di documenti, contenenti “dati sensibili e giudiziari”¹⁴⁷.

Ferma restando, dunque, una possibilità di valutazione “caso per caso”, che potrebbe talvolta consentire di ritenere prevalenti le esigenze difensive in questione (cfr. Cons. St., sez. VI, 29 luglio 2008, n. 3798¹⁴⁸, che ammette l’accesso al contenuto delle dichiarazioni di lavoratori agli ispettori del lavoro, ma “con modalità che escludano l’identificazione degli autori delle medesime”), non può però dirsi sussistente una generalizzata soccombenza dell’interesse pubblico all’acquisizione di ogni possibile informazione, per finalità di controllo della regolare gestione di delicate funzioni pubbliche (al cui corretto esercizio sono talvolta connessi valori, a loro volta, costituzionalmente

¹⁴⁴ Per il comma 6, lettera d) dell’art. 24 L. 241/1990 vedi *supra* nota n. 115, pag. 55.

¹⁴⁵ Per gli artt. 2 e 3 D.M. 757/1994 vedi *supra* nota n. 125, pag. 58.

¹⁴⁶ Nella sentenza n. 5 del 4 febbraio 1997 del Consiglio di Stato in Adunanza Plenaria si stabiliva che il responsabile del servizio tossicodipendenze di una unità sanitaria locale, a tutela dei suoi interessi giuridicamente rilevanti, aveva diritto di prendere visione delle lettere, note o segnalazioni con le quali tossicodipendenti in cura, o loro genitori, avevano esposto lamentele sul suo operato, indipendentemente da esigenze di riservatezza dei tossicodipendenti stessi, o dai timori, comunque infondati, di possibili ritorsioni a loro danno (nella specie, la decisione ordinava all’amministrazione non solo di lasciar prendere visione agli interessati dei documenti richiesti, ma anche di rilasciarne copia). Per una trattazione più approfondita del caso si veda *infra* la nota n. 175, pag. 77.

¹⁴⁷ Il medesimo assunto è stato espresso più di recente nella sentenza n. 5515 del 20 novembre 2013 del Consiglio di Stato, sez. VI già esaminata a pag. 52.

¹⁴⁸ Per la sentenza n. 3798 del 29 luglio 2008 del Consiglio di Stato, sez. VI vedi *supra* nota n. 123, pag. 58.

garantiti)¹⁴⁹. Dette finalità di controllo, infatti, non potrebbero non essere compromesse dalla comprensibile reticenza dei soggetti contattati dall'organo ispettivo, ai quali non si accordasse la tutela di cui si discute; il diritto di difesa, invece, risulta comunque garantito dall'obbligo di motivazione per eventuali contestazioni, nonché dalla possibilità di ottenere accertamenti istruttori in sede giurisdizionale (accertamenti che possono essere condotti anche con piena tutela delle ricordate esigenze di riservatezza, ma con pieno accertamento dei fatti). Nella situazione in esame, - rileva l'organo giudicante - la docente interessata è stata messa in grado di conoscere fatti sufficientemente circostanziati, circa l'esistenza di plurime testimonianze su condotte reiterate, nei confronti sia degli allievi che di colleghi (per la verità, almeno questi ultimi, facilmente individuabili dall'interessata).

Sotto il profilo in questione, la sezione non ravvisa ragioni per discostarsi dal contenuto della propria sentenza 9 febbraio 2011, n. 895: nel caso di specie, l'amministrazione scolastica - sia pure con gli omissis indispensabili per non far identificare chi avesse reso le dichiarazioni - aveva consentito l'accesso alla documentazione acquisita al fine di attivare il procedimento di trasferimento d'ufficio, precisando come in quella documentazione l'istante potesse trovare ogni utile spiegazione in ordine alla pluralità degli episodi che l'avevano vista diretta protagonista, nonché alle dichiarazioni delle persone che avevano avuto percezione diretta dei fatti, rilevanti ai fini del suo trasferimento per incompatibilità ambientale (istituto che non ha finalità sanzionatorie, ma è piuttosto diretto a restituire serenità all'ambiente di lavoro in cui opera il personale dipendente, attraverso la rimozione di tutti gli ostacoli che possono incidere negativamente sul buon andamento dell'azione amministrativa)¹⁵⁰.

¹⁴⁹ Il medesimo assunto è stato espresso più di recente nella **sentenza n. 4035 del 31 luglio 2013 del Consiglio di Stato, sez. VI** già esaminata a pag. 57 e ss.

¹⁵⁰ Il Consiglio di Stato con questa sentenza aderisce ad un orientamento piuttosto datato (Tar Lazio, sez. III bis, n. 1189/2007) e, più di recente a quello risultante dalla sentenza del Consiglio di Stato, sez. VI, n. 895 del 9 febbraio 2011) sostenendo che la normativa coinvolta (l'art. 24 l. 241/1990 e gli artt. 2 e 3 del D.M. 757/1994) tutelano non solo la riservatezza dei controinteressati, ma anche l'interesse dei medesimi a non essere destinatari di azioni pregiudizievoli da parte del destinatario delle dichiarazioni. La decisione contrasta solo apparentemente con la quasi coeva **sentenza n. 4122 del 12 luglio 2012 del Consiglio di Stato, sez. IV** ove il Collegio ha rilevato che allorché prevalgono le esigenze del c.d. accesso difensivo, l'accesso è consentito nei soli limiti della visione ed esame del documento, con esclusione dell'estrazione di copia e duplicazione: "L'art. 24 dalla legge n. 241 del 1990 opera, invero, un prudente bilanciamento fra i due contrapposti interessi inerenti alla riservatezza ed alle esigenze di difesa, stabilendo che ove l'accesso sia necessario per "curare e difendere propri interessi giuridici" - tale ultima evenienza che ricorre nella fattispecie di cui è controversia - assume carattere prevalente sulla tutela della riservatezza. In tale ipotesi la soglia di tutela si sposta sulle modalità con le quali deve avvenire l'accesso - secondo quanto previsto dall'art. 25, comma 3, della legge n. 241 del 1990 - consentendo l'accesso nei soli limiti della visione ed esame del documento, con esclusione dell'estrazione di copia e duplicazione; ciò a salvaguardia di ogni potenziale divulgazione del documento oltre il limite della conoscenza da parte del soggetto direttamente interessato".

Si osservi, inoltre, che la giurisprudenza amministrativa formatasi precedentemente alla novella legislativa del 2005, riteneva che, al fine di risolvere il conflitto tra diritto di accesso e diritto alla privacy, fosse imposto al giudice, e prima ancora all'Amministrazione, di scegliere le modalità che garantivano il più possibile il rispetto dell'altrui privacy. Si riteneva, in particolare, che l'obiettivo del rispetto dell'altrui riservatezza poteva essere raggiunto attraverso una serie di modalità di accesso differenti dalla estrazione di copia, elaborate dall'Amministrazione o trovate dal giudice: l'oscuramento di alcune parti non ritenute indispensabili per la tutela di quell'interesse giuridico (c.d. omissis) o la mera visione del documento che tutela maggiormente il privato. Dopo la riforma del 2005, la giurisprudenza ha, invece, escluso che l'amministrazione destinataria dell'istanza possa limitare, per tutelare la riservatezza altrui, l'esercizio del diritto di accesso alla mera visione dei documenti, non consentendo anche l'estrazione di copia. E ciò sulla base di due considerazioni: anzitutto, la legge n. 241, come riscritta dalle novelle legislative del 2005, e il nuovo regolamento di attuazione non prevedono più la possibilità di limitare il diritto di accesso alla mera visione del documento di cui si è chiesta l'ostensione ed, inoltre, l'art. 22 espressamente definisce il diritto di accesso come il diritto degli interessati di "prendere visione e di estrarre copia" di documenti amministrativi. Sicché, in presenza dei presupposti legittimanti, occorre garantire la tutela piena dell'accesso, tramite presa visione ed estrazione di copia, senza che sia più possibile distinguere - come avvenuto nel caso della citata **sentenza n. 4122 del 12 luglio 2012 del Consiglio di Stato, sez. IV** - tra diritto alla mera visione degli atti e diritto all'estrazione di copia.

- Sentenza n. 116 del 3 febbraio 2012 – Tar Veneto, Sez. III - Argomento: diritto di accesso a denunce ed esposti da parte del destinatario di essi

Il caso in esame riguarda la richiesta di un docente di accedere a corrispondenza, relazioni, esposti e/o denunce, nonché al proprio fascicolo personale a seguito di segnalazioni presentate nei suoi confronti da colleghi, genitori ed alunni. Il dirigente scolastico negava in prima battuta l'accesso affermando la genericità della domanda e la asserita necessità di tutelare la riservatezza dei terzi.

Il professore adiva quindi la Commissione per l'accesso agli atti amministrativi di cui all'art. 25 l. 241/90¹⁵¹ che gli riconosceva un accesso parziale. Si uniformava a tale decisione il dirigente scolastico il quale si opponeva a successive richieste di accesso adducendo l'impossibilità connessa allo svolgimento di indagini ispettive.

Il Tar adito accoglie le istanze di accesso asserendo che: “la denuncia o l'esposto non possono considerarsi un fatto circoscritto al solo autore, all'Amministrazione competente al suo esame e all'apertura dell'eventuale procedimento, ma riguardano direttamente anche i soggetti denunciati, i quali ne risultano comunque incisi. Nell'ordinamento delineato dalla legge n. 241/90, ispirato ai principi della trasparenza, del diritto di difesa e della dialettica democratica, ogni soggetto deve, pertanto, poter conoscere con precisione i contenuti e gli autori di segnalazioni, esposti o denunce che, fondatamente o meno, possano costituire le basi per l'avvio di un procedimento ispettivo o sanzionatorio, non potendo la P.A. procedente opporre all'interessato esigenze di riservatezza (Tar Lombardia, sent. 1469/2008¹⁵²)”.

L'Organo giudicante conclude quindi ritenendo ostensibili gli esposti e le denunce, escludendo l'accessibilità ai rapporti informativi, mentre, per quanto concerne i documenti oggetto di corrispondenza, dispone che l'Amministrazione valuti caso per caso la riconducibilità o meno di tali documenti alle categorie sottratte all'accesso ex art. 24 L. 241/90. Infine, dispone che l'Amministrazione consenta l'accesso informale al fascicolo personale atteso l'indubbio diritto del dipendente a verificare tutti i documenti presenti nel fascicolo stesso.

- Sentenza n. 3789 del 22 ottobre 2010 - Tar Puglia, Sez. II - Argomento: accesso consentito anche in presenza di dati sensibilissimi in considerazione delle modalità con le quali è chiesto l'accesso, quando non si rileva alcuna compromissione del diritto alla riservatezza

Meritevole di esame, per la peculiarità del tema trattato, è la pronuncia citata che riguarda il diniego di accesso relativamente a documentazione sanitaria contenente dati sensibilissimi. In particolare, nell'ambito del procedimento selettivo interno preordinato al trasferimento dei cd. docenti “soprannumerari”, veniva negato alla ricorrente sig.ra X l'accesso alla certificazione medica esibita dall'odierna controinteressata afferente la figlia minore, per poter fruire dei benefici previsti dalla legge 104/1992. Nel caso di specie, la stessa ricorrente richiede che la copia del certificato in questione sia rilasciata previo oscuramento del nome della minore e della relativa diagnosi ritenendo sufficiente, ai fini della tutela delle sue ragioni in sede giudiziaria, acquisire il dato relativo allo stato di gravità cui è collegato il beneficio dell'esclusione dalla graduatoria dei docenti soprannumerari. Pertanto - come osserva il Tar che accoglie il ricorso – “sebbene la documentazione richiesta contenga potenzialmente dati cd. sensibilissimi poiché idonei a rivelare lo stato di salute di una minore, in considerazione delle modalità con le quali l'interessata stessa chiede di accedervi, non si rileva in concreto alcuna compromissione del diritto alla riservatezza”. In buona sostanza, statuisce il collegio, “i dati sensibilissimi verrebbero celati, con ciò stesso restando esclusa la necessità di operare sia la valutazione della stretta indispensabilità dell'accesso sia la comparazione ed il bilanciamento degli interessi in gioco

¹⁵¹ Per l'art. 25 L. 241/1990 vedi *infra* nota n. 158, pag. 70.

¹⁵² Per la sentenza n. 1469 del 29 ottobre 2008 del Tar Lombardia, Brescia, sez. I vedi *infra* a pag. 70.

di cui al combinato disposto degli artt. 24, comma 7 della legge 241/90 e 60 del d.lgs. 196/2003. L'accesso, pertanto, deve essere consentito alla ricorrente previo oscuramento del nome della minore e della relativa diagnosi ma secondo l'omnicomprensivo concetto risultante dalla riforma del 2005 che vi ha invero incluso sia la visione degli atti che l'estrazione di copia degli stessi, superando le originarie previsioni dell'art. 24 della legge 241/90 e con esse l'accesso limitato alla sola visione”.

- **Sentenza n. 2590 del 6 ottobre 2010 – Tar Sardegna, Sez. II - Argomento: diniego all'accesso per evitare ritorsioni dell'insegnante e per necessità di tutela dell'alunno minore**

Molto interessante è la pronuncia in esame che aderisce all'orientamento minoritario a favore del diniego all'accesso. Trattasi del ricorso proposto da una docente contro il M.I.U.R. per l'annullamento del diniego opposto all'istanza di accesso agli atti e per ottenere l'esibizione integrale di tutta la documentazione richiesta senza omissione dei nominativi degli autori dell'esposto in conseguenza del quale veniva avviato un procedimento disciplinare a carico della stessa ricorrente. In particolare, nella richiesta di accesso la docente precisava che, nonostante l'archiviazione del procedimento disciplinare a suo carico, la medesima aveva comunque un interesse diretto, concreto ed attuale in relazione alla violazione di una situazione giuridica rilevante cui sarebbe seguita, secondo le sue intenzioni, la tutela presso le sedi competenti.

L'amministrazione scolastica rigettava l'istanza, sostenendo che, essendo decaduta ogni esigenza di difesa della richiedente, non si palesava un interesse diretto, concreto ed attuale, corrispondente ad una situazione giuridicamente tutelata, collegata alla richiesta stessa.

Il Tar adito osserva che “la questione in esame investe il problema del bilanciamento e contemperamento tra il diritto di accesso ai documenti amministrativi e la tutela dei terzi i cui dati personali siano contenuti nella documentazione richiesta, con particolare riferimento all'esigenza di tutela della riservatezza dei firmatari di un esposto (...). Pur considerato che la giurisprudenza prevalente riconosce, in via generale, la necessità che venga comunque tutelato il diritto di accesso, deve prendersi atto dell'esistenza di casi particolari nei quali l'esigenza della tutela della riservatezza assume connotati speciali, come, ad esempio, nell'ipotesi di lavoratori firmatari di un esposto nei confronti del datore di lavoro che ha dato luogo ad ispezioni del Ministero del lavoro e della previdenza sociale, nella quale rileva in modo speciale l'esigenza della tutela dei lavoratori medesimi da eventuali ritorsioni del datore di lavoro¹⁵³”.

Nel caso di specie, il Collegio argomenta che “la sola mera possibilità teorica ed ipotetica di una possibile eventuale ritorsione di un insegnante su un bambino alunno della scuola primaria, comporta la necessità della rivalutazione della questione controversa nel senso di assicurare, in primo luogo, la tutela del minore, con conseguente rigetto delle richieste della ricorrente volta a conoscere i nominativi degli autori dell'esposto, che, alla luce del contenuto dell'esposto medesimo, e delle precisazioni offerte dall'amministrazione resistente, sono genitori di minori “che continuavano e continuano ad essere alunni dell'ins. XXX¹⁵⁴(...). Deve altresì ritenersi, a

¹⁵³ Si confronti la **sentenza n. 198 del 23 luglio 2001 del Tar Abruzzo, Pescara** in cui si evidenzia la particolare rilevanza dell'esigenza di tutelare quei soggetti, che svolgendo un'attività di lavoro subordinato, si pongono in una posizione particolarmente debole nei confronti del datore di lavoro, in quanto possono subire eventuali ritorsioni in relazione a quanto hanno avuto modo di esporre in eventuali denunce presentate alla Direzione provinciale del lavoro. Si vedano altresì la **sentenza n. 1604 del 19 novembre 1996 del Consiglio di Stato, sez. VI** e la **sentenza n. 822 del 17 dicembre 1997 del Tar Toscana, sez. II**: in entrambi i casi la giurisprudenza amministrativa ha precisato che non sussiste il diritto di accesso, da parte di un'impresa che abbia subito un'ispezione degli ispettori del lavoro, alla documentazione allegata al verbale ispettivo ed in particolare alle dichiarazioni rese dai dipendenti dell'impresa stessa, in relazione all'esigenza di salvaguardare la vita privata e la riservatezza dei dipendenti stessi.

¹⁵⁴ A sostegno della propria decisione il Collegio richiama il precedente giurisprudenziale del **Tar Lombardia, Milano, sez. IV, n. 5716 dell'8 novembre 2004** nel quale è stato affermato che “in tema di bilanciamento tra il diritto di accesso ai documenti amministrativi e la tutela dei terzi i cui dati personali siano contenuti nella documentazione richiesta, deve ritenersi che le esigenze di tutela della riservatezza dei firmatari di un esposto nei confronti di

giudizio del collegio, che, nel caso di specie, non possa configurarsi un effettivo pregiudizio degli interessi giuridicamente rilevanti della Signora XXX, in conseguenza del diniego opposto dall'amministrazione scolastica a fare conoscere i nominativi degli autori dell'esposto. Deve infatti ritenersi, ad una prima valutazione, che ogni richiesta di risarcimento del danno che la ricorrente possa eventualmente avanzare nei confronti degli autori dell'esposto, necessiti della previa qualificazione della rilevanza penale del contenuto dell'esposto. Ciò premesso, nulla impedisce alla ricorrente – nel caso – di presentare denuncia o querela contro ignoti sulla base dell'esposto in suo possesso e del suo contenuto, posto che, una volta ritenuta dalla competente autorità penale la possibile rilevanza penale del contenuto dell'esposto, non sussisterebbe ovviamente alcun ostacolo per la procedibilità dell'azione penale, posto che, in tal caso, i nominativi degli autori dell'esposto potrebbero essere acquisiti dal giudice penale”.

- Seduta n. 29 del 4 maggio 2010 – Commissione per l'accesso ai documenti amministrativi¹⁵⁵ presso presidenza del Consiglio dei Ministri e sentenza n. 6450 dell'8 luglio 2008 - Tar Lazio, Sez. III - Argomento: accesso agli atti di un concorso¹⁵⁶

Benché esuli dall'ambito prettamente scolastico, si ritiene utile richiamare la pronuncia del 4 maggio 2010 della Commissione per l'accesso ai documenti amministrativi, in quanto ben esplicativa sul tema del rapporto tra diritto di accesso e privacy in un settore molto delicato, quale quello dei concorsi. Nel caso esaminato il ricorrente, classificatosi al settimo posto di una graduatoria per un concorso, chiedeva di poter accedere ai documenti allegati alla domanda di presentazione da parte di altri due concorsisti classificatisi al primo e secondo posto. L'istituto resistente negava l'accesso adducendo la legittimità della graduatoria e l'opposizione dei presunti controinteressati. Avverso il provvedimento di rigetto, il ricorrente presentava ricorso alla Commissione per l'accesso ai documenti amministrativi chiedendo il rilascio e l'estrazione di copia dei documenti. Riconoscendo la fondatezza del ricorso e consentendo l'accesso, l'adita Commissione affermava - in linea con la copiosa giurisprudenza sia del giudice amministrativo sia della Commissione stessa - la pressoché **totale accessibilità dei documenti formati dalla commissione esaminatrice e prodotti dagli altri candidati**: le domande ed i documenti prodotti dai candidati, i verbali, le schede di valutazione e gli stessi elaborati costituiscono, infatti, documenti rispetto ai quali deve essere esclusa in radice l'esigenza di riservatezza a tutela dei terzi, posto che i concorrenti, prendendo parte alla selezione, hanno evidentemente acconsentito a misurarsi in una competizione di cui la comparazione dei valori di ciascuno costituisce l'essenza. **Tali atti, quindi, una volta acquisiti alla procedura, escono dalla sfera personale dei partecipanti che, pertanto, non assumono la veste di controinteressati in senso tecnico.**

Tali principi erano già stati affermati nella **sentenza n. 6450 dell'8 luglio 2008 del Tar Lazio**. Il caso riguardava il diniego opposto all'istanza di accesso presentata da un partecipante ad una procedura concorsuale di prendere visione e di estrarre copia degli elaborati di alcuni candidati che avevano superato la prova scritta. Il contestato diniego si basava sulla circostanza che l'accesso ai suddetti elaborati poteva essere consentito solamente dopo che fosse stata data opportuna comunicazione ai diretti interessati, consentendo, quindi, agli stessi di potere opporsi motivatamente a tale richiesta. La tesi dell'amministrazione resistente era stata contestata dall'istante il quale, sulla

un professionista, presentato al relativo Ordine professionale e del quale il primo chieda l'ostensione, possano essere garantite mediante la mascheratura dei nominativi. Il diritto all'accesso potrà quindi essere esercitato, dal professionista interessato, con tale modalità”.

¹⁵⁵ Per le funzioni della Commissione per l'accesso ai documenti amministrativi si veda il link: http://www.governo.it/Presidenza/DICA/4_ACCESSE/funzioni.html.

¹⁵⁶ In tema di procedure concorsuali si vedano anche le seguenti pronunce del Consiglio di Stato: Tar Campania, Napoli, sez. II, n. 3809/2006; C.d.S., sez. IV, n. 1249 del 31.10.1997; C.d.S., sez. IV, n. 5 del 13.1.1995; C.d.S., sez. VI, n. 1715 del 25.11.1994; C.d.S., sez. IV, n. 21 dell'11.1.1994.

base della giurisprudenza in materia, ne aveva prospettato l'illegittimità per palese violazione delle disposizioni di cui agli artt. 22, 24¹⁵⁷ e 25¹⁵⁸ della L. 241/1990, che disciplinano l'esercizio del diritto di accesso.

Il Collegio, nel caso di specie, riconosceva la fondatezza del gravame e osservava che **il ricorrente, avendo partecipato alla procedura concorsuale¹⁵⁹, è titolare di un interesse qualificato e differenziato alla regolarità della procedura** che, come tale, concretizza quell'"interesse personale e concreto per la tutela di situazioni giuridicamente rilevanti" che l'art. 2¹⁶⁰ del D.P.R. n. 352/1992, in puntuale applicazione dell'art. 22 della L. 241/1990, richiede quale presupposto necessario per il riconoscimento del diritto di accesso. Tale interesse era stato puntualmente

¹⁵⁷ Per gli artt. 22 e 24 L. 241/1990 vedi *supra* rispettivamente la nota n. 110, pag. 52 e la nota n. 115, pag. 55.

¹⁵⁸ In L. 241/1990, Capo V "Accesso ai documenti amministrativi", art. 25 "Modalità di esercizio del diritto di accesso e ricorsi": "1. Il diritto di accesso si esercita mediante esame ed estrazione di copia dei documenti amministrativi, nei modi e con i limiti indicati dalla presente legge. L'esame dei documenti è gratuito. Il rilascio di copia è subordinato soltanto al rimborso del costo di riproduzione, salve le disposizioni vigenti in materia di bollo, nonché i diritti di ricerca e di visura.

2. La richiesta di accesso ai documenti deve essere motivata. Essa deve essere rivolta all'amministrazione che ha formato il documento o che lo detiene stabilmente.

3. Il rifiuto, il differimento e la limitazione dell'accesso sono ammessi nei casi e nei limiti stabiliti dall'articolo 24 e debbono essere motivati.

4. Decorso inutilmente trenta giorni dalla richiesta, questa si intende respinta. In caso di diniego dell'accesso, espresso o tacito, o di differimento dello stesso ai sensi dell'articolo 24, comma 4, il richiedente può presentare ricorso al tribunale amministrativo regionale ai sensi del comma 5, ovvero chiedere, nello stesso termine e nei confronti degli atti delle amministrazioni comunali, provinciali e regionali, al difensore civico competente per ambito territoriale, ove costituito, che sia riesaminata la suddetta determinazione. Qualora tale organo non sia stato istituito, la competenza è attribuita al difensore civico competente per l'ambito territoriale immediatamente superiore. Nei confronti degli atti delle amministrazioni centrali e periferiche dello Stato tale richiesta è inoltrata presso la Commissione per l'accesso di cui all'articolo 27 nonché presso l'amministrazione resistente. Il difensore civico o la Commissione per l'accesso si pronunciano entro trenta giorni dalla presentazione dell'istanza. Scaduto infruttuosamente tale termine, il ricorso si intende respinto. Se il difensore civico o la Commissione per l'accesso ritengono illegittimo il diniego o il differimento, ne informano il richiedente e lo comunicano all'autorità disponente. Se questa non emana il provvedimento confermativo motivato entro trenta giorni dal ricevimento della comunicazione del difensore civico o della Commissione, l'accesso è consentito. Qualora il richiedente l'accesso si sia rivolto al difensore civico o alla Commissione, il termine di cui al comma 5 decorre dalla data di ricevimento, da parte del richiedente, dell'esito della sua istanza al difensore civico o alla Commissione stessa. **Se l'accesso è negato o differito per motivi inerenti ai dati personali che si riferiscono a soggetti terzi, la Commissione provvede, sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di dieci giorni dalla richiesta, decorso inutilmente il quale il parere si intende reso.** Qualora un procedimento di cui alla sezione III del capo I del titolo I della parte III del decreto legislativo 30 giugno 2003, n. 196, o di cui agli articoli 154, 157, 158, 159 e 160 del medesimo decreto legislativo n. 196 del 2003, relativo al trattamento pubblico di dati personali da parte di una pubblica amministrazione, interessi l'accesso ai documenti amministrativi, il Garante per la protezione dei dati personali chiede il parere, obbligatorio e non vincolante, della Commissione per l'accesso ai documenti amministrativi. La richiesta di parere sospende il termine per la pronuncia del Garante sino all'acquisizione del parere, e comunque per non oltre quindici giorni. Decorso inutilmente detto termine, il Garante adotta la propria decisione.

5. Le controversie relative all'accesso ai documenti amministrativi sono disciplinate dal codice del processo amministrativo".

¹⁵⁹ Per un confronto con procedure non aventi carattere comparativo, quali verifiche e valutazioni degli alunni di una classe, si veda *infra* la sentenza n. 2280 del 20 dicembre 2000 del Tar Calabria, Reggio Calabria a pag. 78.

¹⁶⁰ In D.P.R. 352/1992 "Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell'art. 24, comma 2, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi", art. 2 "Ambito di applicazione": "1. Il diritto di accesso ai documenti amministrativi è esercitato nei confronti di tutte le pubbliche amministrazioni e dei concessionari di pubblici servizi da chiunque vi abbia un interesse personale e concreto per la tutela di situazioni giuridicamente rilevanti.

2. Il diritto di accesso si esercita, con riferimento agli atti del procedimento, e anche durante il corso dello stesso, nei confronti dell'autorità che è competente a formare l'atto conclusivo o a detenerlo stabilmente.

3. Il diritto di accesso s'intende realizzato con la pubblicazione, il deposito o altra forma di pubblicità, comprese quelle attuabili mediante strumenti informatici, elettronici e telematici, dei documenti cui sia consentito l'accesso, secondo le modalità stabilite dalle singole amministrazioni ai sensi dell'art. 22, comma 3, della legge 7 agosto 1990, n. 241".

evidenziato nell'istanza di accesso nella quale il ricorrente aveva manifestato l'intenzione di valutare la legittimità degli atti della procedura concorsuale e, se del caso, di tutelare in sede giurisdizionale le proprie ragioni. Il Tar, quindi, ordinava all'intimato di esibire e consentire al ricorrente di estrarre copia degli atti richiesti con la propria istanza di accesso.

- **Sentenza n. 1469 del 29 ottobre 2008 – Tar Lombardia, Brescia, Sez. I - Argomento: segnalazioni e denunce, diritto di accesso dei soggetti denunciati**¹⁶¹

Prima di prendere in esame il caso, appare opportuno considerare il disposto di cui all'art. 59 C.P., rubricato "Accesso a documenti amministrativi" a mente del quale: *"fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico"*. Tale norma va letta in parallelo con il disposto di cui al comma 7 dell'art. 24¹⁶²

¹⁶¹ Si vedano, in particolare, nello stesso senso a favore del diritto di accesso da parte dei soggetti denunciati: la **sentenza n. 5132 del 28 settembre 2012 del Consiglio di Stato, sez. V** a pag. 63 e la meno recente, ma rilevante **sentenza n. 3601 del 25 luglio 2007 del Consiglio di Stato, sez. VI** approfondita *infra* a pag. 75.

¹⁶² Si ritiene opportuno riportare per intero il testo dell'**art. 24 della Legge 241/1990** rubricato "Esclusione dal diritto di accesso" a mente del quale: *"1. Il diritto di accesso è escluso: a) per i documenti coperti da segreto di Stato ai sensi della legge 24 ottobre 1977, n. 801, e successive modificazioni, e nei casi di segreto o di divieto di divulgazione espressamente previsti dalla legge, dal regolamento governativo di cui al comma 6 e dalle pubbliche amministrazioni ai sensi del comma 2 del presente articolo; b) nei procedimenti tributari, per i quali restano ferme le particolari norme che li regolano; c) nei confronti dell'attività della pubblica amministrazione diretta all'emanazione di atti normativi, amministrativi generali, di pianificazione e di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione; d) nei procedimenti selettivi, nei confronti dei documenti amministrativi contenenti informazioni di carattere psico-attitudinale relativi a terzi.*

2. Le singole pubbliche amministrazioni individuano le categorie di documenti da esse formati o comunque rientranti nella loro disponibilità sottratti all'accesso ai sensi del comma 1.

3. Non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.

4. L'accesso ai documenti amministrativi non può essere negato ove sia sufficiente fare ricorso al potere di differimento.

5. I documenti contenenti informazioni connesse agli interessi di cui al comma 1 sono considerati segreti solo nell'ambito e nei limiti di tale connessione. A tale fine le pubbliche amministrazioni fissano, per ogni categoria di documenti, anche l'eventuale periodo di tempo per il quale essi sono sottratti all'accesso.

6. Con regolamento, adottato ai sensi dell'articolo 17, comma 2, della legge 23 agosto 1988, n. 400, il Governo può prevedere casi di sottrazione all'accesso di documenti amministrativi: a) quando, al di fuori delle ipotesi disciplinate dall'articolo 12 della legge 24 ottobre 1977, n. 801, dalla loro divulgazione possa derivare una lesione, specifica e individuata, alla sicurezza e alla difesa nazionale, all'esercizio della sovranità nazionale e alla continuità e alla correttezza delle relazioni internazionali, con particolare riferimento alle ipotesi previste dai trattati e dalle relative leggi di attuazione; b) quando l'accesso possa arrecare pregiudizio ai processi di formazione, di determinazione e di attuazione della politica monetaria e valutaria; c) quando i documenti riguardino le strutture, i mezzi, le dotazioni, il personale e le azioni strettamente strumentali alla tutela dell'ordine pubblico, alla prevenzione e alla repressione della criminalità con particolare riferimento alle tecniche investigative, alla identità delle fonti di informazione e alla sicurezza dei beni e delle persone coinvolte, all'attività di polizia giudiziaria e di conduzione delle indagini; d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'amministrazione dagli stessi soggetti cui si riferiscono; e) quando i documenti riguardino l'attività in corso di contrattazione collettiva nazionale di lavoro e gli atti interni connessi all'espletamento del relativo mandato.

7. Deve comunque essere garantito ai richiedenti l'accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e

L. 241/90 che recita che: “deve comunque essere garantito ai richiedenti l’accesso ai documenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili e giudiziari, l’accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall’articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale”.

Venendo al caso di specie, in quell’ipotesi era stata respinta l’istanza di accesso avanzata da un genitore per acquisire copia della segnalazione pervenuta al Servizio Emergenza Infanzia 114 al fine di conoscere le generalità di chi inoltrava detta segnalazione da cui fu avviata una successiva indagine circa pretesi maltrattamenti, perpetrati in ambito familiare, nei confronti dei figli, indagine rivelatasi poi negativa. Il Comune aveva negato l’accesso, evidenziando che il diritto alla riservatezza del terzo e la tutela del segreto d’ufficio dovevano considerarsi prevalenti rispetto al diritto all’accesso ai documenti amministrativi.

Il Tar, interpellato, esamina in primo luogo, il rapporto tra il diritto di accesso e il diritto alla riservatezza richiamato dall’Amministrazione comunale a sostegno del proprio diniego. Il Collegio, accogliendo il ricorso, aderisce a quell’orientamento giurisprudenziale secondo cui il diritto alla riservatezza non può essere invocato quando la richiesta di accesso ha per oggetto, come nella presente fattispecie, il nome di coloro che hanno reso segnalazioni, denunce o rapporti informativi nell’ambito di un procedimento ispettivo. L’organo giudicante evidenzia che il rapporto tra diritto di accesso e diritto alla riservatezza è stato risolto dal legislatore ricorrendo al Codice Privacy, alla Legge 241/90, alla Legge 15/2005 e al D.P.R. 184/2006 che hanno, in buona sostanza, avanzato la soglia di tutela dell’accesso. In particolare, il richiamo è agli artt. 59 C.P. e 24, comma 7 L. 241/90 già citati.

Nel caso in esame, l’istanza dei ricorrenti non riguardava dati sensibili di cui all’art. 60 per cui il Tar sottolinea che la denuncia o l’esposto non può considerarsi un fatto circoscritto al solo autore, all’Amministrazione competente al suo esame e all’apertura dell’eventuale procedimento, ma riguarda direttamente anche i soggetti “denunciati”, i quali ne risultano comunque incisi. Ciò vale a maggior ragione quando tali denunce hanno sviluppi così penetranti come quelli che hanno coinvolto, nel caso di specie, la sfera personale e familiare dei ricorrenti. Nell’ordinamento delineato dalla L. 241/1990, ispirato ai principi della trasparenza, del diritto di difesa e della dialettica democratica, ogni soggetto deve, pertanto, poter conoscere con precisione i contenuti e gli autori di segnalazioni, esposti o denunce che, fondatamente o meno, possano costituire le basi per l’avvio di un procedimento ispettivo o sanzionatorio, non potendo la P.A. procedente opporre all’interessato esigenze di riservatezza. La tolleranza verso denunce segrete e/o anonime, del resto, è un valore estraneo al nostro ordinamento giuridico. Emblematico, in tal senso, è l’art. 111 Cost. che, nel sancire (come elemento essenziale del giusto processo) il diritto dell’accusato di interrogare o far interrogare le persone che rendono dichiarazioni a suo carico, inevitabilmente presuppone che l’accusato abbia anche il diritto di conoscere il nome dell’autore di tali dichiarazioni. Tale sfavore verso le denunce e le dichiarazioni anonime emerge poi, a più riprese, anche dal codice di procedura penale: si pensi all’art. 240 c.p.p. in forza del quale i documenti che contengono dichiarazioni anonime non possono essere acquisiti né in alcun modo utilizzati, salvo che costituiscano il corpo del reato o provengano comunque dall’imputato; all’art. 195, comma 7, c.p.p. che sancisce l’inutilizzabilità della testimonianza di chi si rifiuta o non è in grado di indicare la persona o la fonte

giudiziari, l’accesso è consentito nei limiti in cui sia strettamente indispensabile e nei termini previsti dall’articolo 60 del decreto legislativo 30 giugno 2003, n. 196, in caso di dati idonei a rivelare lo stato di salute e la vita sessuale”.

La lettura dell’art. 24 L. 241/1990 va completata esaminando il **D.P.R. 352/1992** “Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell’art. 24, comma 2, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”.

da cui ha appreso la notizia dei fatti oggetto dell'esame; all'art. 203 c.p.p. che pure prevede l'inutilizzabilità delle informazioni rese dagli informatori alla polizia giudiziaria quando il nome di tali informatori non venga svelato.

Da questa cornice emerge, quindi, chiaramente che al diritto alla riservatezza, pure costituzionalmente rilevante, non può certo riconoscersi ampiezza tale da includere il "diritto all'anonimato" di colui che rende una dichiarazione a carico di terzi nell'ambito di un procedimento ispettivo o sanzionatorio. L'anonimato sulle denunce o sulle dichiarazioni accusatorie è, al contrario guardato con particolare sospetto dall'ordinamento: da qui l'evanescenza e l'infondatezza di ogni tentativo volto a qualificare tale inesistente diritto all'anonimato come una prerogativa del diritto alla riservatezza¹⁶³.

Quanto poi al rapporto tra diritto di accesso e segreto professionale (dell'assistente sociale)¹⁶⁴ anch'esso richiamato dall'Amministrazione comunale a sostegno del proprio diniego, il Tar evidenzia come in linea di principio il segreto professionale rientri nell'ambito delle ipotesi, previste dall'art. 24 della Legge 241/90, che prevalgono sul diritto all'accesso. Questo non significa comunque che tutti gli atti formati o detenuti dal soggetto su cui incombe il segreto professionale siano automaticamente sottratti all'accesso, poiché si tratta di applicare una deroga, pur prevista dall'ordinamento, al principio generale, previsto dallo stesso ordinamento, dell'accessibilità a tutti gli atti dell'Amministrazione: trattandosi di una deroga, essa va applicata secondo il principio di stretta interpretazione. Il Collegio ritiene, infatti, che all'istanza di accesso formulata dai ricorrenti non possa essere legittimamente opposto il segreto professionale che incombe sull'assistente sociale del Comune. Al riguardo, osserva che: la segnalazione di pretesi maltrattamenti in famiglia (recante il nominativo di colui che ha effettuato detta segnalazione) non è pervenuta all'assistente sociale da un proprio informatore confidenziale, ma attraverso un servizio di pubblica utilità gestito da un ente terzo; si tratta di un documento formatosi all'esterno dell'ambito di competenza propria dell'assistente sociale e detenuto dall'Amministrazione comunale in quanto ente preposto ai relativi controlli; la circostanza secondo cui il documento contenente detta segnalazione sia pervenuto all'assistente sociale del Comune costituisce un semplice aspetto dell'organizzazione interna del Comune stesso, in cui può esistere una partizione organizzativa (ad esempio l'area o settore servizi sociali); è, di conseguenza, il Comune a dover garantire il diritto d'accesso non potendosi trincerare dietro uno specifico segreto professionale che non può trovare applicazione nel caso in esame.

- **Sentenza n. 1842 del 22 aprile 2008 – Consiglio di Stato, Sez. VI- Argomento: diniego all'accesso e prevalenza dell'interesse pubblico all'acquisizione di ogni possibile informazione, a tutela della sicurezza e regolarità dei rapporti di lavoro, rispetto al diritto di difesa delle società o imprese sottoposte ad ispezione**

Aderente all'orientamento minoritario a favore della prevalenza del diritto alla riservatezza rispetto a quello alla difesa è la sentenza in esame, peraltro citata da tutte quelle successive del medesimo tenore¹⁶⁵. Il caso riguardava, come tanti altri, la materia ispettiva ed, in particolare, la richiesta da parte di una società di prendere visione ed estrarre copia dei documenti inerenti l'ispezione effettuata dall'Ispettorato del Lavoro e conclusasi con verbali di contestazione di illeciti inerenti la

¹⁶³ Il medesimo principio era già stato espresso nella meno recente **sentenza n. 3601 del 25 luglio 2007 del Consiglio di Stato, sez. VI** di cui trattasi *infra* a pag. 75 (richiamo a pag. 76).

¹⁶⁴ In particolare, l'Amministrazione evidenzia che, nel caso in esame, trova applicazione l'obbligo di segreto di cui all'**art. 1 della Legge n. 119/2001**, secondo cui: "*Gli assistenti sociali iscritti all'albo professionale istituito con legge 23 marzo 1993, n. 84, hanno l'obbligo del segreto professionale su quanto hanno conosciuto per ragione della loro professione esercitata sia in regime di lavoro dipendente, pubblico o privato, sia in regime di lavoro autonomo libero-professionale*".

¹⁶⁵ Si vedano, in particolare, *supra*: la **sentenza n. 5515 del 20 novembre 2013 del Consiglio di Stato, sez. VI** a pag. 52 e ss. (richiamo della pronuncia a pag. 57) e la **sentenza n. 4035 del 31 luglio 2013 del Consiglio di Stato, sez. VI** a pag. 57 e ss. (richiamo della pronuncia a pag. 58).

posizione di numerosi collaboratori. L'accesso, negato dall'Amministrazione a motivo della salvaguardia da possibili azioni pregiudizievoli, recriminatorie e/o di pressione nei confronti dei lavoratori e collaboratori della società, veniva invece consentito dal Tar Liguria in considerazione delle esigenze di difesa della società ricorrente, nonché della già avvenuta cessazione dei rapporti di lavoro in contestazione.

In sede di appello, l'Amministrazione sottolineava come, viceversa, il diniego di accesso dovesse ricondursi, nella fattispecie, all'esigenza di salvaguardare la riservatezza e la vita privata di soggetti terzi, in considerazione della peculiarità del rapporto sottostante, trattandosi di rapporto di lavoro normalmente caratterizzato dalla presenza di una "parte debole", il lavoratore, per il quale era giustificata una maggiore tutela da parte dell'ordinamento.

Le ragioni difensive dell'appellante sono pienamente condivise dal Consiglio di Stato che evidenzia come: *"le disposizioni in materia di diritto di accesso mirano a coniugare la ratio dell'istituto, quale fattore di trasparenza e garanzia di imparzialità dell'Amministrazione – come enunciato dall'art. 22 della citata legge n. 241/90¹⁶⁶ – con il bilanciamento da effettuare rispetto ad interessi contrapposti, fra cui – specificamente – quelli dei soggetti "individuati o facilmente individuabili" che dall'esercizio dell'accesso vedrebbero compromesso il loro diritto alla riservatezza"* (art. 22 cit., comma 1, lettera c); *il successivo articolo 24 della medesima legge, che disciplina i casi di esclusione dal diritto in questione, prevede al sesto comma casi di possibile sottrazione all'accesso in via regolamentare e fra questi – al punto d)¹⁶⁷ – quelli relativi a "documenti che riguardino la vita privata o la riservatezza di persone fisiche, persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all'Amministrazione dagli stessi soggetti a cui si riferiscono". In via attuativa, il D.M. 4.11.1994, n. 757 (regolamento concernente le categorie di documenti, formati o stabilmente detenuti dal Ministero del lavoro e della previdenza sociale sottratti al diritto di accesso) inserisce fra tali categorie – all'art. 2, lettere b) e c)¹⁶⁸ – "i documenti contenenti le richieste di intervento dell'Ispettorato del Lavoro", nonché "i documenti contenenti notizie acquisite nel corso delle attività ispettive, quando dalla loro divulgazione possano derivare azioni discriminatorie, o indebite pressioni o pregiudizi a carico di lavoratori o di terzi".*

In rapporto a tale inequivoco quadro normativo, anche la giurisprudenza ha più volte confermato la sottrazione al diritto di accesso della documentazione, acquisita dagli ispettori del lavoro nell'ambito dell'attività di controllo loro affidata (cfr., fra le tante, Cons. St., sez. VI, 27.1.1999, n. 65 e 19.11.1996, n. 1604). Nessuna ragione, nel caso di specie, giustifica una deroga alle regole ed alle pronunce sopra ricordate: ***l'avvenuta cessazione di un rapporto di lavoro non esclude, infatti, l'esigenza di riservatezza di chi abbia reso dichiarazioni, riguardanti se stesso o anche altri soggetti, senza autorizzarne la divulgazione, non attenendo la sfera di interessi in questione alla sola tutela delle posizioni del lavoratore ed essendo queste ultime, comunque, rilevanti anche in rapporto all'ambiente professionale di appartenenza, più largamente inteso.***

Sembra appena il caso di sottolineare, al riguardo, ***la prevalenza dell'interesse pubblico all'acquisizione di ogni possibile informazione, a tutela della sicurezza e della regolarità dei rapporti di lavoro, rispetto al diritto di difesa delle società o imprese sottoposte ad ispezione: il primo, infatti, non potrebbe non essere compromesso dalla comprensibile reticenza di lavoratori, cui non si accordasse la tutela di cui si discute, mentre il secondo risulta comunque garantito dall'obbligo di motivazione per eventuali contestazioni e dalla documentazione che ogni datore di lavoro è tenuto a possedere***¹⁶⁹.

¹⁶⁶ Per l'art. 22 L. 241/1990 vedi *supra* nota n. 110, pag. 52.

¹⁶⁷ Per il comma 6, lettera d) dell'art. 24 L. 241/1990 vedi *supra* nota n. 115, pag. 55.

¹⁶⁸ Per l'art. 2 del D.M. 757/1994 vedi *supra* nota n. 125, pag. 58.

¹⁶⁹ Identico principio è stato espresso anche nella più recente sentenza n. 4035 del 31 luglio 2013 del Consiglio di Stato, sez. VI approfondita a pag. 57 (richiamo pag. 59).

- Sentenza n. 3601 del 25 luglio 2007 – Consiglio di Stato, Sez. VI- Argomento: prevalenza del diritto di difesa rispetto al diritto alla riservatezza¹⁷⁰

Aderente all'orientamento giurisprudenziale prevalente a favore del diritto alla difesa anche in ambito ispettivo, per lo meno scolastico, è la sentenza citata anch'essa richiamata dalle più recenti pronunce ad essa conformi¹⁷¹.

Nel caso di specie, una docente richiedeva al dirigente scolastico il fascicolo dei rapporti informativi resi da studenti minorenni, genitori e docenti relativi a fatti a seguito dei quali vi era stata un'ispezione del M.I.U.R. nei suoi confronti. Il dirigente, presa visione del pertinente fascicolo, constatava che, pur non essendovi informazioni relative a religione, salute e inclinazioni sessuali sui soggetti coinvolti, vi erano i nomi degli alunni minorenni, dei genitori e dei colleghi che avevano esposto i fatti descritti nel ricorso. Negava pertanto l'ostensione.

Contro tale provvedimento di diniego la professoressa proponeva ricorso ex art. 25 legge n. 241/1990¹⁷², al Tar del Lazio, il quale ordinava all'Amministrazione l'ostensione della documentazione integrale da lei richiesta, ivi compresi, quindi, i nomi degli autori delle dichiarazioni.

Avverso tale decisione proponevano appello, chiedendone in via cautelare la sospensione, il M.I.U.R. e l'Ufficio Scolastico Regionale per il Lazio. La docente proponeva a sua volta appello incidentale che veniva accolto per le seguenti motivazioni. Il Collegio ritiene, anzitutto, che: *“gli autori degli esposti informativi (i cui nomi sono oggetto dell'istanza di accesso presentata dalla ricorrente) non possono essere qualificati controinteressati in senso tecnico. Tali sono infatti non tutti coloro che, a qualsiasi titolo sono nominati o coinvolti nel documento oggetto dell'istanza ostensiva, ma solo coloro che per effetto dell'ostensione vedrebbero pregiudicato il loro diritto alla riservatezza. Ebbene, pur non potendosi sottovalutare l'ampliamento e la progressiva importanza assunta dal diritto alla riservatezza, il Collegio ritiene, tuttavia, che tale situazione giuridica concerna solo quelle vicende collegate in modo apprezzabile alla sfera privata del soggetto, e non anche quelle destinate ad assumere una dimensione di carattere pubblico. Il diritto alla riservatezza non può allora certamente essere invocato quando la richiesta di accesso ha ad oggetto, come nella presente fattispecie, il nome di coloro che hanno reso denunce o rapporti informativi nell'ambito di un procedimento ispettivo (in questi termini, Cons. Stato, sez. V, 22 giugno 1998, n. 923). La denuncia o l'esposto, invero, non può considerarsi un fatto circoscritto al solo autore e all'Amministrazione competente al suo esame ed all'apertura dell'eventuale procedimento, ma riguarda direttamente anche i soggetti “denunciati”, i quali ne risultano comunque incisi. Ciò vale a maggior ragione quando tali denunce hanno sviluppi così penetranti come quelli che hanno coinvolto, nel caso di specie, la sfera personale e professionale della professoressa che, per i fatti oggetto di quegli esposti, è stata sottoposta a procedimento ispettivo-disciplinare e a procedimento penale (all'esito dei quali, peraltro, è risultata estranea agli addebiti mossi). Nell'ordinamento delineato dalla L. 241/1990, ispirato ai principi della trasparenza, del diritto di difesa e della dialettica democratica, ogni soggetto deve, pertanto, poter conoscere con precisione i contenuti e gli autori di esposti o denunce che, fondatamente o meno, possano costituire le basi per l'avvio di un procedimento ispettivo o sanzionatorio, non potendo la p.a. procedente opporre all'interessato esigenze di riservatezza, foss'anche per coprire o difendere il denunciante da eventuali reazioni da parte del denunciato, le quali, comunque, non sfuggirebbero al controllo dell'autorità giudiziaria.”*

¹⁷⁰ Il medesimo principio - costituente fin da questa pronuncia orientamento nettamente prevalente - è espresso, oltre che in quelle esaminate nella trattazione, in svariate altre pronunce, anche precedenti (*ex multis*: Tar Campania, Napoli, sez. VI, n. 14859 del 16 giugno 2010; Tar Lombardia, Milano, sez. I, n. 1030 del 5 aprile 2006; Tar Lombardia, Milano, sez. IV, n. 5716 dell'8 novembre 2004).

¹⁷¹ Si vedano *supra* a pag. 63 la sentenza n. 5132 del 28 settembre 2012 del Consiglio di Stato, sez. V e la sentenza n. 3081 del 19 maggio 2009 del Consiglio di Stato, sez. V richiamata alla nota n. 142, pag. 63.

¹⁷² Per l'art. 25 L. 241/1990 vedi *infra* nota n. 158, pag. 70.

La tolleranza verso denunce segrete e/o anonime è un valore estraneo al nostro ordinamento giuridico. Emblematico, in tal senso, è l'art. 111 Cost. che, nel sancire (come elemento essenziale del giusto processo) il diritto dell'accusato di interrogare o far interrogare le persone che rendono dichiarazioni a suo carico, inevitabilmente presuppone che l'accusato abbia anche il diritto di conoscere il nome dell'autore di tali dichiarazioni (...). Da questa cornice emerge chiaramente che al diritto alla riservatezza, pure costituzionalmente rilevante, non può certo riconoscersi ampiezza tale da includere il "diritto all'anonimato" di colui che rende una dichiarazione a carico di terzi nell'ambito di un procedimento ispettivo o sanzionatorio. L'anonimato sulle denunce o sulle dichiarazioni accusatorie è, al contrario, come si è visto, guardato con particolare sospetto dall'ordinamento: da qui l'evanescenza e l'infondatezza di ogni tentativo volto a qualificare tale inesistente diritto all'anonimato come una prerogativa del diritto alla riservatezza¹⁷³.

Peraltro, evidenzia il Collegio, "la pubblica amministrazione cui è indirizzata la richiesta di accesso, se individua controinteressati è tenuta a dare comunicazione agli stessi, mediante invio di copia con raccomandata con avviso di ricevimento, o per via telematica per coloro che abbiano consentito tale forma di comunicazione. Non risulta, tuttavia, che tale comunicazione sia mai stata inviata agli autori delle dichiarazioni il che dimostra che anche l'Amministrazione ha ritenuto (almeno fino alla costituzione in giudizio davanti al Tar) che la richiesta dalla professoressa non fosse tale da investire il diritto alla riservatezza di nessun soggetto terzo (...).

Non può allora dubitarsi che colui il quale subisce un procedimento di controllo o ispettivo abbia un interesse qualificato a conoscere integralmente tutti i documenti amministrativi utilizzati nell'esercizio del potere di vigilanza, a cominciare dagli atti d'iniziativa e di preiniziativa, quali, appunto, denunce o esposti. Certo, non si può escludere che l'immediata comunicazione del nominativo del denunciante potrebbe riflettersi negativamente sullo sviluppo dell'istruttoria. Ma ciò può, a tutto concedere, giustificare un breve differimento del diritto di accesso. Non consente, invece, il diniego del diritto alla conoscenza degli atti quando ormai (come accade nella fattispecie) il procedimento ispettivo-disciplinare si è definitivamente concluso".

- Sentenza n. 3536 del 28 marzo 2006 – Consiglio di Stato, Sez. VI - Argomento: accesso integrale a registri e verbali del Consiglio di classe

Nel caso di specie i genitori di un alunno frequentante la classe seconda di un liceo scientifico – assumendo l'esistenza di un clima di ostilità nell'istituto scolastico frequentato dal figlio nei riguardi del figlio stesso - chiedevano l'accesso integrale a registri e verbali del Consiglio di classe, sostenendo di non poter considerare e valutare il trattamento riservato al figlio se non in comparazione con quello riservato agli altri alunni della classe.

Il primo giudice aveva respinto il ricorso avverso il diniego di accesso alla documentazione richiesta: ai ricorrenti venivano mostrate le pagine del registro di classe che riguardavano il loro figlio e non quelle degli altri alunni, a tutela di asserite esigenze di privacy degli stessi e sostenendo che le pagine del registro date in visione ai genitori ben avrebbero assolto al compito di consentire la conoscibilità di quanto di loro interesse.

La sentenza veniva appellata ed il ricorso accolto. Va precisato che gli appellanti, nella loro istanza di accesso, avevano chiesto di prendere visione e di estrarre copia dei registri della seconda classe del liceo, con riguardo al periodo di frequenza del figlio, "previo oscuramento, ove necessario, dei dati sensibili relativi ad alunni diversi dal proprio figlio". La sezione riteneva, innanzitutto, la sussistenza dell'interesse degli appellanti alla richiesta di accesso, in quanto essi non potevano considerare e valutare il trattamento riservato al figlio se non in comparazione con quello riservato agli altri alunni della classe. Inoltre, la riservatezza dei terzi poteva essere comunque salvaguardata

¹⁷³ Il medesimo principio viene espresso più di recente anche nella **sentenza n. 1469 del 29 ottobre 2008 del Tar Lombardia, Brescia, sez. I** a pag. 71 (richiamo a pag. 73).

(ad esempio, schermando i nomi degli alunni, come già a suo tempo richiesto dagli appellanti), senza limitare il diritto di accesso. Invero, l'interesse alla riservatezza, tutelato dalla normativa mediante una limitazione del diritto di accesso (art. 24, comma 7 L. 241/90 e art. 8, comma 5, lett. d), del D.P.R. 27 giugno 1992, n. 352¹⁷⁴), recede quando l'accesso stesso sia esercitato, come nella fattispecie in esame, per la difesa di un interesse giuridico, nei limiti in cui esso è necessario alla difesa di quell'interesse (Cons. Stato, ad. plen., 4 febbraio 1997, n. 5¹⁷⁵). Nella specie, l'accesso è

¹⁷⁴ Il riferimento alla necessità di difesa di un interesse emerge anche nel **D.P.R. 352/1992** *“Regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, in attuazione dell’art. 24, comma 2, della legge 7 agosto 1990, n. 241, recante nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi”*. In particolare all’**art. 8** rubricato *“Disciplina dei casi di esclusione”*, comma 5, è disposto che: *“(…) i documenti amministrativi possono essere sottratti all’accesso: (… d) quando i documenti riguardino la vita privata o la riservatezza di persone fisiche, di persone giuridiche, gruppi, imprese e associazioni, con particolare riferimento agli interessi epistolare, sanitario, professionale, finanziario, industriale e commerciale di cui siano in concreto titolari, ancorché i relativi dati siano forniti all’amministrazione dagli stessi soggetti cui si riferiscono. Deve comunque essere garantita ai richiedenti la visione degli atti dei procedimenti amministrativi la cui conoscenza sia necessaria per curare o per difendere i loro stessi interessi giuridici”*.

¹⁷⁵ Il caso, pur esulando dall’ambito scolastico, è analogo a quello testé esaminato ed è degno di nota. Trattasi della **sentenza n. 5 del 4 febbraio 1997 del Consiglio di Stato in Adunanza Plenaria** già esaminata *supra* alla nota n. 146, pag. 65. Un coadiutore sanitario responsabile del Servizio Tossicodipendenze (SER.T) presso la U.S.L. di X impugnava - con ricorso al TAR delle Marche - il rifiuto della Regione Marche di consentire all’interessato l’accesso a tutte le lettere, note o segnalazioni pervenute al Servizio sanità della Regione, concernenti la sua persona quale responsabile del SER.T dell’azienda sanitaria. Il TAR adito dichiarava inammissibile il gravame per mancanza di motivazione della domanda di accesso, condannando il ricorrente al pagamento delle spese processuali. Avverso tale decisione l’interessato proponeva appello. La Sezione IV del Consiglio di Stato rilevava che il soggetto che del procedimento è parte ha, in quanto tale, un diritto incondizionato di prendere visione degli atti del procedimento a norma dell’art. 10 della legge 241/90 e salvo comunque il disposto dell’art. 24. Nella specie, osservava che, contrariamente a quanto ritenuto dal Tribunale, la domanda di accesso, concernendo atti aventi ad oggetto lagnanze rivolte al richiedente in qualità di responsabile del SER.T doveva considerarsi implicitamente motivata, stante l’evidenza dell’interesse cui era preordinata.

Nel merito la Sezione ha rilevato che la questione controversa attiene al conflitto tra accesso e riservatezza dei terzi e che va esaminata nei suoi profili generali, a nulla rilevando che le persone nei cui confronti si invoca il diritto alla difesa appaiano, in ragione della condizione di tossicodipendenti e della soggezione ai poteri del sanitario responsabile della struttura presso la quale sono in cura, i soggetti più deboli.

La Sezione sottolinea a tale proposito come la gerarchia degli interessi appaia chiaramente delineata dal legislatore con norme primarie tassative, dalle quali è dato ricavare la prevalenza del diritto alla riservatezza dei terzi come regola, e viceversa del diritto di accesso, qualora venga in rilievo il fine di curare o difendere interessi giuridici.

Il riconoscimento legislativo nel nostro ordinamento del principio di pubblicità dei documenti amministrativi segna un totale cambiamento di prospettiva, perché comporta che se finora il segreto era la regola e la pubblicità l’eccezione, ora è vero il contrario. Di fronte all’esercizio del diritto di accesso, è la Pubblica amministrazione che deve giustificare il proprio rifiuto all’accesso, motivandolo con la necessità di proteggere mediante il segreto uno o più degli interessi previsti dal legislatore. L’esigenza di motivazione del segreto fondata sul rapporto fra determinate informazioni (che l’Amministrazione ritiene debbano essere segrete) e determinati interessi (che il legislatore ha previsto debbano essere protetti) indica il passaggio anche nel nostro ordinamento da una concezione soggettiva e “personale” del segreto amministrativo ad una concezione oggettiva e “reale”, più consona ad un’Amministrazione moderna. Il segreto amministrativo, cioè, non è più rapportato alla “qualità” della persona che lo detiene, bensì alla “qualità” delle informazioni protette dal segreto; nel segreto di nuovo tipo ciò che rileva è la “qualità” delle informazioni, cioè il loro rapporto con determinati interessi, non la “qualità” del soggetto che le detiene, prevale in sostanza l’elemento oggettivo e “reale” costituito dalle informazioni oggetto del segreto e quindi, indirettamente, dagli interessi che ne formano il vero contenuto. Al rispetto di tale nuovo principio, in base al quale la regola generale è l’accesso e le ipotesi in cui i documenti possono essere sottratti all’accesso sono soltanto eccezioni, è informato anche l’**art. 8** del regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi, approvato con **D.P.R. 27 giugno 1992 n. 352** in attuazione dell’art. 24 secondo comma della L. 7 agosto 1990 n. 241. Sia la norma primaria (art. 24 secondo comma lett. d) L. n. 241 del 1990) sia la norma regolamentare (art. 8 quinto comma, lett. d) D.P.R. n. 352 del 1992) hanno cercato di contemperare esigenze diverse, stabilendo che i richiedenti, di fronte a documenti che riguardano la vita privata o la riservatezza di altri soggetti, non possono ottenere copia dei documenti, né trascriverli, ma possono solo prendere visione degli “atti” di quei procedimenti amministrativi che sono relativi ai loro interessi. Si deve, pertanto, concludere che l’interesse alla riservatezza, tutelato dalla normativa mediante

stato chiesto ai fini della tutela dei diritti e degli interessi legittimi del minore, ivi compresa la richiesta di risarcimento danni patiti dal medesimo a causa di eventuali comportamenti non conformi a diritto posti in essere nei suoi confronti.

- Sentenza n. 2280 del 20 dicembre 2000 – Tar Calabria, Sez. Reggio Calabria - Argomento: accesso limitato agli atti che riguardano l'alunno e non anche gli altri alunni

Per completezza espositiva si ritiene opportuno prendere in esame una pronuncia che si colloca in direzione diametralmente opposta rispetto a quella sopra esaminata. Nel caso di specie, un padre proponeva ricorso contro il diniego all'accesso agli atti (verifiche, valutazioni, ecc...) relativi all'andamento scolastico di tutta la classe frequentata dal proprio figlio.

Il ricorso veniva respinto: il Collegio riteneva che il genitore di un alunno ha sicuramente diritto all'esibizione di tutti gli atti relativi all'andamento scolastico del proprio figlio, ma non anche a quelli relativi a verifiche e a valutazioni riferite a tutti gli altri alunni della classe, la cui conoscenza non si appalesa necessaria alla difesa degli interessi del ricorrente. Nel caso in esame, infatti, non venendo in rilievo una procedura a carattere comparativo, non è configurabile un interesse a conoscere l'operato dell'Amministrazione riguardante altri soggetti. Sul punto, la giurisprudenza ha avuto modo di precisare che nelle procedure concorsuali, il diritto di accesso alla documentazione amministrativa si estende anche alla ricognizione degli elaborati degli altri candidati, che per loro natura sono destinati al confronto con quelli degli altri concorrenti, in un necessario giudizio di relazione proprio di ogni competizione concorsuale o paraconcorsuale¹⁷⁶. La fattispecie in esame si colloca, invece, al di fuori di una procedura concorsuale e si riduce al rapporto tra l'alunno e l'Amministrazione scolastica. Sul punto il Collegio condivide quanto osservato dall'Amministrazione resistente, secondo la quale *“la conoscenza della documentazione relativa alle verifiche e alle valutazioni degli altri alunni è ininfluente (...) per comprendere la giustezza delle verifiche e delle valutazioni dell'alunna (...)”*. Ciò per l'ininfluenza del giudizio comparativo, proprio delle valutazioni competitive come i concorsi, sulla correttezza della determinazione negativa che si intende contestare: infatti, la legittimità del giudizio negativo dell'alunno interessato prescinde dall'andamento scolastico degli altri alunni e va accertata sulla base di parametri oggettivi riconducibili a criteri valutativi astrattamente definiti.

- Sentenza n. 5845 del 10 marzo 2000 – Consiglio di Stato, Sez. VI - Argomento: sussistenza dell'interesse all'accesso agli atti ispettivi a prescindere dall'adozione o meno di provvedimenti disciplinari

Interessante è infine la pronuncia qui richiamata con la quale il Consiglio di Stato si spinge oltre il mero diritto di accesso per finalità difensive, riconoscendo un **più ampio diritto dell'istante a verificare la correttezza dell'azione amministrativa riguardante la propria sfera giuridica**.

una limitazione del diritto di accesso, recede quando l'accesso stesso sia esercitato per la difesa di un interesse giuridico, nei limiti ovviamente in cui esso è necessario alla difesa di quell'interesse.

Passando poi all'esame del caso che ha dato luogo alla controversia, il Consiglio di Stato rileva che il parziale rifiuto all'accesso viene giustificato dalla Regione con l'esigenza di salvaguardare la riservatezza di terzi, nella specie pazienti tossicodipendenti del Ser.T. di X, al fine di non deteriorare il rapporto medico paziente. Il diniego, cioè, non riguarda i “documenti” e le informazioni in esso contenute, bensì la “qualità” dei soggetti denunciati, per cui la Regione sembra avere esercitato, sia pure per ragioni di rilevante valore sociale, un potere discrezionale di diniego che la legge non le conferisce. L'appellante, conclude quindi il Consiglio di Stato, ha diritto di prendere visione dei documenti rifiutati dalla Regione né vi è ragione per ritenere che da tale conoscenza possano derivare possibili ritorsioni nei confronti dei pazienti tossicodipendenti.

¹⁷⁶ Per un confronto con le procedure concorsuali si vedano *supra* la **seduta n. 29 del 4 maggio 2010 della Commissione per l'accesso ai documenti amministrativi** e la **sentenza n. 6450 dell'8 luglio 2008 del Tar Lazio, Sez. III** a pag. 69.

Nel caso di specie, un'insegnante elementare chiedeva l'accesso alla relazione dell'indagine ispettiva nella quale era stata coinvolta per presunte irregolarità, al fine di conoscerne l'esito al pari dell'oggetto preciso dell'accertamento disposto nei suoi riguardi. L'accesso le era stato negato e, a seguito di ricorso, consentito. L'Amministrazione impugnava ed il Consiglio di Stato respingeva l'appello evidenziando come per pacifica giurisprudenza non assuma rilevanza ostativa la circostanza della mancata adozione di provvedimenti disciplinari o sanzionatori all'esito dell'ispezione, posto che l'interesse giuridico idoneo a sorreggere la pretesa esibitoria non coincide necessariamente con la difesa in giudizio, ma si identifica in modo più ampio con l'aspirazione a verificare la correttezza dell'azione amministrativa riguardante la sfera giuridica dell'istante.

IL DIRIGENTE
Stefano Suraniti

MIUR – Ufficio Scolastico Regionale per il Piemonte
Corso Vittorio Emanuele II, 70 Torino
Ufficio VI e Ufficio VII
Dirigente Stefano SURANITI
Rif. [Natalie OLIVERO](#) 011.5163604 natalie.olivero@istruzione.it