Chi, come il sottoscritto, si occupa di documentazione didattica si trova spesso ad interrogarsi sulla legittimità o meno di un determinato
uso delle immagini a scuola
.

Le norme sulla privacy vengono spesso interpretate in maniera arbitraria e questo alimenta molta confusione.

Aggiungo inoltre che, a mio modesto parere, come spesso accade nel nostro Paese, si finisce per passare da un eccesso all'altro: da una reale violazione indiscriminata dei dati personali, ad un eccesso di tutela che finisce per penalizzare l'esigenza irrinunciabile della documentazione.

{loadposition user7}

Ecco dunque l'autorevole parere di Anna Armone sull'uso delle immagini a scuola.

Importante la sottolineatura dell'inutilità della negoziazione di un consenso da parte delle famiglie alla ripresa fotografica dei bambini , indispensabile quando invece chi riprende è un soggetto privato.

Altrettanto importante la differenziazione fatta tra registrazione di immagini e video e diffusione degli stessi. Come potrete leggere, essendo considerate le immagini come dati personali, ogni forma di diffusione oltre la stretta cerchia scolastica-familiare, sarebbe vietata.

Mi chiedo però come sia conciliabile questa interpretazione normativa con altre leggi, come quella dell'obbligo di trasferire l'albo pretorio e tutta la comunicazione scuola - famiglia online, compresi elenchi delle classi ed altri documenti in cui i dati personali risultano assai più diretti di una semplice foto diffuse allo scopo di documentare un determinato percorso didattico relizzato, come dice la norma, a fini istituzionali.

L’uso delle immagini nella scuola
Per una corretta interpretazione della norma

di Anna Armone

Premessa.

Il trattamento dei dati personali diventa “problema” con la nascita della rete, che consente a chiunque di venire a conoscenza di dati riguardanti persone fisiche o giuridiche. Nel presente scritto ci riferiremo al trattamento dei dati ordinari, cioè quelli che consentono di identificare un soggetto.

Le norme giuridiche che regolano il trattamento dei dati personali tendono a garantire l’individuo nei confronti di chiunque abusi del trattamento stesso, ledendo la dignità della persona o esponendola a rischi.

In questo contesto gli alunni devono essere visti come portatori del diritto alla riservatezza e alla protezione dei dati personali. Ma proprio in quanto studenti la loro posizione va analizzata nel contesto di riferimento. È quello che cercheremo di fare, evidenziando le differenze di tutela che derivano dai diversi contesti in cui i diritti su richiamati possono essere violati.

Il contesto scolastico è istituzionalmente pubblico, disciplinato dalle norme di organizzazione amministrativa. Si perseguono interessi pubblici costituzionalmente garantiti che coincidono con l'interesse individuale. Si tratta di una discriminante chiara tra le attività che intercorrono tra privati per loro libera adesione e le attività poste in essere da un soggetto che svolge una funzione sociale e, nel caso della scuola, irrinunciabile da parte del privato cittadino.

Il trattamento di dati personali degli alunni, ancorché comuni, da parte della scuola, deve tener conto della pericolosità potenziale del trattamento, avendo la stessa una responsabilità che deve andare oltre la valutazione dell'immediatezza. Si tratta di valutazioni che il privato non deve fare, poiché in questo caso l'interessato decide liberamente della disponibilità delle informazioni che lo riguardano. Proprio per questo motivo dobbiamo comprendere perché il legislatore ha voluto evidenziare questa differenza tra il regime del trattamento dei dati personali riferito a soggetti privati e il regime riferito a soggetti pubblici.

Una prima riflessione va fatta sul concetto di interesse pubblico.

Mentre gli interessi individuali sono quelli che fanno capo all'individuo; gli interessi collettivi sono gli interessi di quelle entità sociali intermedie promananti dalla comunità che l'ordinamento giuridico qualifica in senso oggettivo, perché sono centri di interesse e di attività alle quali sono immediatamente da riferire quegli interessi e da imputare quelle attività e le loro conseguenze; gli interessi pubblici, infine, sono quelli che hanno come punto di riferimento soggettivo la stessa comunità generale o anche comunità minori che di quella siano derivazioni o anche entità che, comunque, siano dall'ordinamento riconosciute come figure soggettive pubbliche.

La realizzazione di tali interessi costituisce l'interesse pubblico "concreto" perseguito dall'amministrazione che, nel valutarlo deve regolarsi secondo i principi di imparzialità e buon andamento.

Nel sistema dell'istruzione e della formazione qual è l'interesse pubblico da perseguire? Quello declinato nell'art. 30 della Costituzione e negli articoli 1 e 2 del d.lgs n. 297/1994.

La scuola pubblica non è un qualsiasi contraente che offre un servizio negoziabile, bensì un

soggetto che svolge una funzione sociale. Pertanto non possiamo immaginare una scuola che agisce in veste di privato con i genitori nell'ambito dell'attuazione del diritto alla riservatezza. La scuola ha sempre una funzione istituzionale da svolgere; al di fuori di essa non è ammissibile alcuna attività.

I dati che riguardano gli alunni

La scuola rappresenta un settore delicato per la mole di dati personali che circolano al suo interno e verso l'esterno. Il legislatore ha ritenuto di dedicare due soli articoli a questo comparto, articoli che, peraltro, riprendono precedenti normative.

L'art. 96 del Codice conferma il diritto alla riservatezza degli studenti già previsto dallo Statuto delle studentesse e degli studenti. Il contenuto generico della disposizione – la comunità scolastica promuove la solidarietà tra i suoi componenti e tutela il diritto dello studente alla riservatezza – si presta all'individuazione di una molteplicità di situazioni. La tutela della riservatezza in ambito scolastico mira ad evitare che divulgazioni non corrette di dati personali possano ledere la personalità dello studente, indipendentemente dai soggetti che possono realizzare la turbativa, siano essi docenti che personale di segreteria che terzi.

Nell'ambito dei dati relativi agli alunni, una gran parte vengono forniti direttamente dagli stessi o dalla famiglia, altri sono frutto dell'attività svolta nella scuola. Tra le attività scolastiche vanno annoverati eventi, quali le recite, che nulla hanno a che fare con le norme sulla privacy. Come ha spiegato il Garante, le riprese filmate o fotografiche dei propri figli sono fatte a fini personali e destinate ad un ambiente familiare, per cui il loro uso è legittimo.

L'uso delle immagini e dei filmati nella scuola. I limiti e le modalità di utilizzazione

Le finalità della scuola sono rinvenibili nel sistema normativo e in particolare nelle modalità di realizzazione del diritto individuale all'istruzione e all'educazione. Tale missione comporta che la scuola persegua il suo obiettivo anche in dissonanza con la volontà degli stessi genitori. Richiamiamo questo comportamento perché nel caso specifico delle immagini, accade spesso che siano gli stessi genitori a chiederne l'uso o siano oltremodo orgogliosi dell'apparire del proprio figlio. Purtroppo la diffusione e la rete in particolare espongono i minori ad una serie di pericoli che non possono essere tutti previsti, né prevedibili.

La scuola non può considerare il bambino come un utente qualsiasi, ma un soggetto di cui ha responsabilità sociale. Ecco perché non si ritengono applicabili in modo analogico le regole applicabili nei rapporti tra la famiglia e l'editore (la negoziazione del consenso).

Abbiamo più volte richiamato le varie attività dell'istituzione scolastica che portano ad utilizzare dati personali degli alunni. Le immagini e i filmati costituiscono dati personali o fonti di rinvenimento di dati personali.

Quando e perché la scuola deve utilizzare immagini degli alunni? Rientra tale attività tra quelle finalizzate al raggiungimento delle finalità istituzionali? Se ci attestassimo su questa domanda non faremmo molta strada, visto che il percorso didattico pedagogico può intraprendere diversi percorsi per la sua realizzazione.

Dobbiamo, invece, partire dai alcuni punti fermi:

- le immagini costituiscono dati personali;
- la comunicazione di immagini deve seguire il dettato normativo dell'art. 19 del Codice. Ciò significa che deve essere prevista da norme di legge o regolamento o, in mancanza, essere necessaria alla realizzazione delle finalità istituzionali;
- la diffusione deve, parimenti, attenersi al successivo comma dello stesso articolo 19, va a dire deve essere prevista esplicitamente da una norma di legge: "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" .

Nella scuola sono diverse le occasioni che possono portare alla comunicazione e alla diffusione dell'immagine di un minore. Il primo caso è quello di operatori esterni, fotografi, che

riprendono il minore al fine di documentare un certo evento (l'inizio dell'anno scolastico, la recita, la manifestazione sportiva ecc.). In questo caso il comportamento che la scuola deve tenere deve essere improntato alla massima vigilanza sulle attività che si svolgono al suo interno. Relativamente al caso concreto il dirigente deve verificare le credenziali del fotografo e fare in modo di mettere lo stesso in contatto con le famiglie. Saranno le stesse a decidere se prestare il loro consenso alla realizzazione fotografica. In questo caso il consenso è necessario, trattandosi di soggetto privato.

La stessa procedura va adottata nel caso in cui la scuola, nel corso di un partenariato con soggetti esterni, gestisca eventi o manifestazioni, le cui rappresentazioni fotografiche verranno usate per comunicare l'evento a mezzo stampa o televisione. La scuola può esclusivamente mettere in contatto il soggetto esterno con le famiglie per la gestione della procedura di richiesta del consenso. Pensiamo ad un percorso teatrale che prevede la ripresa finale, che il soggetto partner vorrebbe utilizzare a fini divulgativi. La scuola deve fare in modo che le famiglie vengano informate sull'uso che si vuole fare della ripresa e in quel contesto, se d'accordo, può esprimere il consenso al trattamento delle immagini.

La scuola, al contrario, potrebbe organizzare essa stessa la realizzazione di un servizio fotografico mirato a documentare un certo evento. L'attività è lecita se esercitata nell'ambito di attività istituzionali, ma, per quanto riguarda la diffusione di tali immagini, non si rinviene una disposizione che lo consenta. Le immagini devono rimanere agli atti della scuola, in qualità di documentazione del percorso didattico e/o formativo.

Gli stessi principi valgono per i filmati aventi come soggetto i bambini. Al fine della realizzazione o documentazione di attività istituzionali, la scuola deve provvedere alla loro conservazione documentale. Se, invece, la scuola intende utilizzare i filmati per la partecipazione a mostre, fiere, concorsi, occorre fare in modo che il soggetto titolare del trattamento (ad es. Rai, tv locale, associazioni, ecc.) ottenga dall'interessato il consenso. La scuola farà da tramite tra il titolare e la famiglia.

Affrontiamo il caso più delicato relativo alla riproduzione di immagini di minori su giornalini di scuola e/o su siti web di libero accesso.

Il giornale di classe o di scuola rientra nella consuetudine della didattica di ogni ordine e grado; nasce dalla voglia di comunicare degli studenti, e dalla necessità di avere uno strumento rappresentativo che possa far conoscere il proprio pensiero agli altri. In quest'ottica il giornale

scolastico è un elemento forte di comunicazione ed un ambiente in cui si sperimentano vari tipi di scrittura. Le cautele da adottare dipendono dal grado di diffusione del giornalino stesso. Una distribuzione limitata alle famiglie degli allievi va gestita come comunicazione di dati personali. Pertanto, il genitore, all'inizio dell'anno scolastico, in occasione della consegna dell'informativa, ex art. 13 del Codice, avrà notizia dell'uso che sarà fatto delle immagini e, se lo riterrà opportuno, chiederà, ai sensi dell'art. 7 del Codice, che le immagini non vengano utilizzate.

Se, diversamente, il giornalino ha una diffusione indiscriminata, ad esempio viene distribuito sul territorio, non v'è dubbio che si tratti di diffusione di dati personali. In questo caso non è consentito pubblicare foto di minori riconoscibili, anche se legate ad eventi positivi. La ragione di tale comportamento da tenere sta nell'analisi degli indicatori di liceità che devono condurre l'azione. Gli indicatori della pertinenza e non eccedenza sono in primo piano Essi comportano una scrupolosa verifica dell'adeguatezza dei dati agli scopi del trattamento. Se scopo del trattamento specifico è il riconoscimento di un merito al minore per un suo successo scolastico, non v'è ragione di divulgare una sua foto corredata da nome e cognome, poiché basterebbe citare il suo nome di battesimo e la classe per evidenziarne i meriti.

Caso ancora più potenzialmente pericoloso è il sito web della scuola e la pubblicazione sullo stesso del giornalino scolastico. La messa a disposizione della rete, senza alcuna limitazione dell'accesso, crea rischi potenziali di utilizzo delle informazioni illimitati. Ma, senza considerare questo estremo effetto dell'uso delle immagini, basta soffermarsi sul concetto di necessarietà del trattamento del dato. Lo sforzo che bisogna compiere è quello di mirare al raggiungimento del risultato, sia esso il riconoscimento di un merito del bambino, sia esso l'informazione sulle attività che la scuola svolge. È l'invasività che va tenuta sotto controllo. Gli stessi risultati vanno perseguiti con il mezzo e le modalità meno invasive. Esse non devono essere potenzialmente foriere di danno per il minore e non solo in modo diretto, ma anche indiretto (basta pensare a relazioni familiari e parentali difficili, effetti di problemi economici ecc.).

Per concludere, sembra azzardato estendere le disposizioni relative all'attività giornalistica alla scuola, assumendo per analogia la determinazione contenuta in un provvedimento del Garante (Provv. 31 luglio 2002 doc. web n. 1065798), il quale prevede l'applicazione delle regole contenute nella l. 675/1996, art. 25, comma 4 bis, a chiunque si trovi a svolgere, anche occasionalmente, attività di pubblicazione o diffusione di articoli, saggi e altre manifestazioni del pensiero [1] . Il legislatore ha voluto differenziare il regime legale del trattamento della comunicazione e diffusione di dati personali da parte di soggetti pubblici. La specialità della posizione di tali soggetti non ammette deroghe, ma continui richiami alla funzione di garanzia che devono svolgere.

L’uso delle immagini e dei filmati da parte di soggetti interni alla scuola per fini personali

Sin dalla Direttiva MIUR del 30 novembre 2007 sono state diverse le sollecitazioni per un uso personale corretto delle immagini nella scuola da parte di studenti e operatori scolastici. Da ultimo il Garante alla privacy ha in una nota, ha elencato, tra gli altri, tali trattamenti. Purtroppo, non è stato abbastanza chiaro sulle caratteristiche e le finalità di tali operazioni. Infatti, il consenso di cui tratta la nota, si riferisce a trattamenti operati ad uso personale da studenti e operatori scolastici. Sono coloro che a titolo personale utilizzano strumenti elettronici per registrare immagini, filmati o suoni. La richiesta di consenso qui richiamata non riguarda l’istituzione scolastica nell’esercizio delle sue attività istituzionali, ma singoli e privati cittadini che devono rispettare le disposizioni del codice della privacy, tra cui l’art. 23 che prevede la richiesta del consenso da parte dei soggetti privati.

La videosorveglianza a scuola

Atti di vandalismo posti in essere da studenti o da soggetti estranei alla scuola, stanno portando sempre più spesso alla considerazione della possibilità di installare sistemi di videosorveglianza.

Il Garante ha affrontato in modo specifico il problema con un provvedimento del 29 aprile 2004, introducendo quattro principi fondamentali.

Principio di Liceità: i dati devono essere trattati in maniera lecita, cioè secondo le prescrizioni normative. In base a questo principio il trattamento di dati raccolti attraverso un

sistema di videosorveglianza è possibile solo se fondato su uno dei presupposti di liceità previsti dal Codice della Privacy. Tali presupposti, indicati dal Garante, si differenziano a seconda del soggetto titolare del trattamento dei dati. Noi esamineremo esclusivamente il caso in cui il trattamento è effettuato da soggetto pubblico.

Relativamente all'uso di strumenti di videosorveglianza da parte di soggetti pubblici, il Garante afferma che "u*n soggetto pubblico può effettuare attività di videosorveglianza solo ed esclusivamente per svolgere funzioni istituzionali* (art. 18-22 del Codice della Privacy) *che deve individuare ed esplicitare con esattezza e di cui sia realmente titolare in base all'ordinamento di riferimento. Diversamente, il trattamento dei dati non è lecito, anche se l'ente designa esponenti delle forze dell'ordine in qualità di responsabili del trattamento, oppure utilizza un collegamento telematico in violazione del Codice*". Si sottolinea comunque che la differenza principale con quanto previsto in precedenza consiste nel fatto che la videosorveglianza per fini istituzionali non è soggetta al preventivo consenso dell'interessato, come stabilisce l'ultimo comma del paragrafo 5.2 del provvedimento sulla videosorveglianza che richiama l'art. 18 comma 4 del Codice della Privacy.

Non è quindi lecito, nemmeno per un soggetto pubblico, procedere ad una videosorveglianza capillare di intere aree cittadine, riprese integralmente e costantemente e senza adeguate esigenze.

Del pari è vietato il collegamento telematico tra più soggetti, a volte raccordati ad un "centro" elettronico, che possa registrare un numero elevato di dati personali e ricostruire interi percorsi effettuati in un determinato arco di tempo.

Contrariamente a quanto prospettato da alcuni enti locali, l'informativa agli interessati deve essere fornita nei termini illustrati nel paragrafo 3.1 del provvedimento sulla videosorveglianza e non solo mediante pubblicazione sull'albo dell'ente, oppure attraverso una temporanea affissione di manifesti.

Tali soluzioni possono concorrere ad assicurare trasparenza in materia, ma non sono di per sé sufficienti per l'informativa che deve aver luogo nei punti e nelle aree in cui si svolge la videosorveglianza.

Contrariamente a quanto si potrebbe pensare il Garante specifica che: "*Benché effettuata per la cura di un interesse pubblico, la videosorveglianza deve rispettare i principi già richiamati* ".

I principi richiamati sono quelli di liceità, proporzionalità, necessità e finalità in esame. Ciò significa che l'ente pubblico per perseguire le sue finalità con la videosorveglianza è comunque soggetto a tutti gli altri adempimenti previsti dalla legge eccetto che richiedere la manifestazione del consenso da parte degli interessati. Insomma non si applica il principio di bilanciamento degli interessi, non è necessario.

Principio di necessità: evitare un uso superfluo della videosorveglianza e, in particolare, fare a meno di identificare le persone quando l'obiettivo delle riprese può essere raggiunto anche attraverso inquadrature anonime (si pensi, per esempio, al monitoraggio del traffico); altro accorgimento è quello di predisporre l'impianto in modo che possa automaticamente e periodicamente cancellare le immagini eventualmente registrate;

Principio di proporzionalità: i dati non devono essere eccedenti rispetto alle finalità e devono essere conservati solo per il tempo necessario in relazione ai quali sono raccolti e trattati. In base a questo principio bisogna commisurare la necessità del sistema di videosorveglianza al concreto rischio che vuole essere evitato con l'installazione dello stesso sistema, escludendo quindi la videosorveglianza in aree che non sono soggette a pericolo, con particolare riferimento a quei sistemi installati a mero fine di prestigio; la videosorveglianza è lecita solo se è rispettato questo principio sia in relazione a "se installare" sia in relazione a che "cosa e quali apparecchiature installare". Sul punto si richiama integralmente il paragrafo 2.3 del provvedimento generale sulla videosorveglianza che deve essere letto con attenzione.

Procedendo ad un'analisi dettagliata è necessario evidenziare i seguenti precetti.

- Si deve evitare la rilevazione di dati in aree che non sono soggette a concreti pericoli analogamente con riferimento ad attività che non sono soggette a pericoli o per le quali non ricorre un'effettiva esigenza di deterrenza, esempio tipico sono le telecamere che vengono installate per meri fini di apparenza o di "prestigio.

- Prima d'installare un sistema di videosorveglianza (anche se il Garante utilizza il termine ambiguo di "attivare", come se fosse utile e possibile installare e non attivare un sistema di videosorveglianza) è necessario valutare che altre misure sono da considerarsi insufficienti o inattuabili, in sostanza la videosorveglianza dovrebbe essere l'*estrema ratio*.

Principio di finalità: i dati devono essere raccolti e trattati per scopi determinati, espliciti e legittimi. In base a questo principio il titolare del trattamento può perseguire con la videosorveglianza solo finalità di sua pertinenza, esclusivamente per scopi determinati, espliciti e legittimi.

Il Garante ha invece constatato che taluni soggetti (pubblici e privati) si propongono abusivamente, quale scopo della videosorveglianza, finalità di sicurezza pubblica, prevenzione o accertamento dei reati, finalità queste che invece competono solo ad organi giudiziari o di polizia giudiziaria oppure a forze armate o di polizia.

Ciò significa, (come scrive Corrado Giustozzi) che, *ad esempio, la sorveglianza di aree pubbliche, scuole, musei, contro il vandalismo non può essere svolto da istituzioni diverse dalla polizia, alla quale evidentemente occorre rivolgersi per fare installare telecamere laddove serva… e ammesso soprattutto che la polizia abbia tempo e possibilità di occuparsi anche di queste cose* .

Diversi i casi in cui i sistemi di videosorveglianza sono in realtà introdotti come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti. In ogni caso possono essere perseguite solo le finalità comunicate attraverso l'informativa, ossia direttamente

conoscibili attraverso comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria), e non finalità generiche o indeterminate, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti (art. 11, comma 1, lett. b), del Codice). Le finalità così individuate devono essere correttamente riportate nell'informativa.

A scuola le telecamere sono ammesse solo in casi eccezionali come, ad esempio, il controllo dell'Istituto dopo il protrarsi di atti vandalici. L'impianto va attivato dopo l'orario di chiusura della scuola.

Adempimenti

Informativa – Il primo e fondamentale degli adempimenti richiamati dal Garante, a cui il titolare non può sottrarsi, è costituito dall'obbligo d'informare tutti i soggetti che potranno potenzialmente essere ripresi dal sistema di videosorveglianza.

E' necessario cioè informare gli interessati che stanno per accedere o che si trovano in un'area videosorveglianza. Inoltre il titolare deve avvertire gli interessati se le immagini raccolte con il sistema di videosorveglianza vengono semplicemente rilevate oppure registrate e deve informare anche delle finalità del trattamento.

L'informativa circa la presenza di sistemi di videosorveglianza deve avvenire sempre, anche in occasione di spettacoli pubblici o attività pubblicitarie e deve fornire gli elementi previsti dall'art. 13 del Codice della Privacy, anche con formule sintetiche ma chiare.

Il Garante ha dato un'indicazione di massima dell'avviso sintetico che può essere affisso in aree esterne, precisando che in luoghi diversi dalle aree esterne l'avviso semplificato va integrato con almeno un avviso circostanziato, il quale deve riportare tutti gli elementi indicati nell'art. 13 del Codice della Privacy.

Il supporto con l’informativa semplificata:

- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze ma non necessariamente a contatto con la telecamera;

- deve avere formato e posizionamento che lo rendano immediatamente visibile;

- può inglobare un simbolo d’immediata comprensione (il logo o l’immagine di una telecamera);

- non è necessario che sia indicata la presenza di tutte le telecamere, ma è necessario che tutte le aree che vengono video sorvegliate siano dotate degli appositi cartelli di avvertimento.

L’avvertimento circa la presenza delle telecamere è necessario in relazione al principio di necessità. Infatti, la videosorveglianza costituisce un sostanziale vincolo alla libertà dei cittadini, che può estrinsecarsi anche solo in un condizionamento del loro comportamento. E’ per questo motivo che viene vietato ogni uso superfluo di telecamere.

Documentazione delle scelte – Il titolare deve documentare le ragioni delle scelte effettuate in un atto autonomo, il quale dovrà essere conservato presso il titolare (o il responsabile ove designato). Tale documento dovrà essere redatto per iscritto (sarà bene dargli anche data certa).

Il documento delle scelte deve indicare quali soluzioni operative del sistema di videosorveglianza sono state adottate e i motivi di tali scelte che dovranno essere suffragati, se del caso, da casi precedenti che hanno imposto la scelta indicata.

Il documento delle scelte deve quindi indicare:

- se sia sufficiente, ai fini della sicurezza, rilevare immagini che non rendono identificabili i singoli cittadini, anche tramite ingrandimenti, ovvero se sia realmente essenziale, ai fini prefissi, raccogliere immagini dettagliate e per quale motivo;

- quali dati vengono rilevati e se essi vengono o no registrati e, in tale caso, per quale periodo di tempo verrà conservata la registrazione e il motivo di tale scelta, indicando eventualmente i casi precedenti a cui si fa riferimento per giustificare tale scelta;

- se ci si avvale di una rete di comunicazione o una banca di dati indicizzata, ovvero se si utilizzano funzioni di fermo-immagine o tecnologie digitali, anche se abbinate ad altre informazioni o interconnesse con altri sistemi gestiti dallo stesso titolare o da terzi, ed il motivo di tale scelta;

- se avviene la ripresa di luoghi privati o accessi di edifici e per quale motivo;

- se vengono utilizzate specifiche soluzioni quali il collegamento ad appositi “centri” cui inviare segnali di allarme sonoro o visivo, oppure l’adozione di interventi automatici per effetto di meccanismi o sistemi automatizzati d’allarme (chiusura accessi, afflusso di personale di vigilanza, ecc.) ed il motivo di tale scelta;

- se avviene l’eventuale duplicazione delle immagini registrate e per quale motivo;

- i soggetti designati quali incaricati del trattamento dei dati (a visionare le immagini), anche se soggetti “esterni” al titolare, e la diversificazione dei diversi livelli di accesso al sistema e all’utilizzo delle informazioni con esso raccolte, anche con riferimento alle eventuali esigenze di manutenzione.

Si tratta in sostanza dell'obbligo per il titolare di documentare le scelte effettuate ed i motivi specifici che le giustificano.

Il documento delle scelte, che costituisce una chiave di lettura del sistema di sicurezza installato, dovrà essere conservato presso il titolare e dovrà essere messo a disposizione degli interessati che, muniti di un documento d'identità valido, intendano far valere i diritti di cui all'art. 7 del Codice della Privacy.

Misure di sicurezza – Se i dati vengono conservati dovranno, inoltre, essere protetti da idonee misure di sicurezza, in modo da ridurre il rischio di perdita accidentale dei dati o di accesso non autorizzato ovvero di trattamento non consentito o non conforme alla finalità indicata. In particolare la banca dati, ove vengano raccolte le immagini registrate, deve essere sempre protetta da una doppia chiave fisica o logica.

Le misure minime obbligatorie, indicate all'art. 33 del Codice della Privacy e specificate nell'allegato B al Codice, dovranno essere rispettate al fine di evitare le sanzioni di carattere penale previste dal Codice stesso24.

La seconda parte del paragrafo 3.3.2 del provvedimento sulla videosorveglianza dispone:

"*Alcune misure, c.d. "misure minime", sono obbligatorie anche sul piano penale. Il titolare del trattamento che si avvale di un soggetto esterno deve ricevere dall'installatore una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle regole in materia* ".

Tra queste regole il Garante richiama espressamente l'allegato B al Codice della Privacy il quale dispone: "*Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere all'esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente*

disciplinare tecnico ".

Va detto che la terminologia usata dal Garante nel provvedimento sulla videosorveglianza è soggetta a differente interpretazione e può far nascere gravi incomprensioni.

La confusione nasce per l'utilizzazione fatta dal Garante del termine INSTALLATORE che genericamente identifica il soggetto che installa un sistema di videosorveglianza, ma che è anche il termine utilizzato per individuare il soggetto che, su incarico del titolare, provvede a conformare un determinato sistema alle misure minime di sicurezza volute dal Codice della Privacy. Lampante è la differenza che c'è tra l'installatore del sistema di videosorveglianza e l'installatore delle misure minime di sicurezza.

Verifica preliminare – Quando il sistema di videosorveglianza è potenzialmente lesivo di diritti, libertà fondamentali e/o dignità dei cittadini è necessario interpellare preventivamente il Garante per una verifica preliminare circa la liceità del suo utilizzo.

In particolare il Garante prescrive la verifica preliminare quando il sistema di videosorveglianza preveda una raccolta d'immagini collegata e/o incrociata e/o confrontata con particolari dati personali (quali ad esempio quelli biometrici), oppure con codici identificativi di carte elettroniche o con dispositivi che rendono identificabile la voce (sistemi di riconoscimento vocale); la verifica preliminare occorre anche quando le immagini sono digitalizzate o indicizzate, cioè risulta possibile una ricerca automatizzata o nominativa (ad esempio quando inserendo nella banca dati delle immagini registrate un nominativo è possibile consultare tutte le immagini che lo ritraggono), ovvero, infine, nel caso di videosorveglianza dinamico – preventiva che non si limiti a riprendere luoghi in via statica, ma rilevi percorsi o caratteristiche fisionomiche (riconoscimento facciale) o eventi improvvisi, oppure comportamenti non preventivamente classificati.

In tali casi deve essere il Garante, in via preventiva, ad autorizzare il trattamento (anche attraverso autorizzazioni generali.

Notificazione – L’art. 37 del Codice della Privacy viene richiamato dal Garante nel provvedimento sulla videosorveglianza solo per ricordare che l’adempimento della notificazione deve essere effettuato dal titolare esclusivamente se rientra nei casi specifici indicati dalla norma di legge.

La notificazione al Garante della Privacy è una dichiarazione con la quale un soggetto pubblico o privato rende noto al Garante per la protezione dei dati personali l’esistenza di un’attività di raccolta e di utilizzazione dei dati personali da egli svolta quale autonomo Titolare del trattamento.

Conclusioni

Nel corso di un’intervista, Stefano Rodotà, già Garante per la privacy fino al 2003, raccontava che in una scuola elementare Usa, posero al collo dei bambini un medaglione Rfid per controllarli anche in bagno. Una bambina tornando a casa aveva protestato: “Non voglio diventare un pacchetto di cereali”. In una scuola elementare italiana, per bloccare gli atti di vandalismo, un preside chiese l’autorizzazione a mettere la videosorveglianza. Rodotà alzò il telefono e gli ha chiese “è un educatore o un poliziotto? E poi che fa, denuncia il bambino vandalo? Non si preoccupa di verificare perché il bimbo non ama la scuola?».

Alla domanda dell’intervistatore sulla risposta fornita dal Preside, Rodotà raccontò che quello, imbarazzato, rispose: “Lei dice?”.

La videosorveglianza è uno strumento da utilizzare in modo intelligente, altrimenti delega la difesa alla tecnologia e de-responsabilizza. E’ un sistema peraltro costosissimo, inefficiente, che ha effetti boomerang. E’ vero che ci sono aree metropolitane a rischio: il problema è bonificarle, non solo acciuffare i delinquenti. E quando si tratta di una scuola è opportuno valutare le variabili esterne, ma anche ciò che si offre e si comunica all’interno.

Fonte: Educazione&Scuola

{jcomments on}

{loadposition user6}