LA VIDEOSORVEGLIANZA NELLE SCUOLE: TRATTAMENTO DEI DATI PERSONALI E RISPETTO DELLA PRIVACY

In data 8 maggio 2013 è stato pubblicato, dopo lungo trattenimento in istruttoria, il Provvedimento del Garante della Privacy n. 230 del Registro dei Provvedimenti[1], concernente l'utilizzo della videosorveglianza in un asilo nido privato.
In tale struttura era stato installato un sistema di ripresa video nell'area didattica dell'asilo, che consentiva la trasmissione dei fotogrammi dei bambini quando essi erano affidati alle maestre, e la visualizzazione attraverso internet dei fotogrammi stessi da parte dei genitori dei bambini muniti di credenziali identificative.
Il Garante, piuttosto prevedibilmente, ha dichiarato illecito tale trattamento e ha vietato l'ulteriore trattamento delle immagini.
La pronuncia offre l'occasione per una breve disamina della possibilità di utilizzo della videosorveglianza nelle scuole, tematica – questa – che involve delicati profili sia in relazione al trattamento dei dati personali, sia in relazione al rispetto della legge n. 300/70.

Principi generali e utilizzo della videosorveglianza ai fini di tutela della proprietà.
Allo stato attuale dell'evoluzione normativa e dell'interpretazione che di essa viene data, i sistemi di videosorveglianza nelle scuole vengono esplicitamente ritenuti leciti solo se utilizzati con presupposti e modalità tali da non essere più ritenuti soddisfacenti da quella parte di opinione pubblica, che, anche alla luce degli infami fatti di cronaca purtroppo resi noti negli ultimi anni, invocherebbe un utilizzo più libero dei mezzi di videosorveglianza a tutela dei minori.
Dal punto di vista della disciplina sul trattamento dei dati personali, l'installazione e l'utilizzo di un sistema di videosorveglianza nelle scuole comportano innanzitutto il rispetto della fonte principale in materia, cioè il d. lgs. 196/03, nonché, in modo più specifico, del Provvedimento in materia di videosorveglianza del Garante datato 8 aprile 2010 e pubblicato sulla Gazzetta Ufficiale n. 99 del 29 aprile 2010[2].
Ovviamente, vi sono anche altri Provvedimenti del Garante in materia di videosorveglianza che, pur riguardando casi specifici sottoposti al vaglio della suddetta Autorità, consentono ugualmente di ricavare principi generali sempre applicabili a ogni ipotesi di videosorveglianza.
Importantissime indicazioni sono poi contenute nel Parere 2/2009 sulla "*Protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole)*", adottato l'11 febbraio 2009 dal Gruppo di Lavoro articolo 29 sulla protezione dei dati personali[3], e nella guida del Garante della Privacy "*La privacy tra i banchi di scuola*"[4], ove è contenuto un apposito paragrafo dedicato alla videosorveglianza.
Inoltre, anche l'art. 2, comma 2, del D.P.R. n. 249/1998, nel riconoscere esplicitamente "*il diritto dello studente alla riservatezza*", obbliga a tenere conto di tale diritto quando si affronta l'eventuale installazione di un impianto di videosorveglianza.
L'analisi dei provvedimenti dell'Autorità indipendente lascia trasparire un dato certo: la videosorveglianza è tuttora vista nell'ottica del Garante come un strumento particolarmente invasivo, e da utilizzare con l'ausilio di una serie di accorgimenti tali da limitare il più possibile l'intrusione nella vita privata degli interessati.
Da questo punto di vista, il problema del rispetto dei principi di liceità, necessità, proporzionalità e finalità sanciti dal d. lgs. 196/03[5], che devono informare ogni trattamento di dati personali, si pone in modo ancora più stringente laddove il trattamento venga effettuato con mezzi teoricamente invasivi in modo particolare (quali la videosorveglianza) e possa riguardare anche soggetti sottoposti a particolare tutela nell'interesse del corretto sviluppo della loro personalità (come ad

1 doc. web n. 2433401.
2 doc. web n. 1712680.
3 Consultabile in lingua italiana su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_it.pdf .
4 Si tratta di una sorta di vademecum pubblicato in forma di opuscolo che è possibile reperibile anche all'indirizzo internet http://www.garanteprivacy.it/documents/10160/2416443/La_privacy_tra_i_banchi_di_scuola.pdf .
5 Cfr. art. 3 e art. 11 del d. lgs. 196/03.

esempio i minori).
L'installazione di un sistema di videosorveglianza in una scuola deve innanzitutto rispettare il principio di liceità: il trattamento di dati può essere lecitamente effettuato da privati ed enti pubblici economici solamente se vi sia il consenso preventivo dell'interessato oppure se ricorra uno dei presupposti di liceità previsti in alternativa al consenso[6], o lo svolgimento di funzioni istituzionali per gli enti pubblici non economici[7]; dovrà essere fornita agli interessati un'idonea informativa, anche breve ma ben visibile, da collocarsi nelle immediate adiacenze delle aree sottoposte a riprese; dovranno essere designati incaricati del trattamento con differenti competenze di accesso, ed eventualmente uno o più responsabili del trattamento; dovranno essere adottate idonee misure di sicurezza che riducano al minimo i rischi di distruzione, di perdita (anche accidentale), di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini[8]; nel caso in cui sia stato scelto un sistema che preveda la conservazione delle immagini, la conservazione dovrà essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché l'ipotesi in cui si debba aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.
Bisogna inoltre considerare che il principio di liceità comporta che la videosorveglianza debba avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, anche di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi; nel caso specifico, assume particolare rilievo il rispetto delle norme dello Statuto dei Lavoratori.
Il rispetto del principio di necessità comporta poi che i sistemi di videosorveglianza vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi, e in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.
Il principio di proporzionalità obbliga il titolare, da un lato, a installare un impianto di videosorveglianza solo quando altre misure siano correttamente valutate insufficienti o inattuabili; dall'altro, a scegliere in ogni fase del trattamento la concreta modalità di utilizzo della videosorveglianza che sia sufficiente ma non ridondante per raggiungere la finalità perseguita.
In base al principio di finalità, gli scopi perseguiti dal titolare devono essere determinati, espliciti e legittimi[9], e il titolare può perseguire solo finalità di sua pertinenza: ad esempio, finalità di sicurezza pubblica, prevenzione o accertamento dei reati competono solo ad organi giudiziari o di polizia giudiziaria oppure a forze armate o di polizia.
Ciò premesso, l'unica ipotesi di videosorveglianza scolastica espressamente ritenuta lecita dal Garante senza necessità di ulteriori verifiche riguarda la finalità di tutela dell'edificio scolastico e dei beni scolastici da atti vandalici, purché le riprese riguardino le sole aree interessate e vengano attivate negli orari di chiusura degli istituti[10]; per detta finalità, viene pertanto esclusa la possibilità di attivare le riprese "*in coincidenza con lo svolgimento di eventuali attività extrascolastiche che si svolgono all'interno della scuola*", e, ciò che ovvio, in coincidenza con gli orari standard delle lezioni.
Ricordiamo, peraltro, che anche nella ipotesi di telecamere installate per motivi di antivandalismo dovranno comunque essere rispettate tutte le altre condizioni previste dalla legge e dal Provvedimento a carattere generale del Garante, tra cui l'informativa, l'adozione di misure di sicurezza, la limitazione della eventuale conservazione dei dati.
Non dovrà invece essere di regola ottenuto il preventivo consenso degli interessati, poiché il

6 Artt. 23 e 24 del d. lgs. 196/03.
7 Artt. 18-22 del d. lgs. 196/03.
8 Cfr. Allegato B al d. lgs. 196/03 e paragrafo 3.3.1 del Provvedimento a carattere generale in tema di videosorveglianza 8 aprile 2010.
9 Cfr. art. 11, comma 1, lett. b), del d. lgs. 196/03.
10 Si veda il paragrafo 4.3 del Provvedimento in materia di videosorveglianza del Garante datato 8 aprile 2010. Si tratta di prescrizione poi ribadita nella guida del Garante "*La privacy tra i banchi di scuola*", ove si afferma che "*In caso di stretta necessità le telecamere sono ammesse, ma devono funzionare solo negli orari di chiusura degli istituti*".

trattamento può in questo caso lecitamente avvenire pure in assenza del consenso in applicazione dell'istituto del bilanciamento di interessi[11].

Apertura alla possibilità di utilizzare la videosorveglianza nelle scuole anche per finalità diverse dall'antivandalismo?

Il fatto che il Garante abbia esplicitamente riconosciuto la legittimità – alle condizioni già dette – del sistema di videosorveglianza nelle scuole per finalità di tutela della proprietà dovrebbe, di per sé, avere valore neutro rispetto ad altre finalità; esso, cioè, non dovrebbe essere un argomento né a favore né contro la possibilità di installare e utilizzare la videosorveglianza per finalità diverse da quelle di mero antivandalismo.

In realtà, il generale sfavore verso l'utilizzo della videosorveglianza per finalità differenti, sebbene non espresso esplicitamente, pareva trasparire dal divieto, più volte ribadito, di mettere in funzione le telecamere durante gli orari di apertura della scuola.

Una moderata apertura pare ora giungere dal provvedimento inizialmente citato[12], in cui il Garante ha valutato illegittima la videosorveglianza installata nell'asilo nido a causa delle caratteristiche del sistema: ripresa video in tempo reale nell'area didattica dell'asilo, con trasmissione dei fotogrammi dei bambini aggiornati ogni tre secondi quando essi erano affidati alle maestre, e con possibilità di visualizzazione attraverso internet dei fotogrammi stessi da parte dei genitori dei bambini muniti di credenziali identificative.

Il Garante ha dunque affermato che, nel caso specifico, risultavano esplicitamente violati sia il principio di necessità che quello di proporzionalità: da un lato, non era stato dimostrato che la finalità di garantire la sicurezza dei minori iscritti all'asilo nido potesse essere assicurata solo attraverso l'implementazione di un ulteriore strumento di videosorveglianza, in grado di identificare direttamente ed immediatamente gli interessati anche all'interno della "zona didattica", nonostante la presenza di altre telecamere presso la struttura; dall'altro, non era stato dimostrato che l'asilo nido fosse ubicato in un contesto ambientale "difficile", e che le "tradizionali" scelte organizzative adottate per gestire la struttura sino al momento dell'introduzione della webcam si fossero dimostrate inadeguate a impedire il verificarsi degli episodi che si intenderebbe scongiurare.

Analizzando le caratteristiche del sistema installato nel caso specifico, risultano in realtà violati anche i principi di liceità e di finalità.

Quello di liceità, perché il sistema non assicura che la visione delle immagini resti circoscritta ai soli soggetti muniti di credenziali, e, soprattutto, perché la visione da parte dei genitori non è limitata esclusivamente alle attività del proprio figlio, ma si estende anche alla condotta degli altri minori iscritti e dei docenti.

Quello di finalità, perché la tutela della sicurezza dei bambini non avrebbe comunque richiesto la presenza, a favore dei genitori, di collegamento via web con il sistema, visto che in questo caso la finalità sarebbe – piuttosto – quella di "*placare eventuali ansie o a soddisfare semplici curiosità dei genitori*".

Il trattamento è stato dunque considerato illegittimo, ma il Garante, nel fare ciò, ha affermato qualcosa di molto importante, e, in un certo senso, in controtendenza rispetto al suo precedente Provvedimento datato 8 aprile 2010[13] e alla guida "*La privacy tra i banchi di scuola*"[14]: e cioè che – citando un parere della Commissione Europea – "*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*", considerato che la tutela dell'incolumità fisica dei minori è una finalità "*senz'altro lecita*".

Non più, dunque, chiusura totale alla installazione della videosorveglianza per fini diversi dall'antivandalismo, ma una moderata apertura anche per la finalità di tutela della sicurezza fisica e morale dei minori contro possibili violenze o atti vessatori, purché – ed è questo il punto

11 Istituto previsto dall'art. 24, comma 1, lett. g), del d. lgs. 196/03.

12 Provvedimento 8 maggio 2013, doc. web n. 2433401.

13 Cfr. nota 3.

14 Cfr. nota 5.

fondamentale – vengano salvaguardati "*al contempo, anche altri interessi fondamentali* [dei bambini e dei ragazzi, ndr]*, tra i quali quello alla loro riservatezza, soprattutto attraverso il rispetto dei principi di necessità e proporzionalità posti dal Codice*".

Tutela della sicurezza di bambini e ragazzi per mezzo della videosorveglianza scolastica.

Alla luce dei principi espressi dal Garante, occorre pertanto chiedersi se vi possono realmente essere eventuali spazi per un utilizzo della videosorveglianza in ambito scolastico diverso da quello di mero controllo antivandalismo, e, in particolare, per utilizzare tale strumento in funzione di tutela dei bambini e dei ragazzi.

Un primo problema preliminare da risolvere è quello del rispetto della normativa posta a tutela del controllo a distanza dei lavoratori, e, in particolare, dell'art. 4 dello Statuto dei Lavoratori, il quale prevede che «*È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro 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*».

La norma contempla dunque due fattispecie, distinte dal legislatore in base alle finalità cui l'uso degli impianti è diretto: il primo comma sancisce un divieto assoluto del controllo intenzionale, cioè dell'utilizzo di apparecchiature finalizzate al mero controllo dell'attività lavorativa, sul presupposto che la vigilanza sul lavoro, ancorché necessaria all'organizzazione produttiva, vada mantenuta in una dimensione "umana", non esasperata, cioè, dall'uso di tecnologie che possano eliminare ogni zona di riservatezza e di autonomia nello svolgimento del lavoro[15]; il secondo comma consente al datore di lavoro il controllo preterintenzionale, e cioè gli garantisce la possibilità di installare e utilizzare quegli impianti che, anche se idonei a controllare a distanza i lavoratori, siano tuttavia diretti a soddisfare esigenze organizzative, produttive o di sicurezza, e purché vi sia un preventivo accordo con le rappresentanze sindacali oppure vi sia un'autorizzazione dell'Ispettorato del Lavoro.

Per effetto del richiamo contenuto nell'art. 114 del d. lgs. 196/03[16], l'eventuale violazione del divieto assoluto previsto dall'art. 4, comma 1, dello Statuto dei Lavoratori comporterà non solo l'illiceità del comportamento del datore di lavoro dal punto di vista giuslavoristico (sanzioni penali; inutilizzabilità delle immagini per l'esercizio di eventuali azioni disciplinari; comportamento antisindacale), ma anche l'illegittimità del trattamento dei dati da parte del titolare del trattamento stesso.

Come precisato dal Garante nel Provvedimento in materia di videosorveglianza 8 aprile 2010, infatti, nelle attività di sorveglianza occorre comunque rispettare il divieto di controllo a distanza dell'attività lavorativa, pertanto, ai sensi dell'art. 4, comma 1, della legge 300/1970, è vietata l'installazione di apparecchiature specificatamente preordinate alla predetta finalità: "*non devono quindi essere effettuate riprese al fine di verificare l'osservanza dei doveri di diligenza stabiliti per il rispetto dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa* (...)".

Il confine è a volte labile.

L'utilizzo della videosorveglianza nelle aree didattiche, a ciclo continuo, è a rischio di potere essere inquadrato nel primo comma dell'art. 4: si potrebbe infatti sostenere che la ristrettezza degli spazi, la presenza costante dei docenti e degli educatori e la funzione per cui verrebbe installata la

15 Cfr. anche la sentenza della Suprema Corte n. 15982 del 17.07.2007, dove è stato ribadito che l'articolo 4 dello Statuto dei Lavoratori "*fa parte di quella complessa normativa diretta a contenere in vario modo le manifestazioni del potere organizzativo e direttivo del datore di lavoro che, per le modalità di attuazione incidenti nella sfera della persona, si ritengono lesive della dignità e della riservatezza del lavoratore….sul presupposto – espressamente precisato nella Relazione ministeriale – che la vigilanza sul lavoro, ancorché necessaria nell'organizzazione produttiva, vada mantenuta in una dimensione umana, e cioè non esasperata dall'uso di tecnologie che possono rendere la vigilanza stessa continua e anelastica, eliminando ogni zona di riservatezza e di autonomia nello svolgimento del lavoro*".

16 "*Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300*".

videosorveglianza, concorrano a configurare proprio la tipica installazione volta a controllare la correttezza nell'esecuzione della prestazione lavorativa.
Il problema è in realtà a mio parere superabile, se si considera che la reale finalità di un'installazione di questo tipo non è il controllo dell'adempimento della prestazione lavorativa (orari, svolgimento del programma, ecc.), ma quella di garantire la sicurezza dei minori, controllando e prevenendo in particolare la commissione di eventuali atti illeciti del personale scolastico.
Il controllo potrebbe essere quindi inquadrato come meramente difensivo, o quanto meno come incidentale rispetto a esigenze organizzative, di tal che esso potrebbe rientrare nella previsione del secondo comma dell'art. 4 dello Statuto dei Lavoratori: la videosorveglianza, quando resa necessaria da esigenze organizzative o produttive, ovvero è richiesta per la sicurezza del lavoro, ma da cui possa anche derivare la possibilità di controllo a distanza dell'attività dei lavoratori, non è illegittima *tout court*, ma necessita del "*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*."
Addirittura, secondo un orientamento giurisprudenziale (che oggi pare forse in via di superamento), qualora controlli di questo tipo fossero qualificati come meramente difensivi – e volti dunque alla mera repressione di atti illeciti dei dipendenti – , potrebbero anche essere installati in forma occulta.
Anche di recente, con sentenza n. 2722 del 23.02.2012, la Sezione Lavoro della Suprema Corte, nello statuire la legittimità dei controlli occulti del datore di lavoro sull'attività informatica dei dipendenti, ha precisato che nel caso specifico "*il datore di lavoro ha posto in essere una attività di controllo sulle strutture informatiche aziendali che prescindeva dalla pura e semplice sorveglianza sull'esecuzione della prestazione lavorativa degli addetti ed era, invece, diretta ad accertare la perpetrazione di eventuali comportamenti illeciti (poi effettivamente riscontrati) dagli stessi posti in essere. Il cd. controllo difensivo, in altre parole, non riguardava l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa immagine dell'Istituto bancario presso i terzi. In questo caso entrava in gioco il diritto del datore di lavoro di tutelare il proprio patrimonio, che era costituito non solo dal complesso dei beni aziendali, ma anche dalla propria immagine esterna, così come accreditata presso il pubblico. Questa forma di tutela egli poteva giuridicamente esercitare con gli strumenti derivanti dall'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale. Tale situazione, ad una lettura attenta, è già esclusa dal campo di applicazione dell'art. 4 dalla sopra citata giurisprudenza (che già esclude dai controlli difensivi vietati quelli aventi ad oggetto la tutela di beni estranei al rapporto di lavoro, v. Cass. n. 15892 del 2007 cit)*".
La ancora più recente Corte di Cassazione, sez. Lavoro, sentenza 01.10.2012, n. 16622, ha invece sposato l'orientamento opposto (già peraltro espresso con la sentenza n. 4375 del 23.02.2010), rilevando come "*l'effettività del divieto di controllo a distanza dell'attività dei lavoratori richiede che anche per i c.d. controlli difensivi trovino applicazione le garanzie del citato art. 4, secondo comma, e che, comunque, quest'ultimi, così come la altre fattispecie di controllo ivi previste, non si traducano in forme surrettizie di controllo a distanza dell'attività lavorativa dei lavoratori. Se per l'esigenza di evitare attività illecite o per motivi organizzativi o produttivi, possono essere installati impianti ed apparecchiature di controllo che rilevino dati relativi anche alla attività lavorativa dei lavoratori, la previsione che siano osservate le garanzie procedurali di cui all'art. 4, secondo comma, non consente che attraverso tali strumenti, sia pure adottati in esito alla concertazione con le r.s.a., si possa porre in essere, anche se quale conseguenza mediata, un controllo a distanza dei lavoratori che, giova ribadirlo, è vietato dall'art. 4, comma 1, cit.*".
Un approccio cauto al problema, anche alla luce del più recente orientamento giurisprudenziale, induce a ritenere comunque necessario il preventivo accordo sindacale, o, in mancanza, l'istanza all'Ispettorato del Lavoro.
Tra l'altro, il problema della configurabilità della videosorveglianza come controllo difensivo e quindi potenzialmente installabile in forma occulta è in realtà più teorico che pratico: la presenza,

oltre ai lavoratori, di altri interessati (gli utenti), impone di informare questi ultimi (o, nel caso si tratti di minori, coloro che esercitano la potestà genitoriale) del trattamento, e, quindi, presuppone una conoscibilità "di fatto" della videosorveglianza stessa che renderebbe comunque inutile la videosorveglianza occulta.
In ogni caso, se fosse possibile installare il sistema di videosorveglianza ai sensi del secondo comma dell'art. 4 dello Statuto dei Lavoratori, le immagini trattate potrebbero essere utilizzate solo per la finalità di sicurezza dei minori e accertamento di eventuali atti illeciti, mentre non potrebbero in alcun modo essere utilizzate per tutto ciò che potrebbe essere ricondotto al controllo sull'attività lavorativa (accertamento circa il corretto svolgimento del programma scolastico; metodo delle lezioni; rispetto dell'orario di lavoro; ecc.), e neanche per controllare il comportamento dei discenti.
Molto più complesso è il rispetto dei principi di necessità e proporzionalità.
Come affermato anche dal parere n. 2/2009 sulla "*Protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole)*" del Gruppo *ex* art. 29, "*poiché i sistemi CCTV possono incidere sulle libertà personali, la loro installazione nelle scuole richiede particolari precauzioni. In altri termini, andrebbero autorizzati se necessari e se l'obiettivo non può essere raggiunto con altri mezzi disponibili meno intrusivi*".
Due, quindi, i requisiti che dovrebbero essere presi in considerazione: la necessità dell'installazione del sistema di videosorveglianza e l'impossibilità di raggiungere la finalità di tutela con mezzi meno invasivi.
In questa ottica, il Gruppo *ex* art. 29 ha riscontrato la sussistenza dei suddetti requisiti con riguardo ai sistemi di videosorveglianza installati all'entrata e all'uscita delle scuole, oppure a quelli installati negli spazi in cui possono circolare persone esterne alla popolazione scolastica (si pensi, ad esempio, a eventuali spazi – giardini, parchi, cortili – condivisi tra la scuola e altri enti).
Sempre il già citato Parere n. 2/2009 sulla "*Protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole)*" del Gruppo *ex* art. 29, precisa però che "*nella maggior parte degli altri spazi scolastici il diritto al rispetto della vita privata degli alunni (e degli insegnanti e del restante personale scolastico) e la libertà fondamentale di insegnamento si oppongono all'esigenza di una sorveglianza permanente con sistemi CCTV. Ciò vale soprattutto per le aule, dove la videosorveglianza può interferire non solo con la libertà di apprendimento e di parola degli studenti, ma anche con la libertà di insegnamento. Lo stesso dicasi per gli spazi ricreativi, le palestre e gli spogliatoi, dove la sorveglianza può interferire con il diritto al rispetto della vita privata*".
Fermo restando che spogliatoi e bagni devono rimanere ambienti privi di qualsiasi controllo tecnologico invasivo, con riguardo agli altri spazi scolastici la correttezza delle conclusioni espresse dal Gruppo *ex* art. 29 deriva però dal presupposto dal quale si parte: quello per cui la tutela della sicurezza dei minori deve essere rivolta nei confronti di minacce *esterne*, provenienti da soggetti non facenti parte della popolazione scolastica e che potrebbero introdursi nell'area della scuola.
E' ovvio che se si accoglie questo punto di vista, difatti, le esigenze di sicurezza potrebbero essere bene tutelate utilizzando altri mezzi meno invasivi e più proporzionati rispetto alla videosorveglianza *interna*: dissuasori fisici nel perimetro (cancellate, muri, ecc.), sorveglianza e guardiania all'entrata e all'uscita della scuola, eventualmente anche videosorveglianza all'entrata e all'uscita (in presenza tuttavia di alcune condizioni: ad esempio qualora la scuola sia situata in un contesto ambientale "difficile", oppure qualora vi siano stati precedenti episodi che hanno dimostrato l'inutilità delle altre e più proporzionate misure, oppure quando le altre misure siano oggettivamente insufficienti o impraticabili fin dal principio – si pensi a strutture scolastiche di dimensioni particolarmente estese).
Il Garante della Privacy e il Gruppo *ex* art. 29 non sembrano invece voler considerare – se non incidentalmente – la problematica di poter tutelare bambini e ragazzi anche nei confronti di minacce provenienti dall'*interno* dalla scuola stessa: ci riferiamo, in particolare, agli infami episodi delittuosi che hanno purtroppo visto come protagonisti alcuni insegnanti, educatori e collaboratori scolastici proprio nei confronti di bambini – anche molto piccoli – a loro affidati.
Se, infatti, la minaccia non proviene più dall'esterno, ma dall'interno, è altrettanto evidente che i

mezzi di cui sopra (cancellate, guardiania, videosorveglianza esterna), che sono certamente proporzionati alla finalità da perseguire quando si tratta di non consentire l'ingresso a scuola di estranei, possono invece non essere più sufficienti per realizzare le esigenze di tutela rispetto a eventuali minacce interne.
Allo stato attuale della normativa e dell'interpretazione che di essa viene data, appare comunque molto difficile poter ipotizzare una videosorveglianza interna e continua anche solo nelle aree didattiche.
Sicuramente, è del tutto impraticabile potere ipotizzare una trasmissione delle immagini via web con possibilità di visione da parte dei genitori.
Una soluzione di questo tipo si scontrerebbe con: la violazione del principio di proporzionalità, essendo del tutto superflua, ai fini di tutelare la sicurezza dei minori, la possibilità di vedere le immagini in tempo reale da parte di un numero molto ampio di soggetti; la difficoltà di rispettare le misure di sicurezza[17]; l'attribuzione della qualifica di incaricato del trattamento a un numero potenzialmente ampio di persone, in contrasto con quanto prescritto dal Garante con il Provvedimento 8 aprile 2010[18]; l'impossibilità di garantire – stante anche l'ampio numero di soggetti che sarebbero incaricati del trattamento – che la visione delle immagini rimanga effettivamente prerogativa solo degli incaricati stessi.
Stabilito dunque che allo stato attuale non appare lecita l'installazione di videosorveglianza con collegamento via web, anche un sistema più "tradizionale" in cui la videosorveglianza è installata nelle aree didattiche, ma senza collegamento internet, appare comunque di difficile fattibilità.
In primo luogo, il sistema dovrebbe probabilmente prevedere l'impossibilità di riconoscimento degli interessati, visto che la tutela della sicurezza degli alunni, e dunque la possibilità di intervenire a tutela degli stessi, non potrebbe essere inficiata dal fatto che il singolo alunno sia identificabile: la preferenza per i dati anonimi dovrebbe forse prevalere.
Altro problema complesso riguarda il consenso al trattamento.
Qualora si tratti di scuola pubblica, non sarà necessario il consenso degli interessati, ma l'ente potrà trattare i dati solo nell'esercizio delle sue funzioni istituzionali, come previsto dagli artt. 18-22 del d. lgs. 196/03; a questo punto, la liceità del trattamento dipenderà da come vengono inquadrate le funzioni istituzionali di una scuola pubblica: se tra queste possono essere fatte rientrare anche quelle della protezione dei minori e più in generale dei suoi studenti, allora effettivamente il consenso di tutti gli interessati non sarebbe necessario.
Qualora si tratti di scuola privata, occorrerà invece il consenso di tutti gli interessati per potere mettere in funzione il sistema di videosorveglianza. Tale necessità potrebbe causare problemi tecnici non indifferenti, perché è praticamente impossibile che il sistema possa automaticamente riprendere alcuni bambini e non altri, a meno di immaginare – soluzione, questa, che presterebbe però il fianco a critiche di tipo diverso – la formazione di classi con bambini sottoposti a videosorveglianza e di classi prive di telecamere.
Di fatto, il sistema nelle scuole private potrebbe quindi funzionare solo con il consenso di tutti gli interessati, e, dunque, non consentendo l'iscrizione a coloro i quali manifestassero la volontà di non prestare il consenso al trattamento[19].
La maggior parte delle problematiche poste dall'utilizzo della videosorveglianza nelle scuole e finora esaminate appaiono dunque – alcune più facilmente, altre più difficilmente – forse superabili.
Ma c'è una questione che, allo stato attuale, impedisce certamente al Garante di cambiare opinione sul punto (a meno di interventi legislativi, oppure di esplicite prese di posizione da parte di

17 Il rispetto delle misure di sicurezza potrebbe comunque essere realizzato assicurando che la trasmissione delle immagini avvenga sempre con tecniche crittografiche che garantiscano la riservatezza dei dati, ad esempio con connessione VPN: si veda, sul punto, il Provvedimento del Garante n. 218 del 24 aprile 2013.

18 "*Il titolare o il responsabile devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate sia ad accedere ai locali dove sono situate le postazioni di controllo, sia ad utilizzare gli impianti e, nei casi in cui sia indispensabile per gli scopi perseguiti, a visionare le immagini (art. 30 del Codice). Deve trattarsi di un numero delimitato di soggetti, specie quando il titolare si avvale di collaboratori esterni*".

19 Ma se così fosse, allora il consenso degli interessati ben difficilmente potrebbe essere definito come espresso liberamente, e, dunque, legittimo.

organismi internazionali): il rispetto del principio di proporzionalità dal punto di vista non dei lavoratori della scuola, ma degli utenti stessi, e cioè dei bambini e dei ragazzi.
Molto spesso, infatti, le critiche all'utilizzo della videosorveglianza nelle scuole provengono soprattutto da chi teme che l'utilizzo di tali mezzi possa rivelarsi un modo per controllare più facilmente – e a relativo basso costo – le prestazioni dei lavoratori, aprendo così la strada a quello che in giurisprudenza viene chiamato "controllo anelastico".
Pochi invece si soffermano sul fatto che il principio di proporzionalità nel trattamento dei dati è in questo caso uno strumento di tutela anche a favore di coloro i quali – ci sia concessa la cacofonia – dovrebbero essere tutelati dalla videosorveglianza stessa.
L'introduzione di un sistema di videosorveglianza nelle classi, pur rispondendo alla lodevole finalità di controllo e prevenzione di eventuali abusi, comporterebbe agli utenti degli svantaggi generalizzati superiori, e comunque sproporzionati, rispetto ai vantaggi di cui essi potrebbero usufruire.
Il controllo costante mediante telecamere nelle aule, a fronte di eventuali vantaggi[20], può infatti facilmente provocare nei bambini e nei ragazzi un danno allo sviluppo della propria personalità, anche grave: come osservato nel Parere 2/2009 sulla "*Protezione dei dati personali dei minori (Principi generali e caso specifico delle scuole)*", adottato l'11 febbraio 2009 dal Gruppo di Lavoro articolo 29 sulla protezione dei dati personali "*In effetti i minori vanno sviluppando una concezione della loro libertà che può essere distorta se fin da piccoli considerano una cosa normale essere sorvegliati da sistemi CCTV*".
L'abitudine ad accettare la videosorveglianza continua per molti anni (dall'asilo nido all'ultimo anno delle scuole superiori, una persona potrebbe trascorrere quasi diciannove anni sotto videosorveglianza pressoché quotidiana), peraltro nel delicato periodo di formazione del proprio carattere, potrebbe inoltre contribuire alla degradazione inconscia del "sentire" tali dati come dati personali e come tali degni di tutela, e dunque potrebbe poi facilitare la formazione di futuri giovani adulti poco attenti alla gestione dei propri dati personali.
Non vanno infine trascurate anche le molto probabili modificazioni comportamentali a cui – più o meno coscientemente – bambini e ragazzi andrebbero incontro sapendo di avere intorno a sé delle telecamere accese.
Queste considerazioni, difficilmente opinabili anche fin dal momento in cui viene frequentata la scuola dell'infanzia, potrebbero forse non essere applicabili agli asili nido, dove i bambini probabilmente potrebbero anche non avere consapevolezza effettiva delle telecamere o comunque di cosa esse comportino.
Il tema, dunque, resta controverso, e le domande sono molte.
Ad alcune di esse, potranno tentare di dare risposta il legislatore, la magistratura, i giuristi, le autorità indipendenti: i cosiddetti "tecnici".
Ma è la società civile, la cui spinta potrebbe nel medio-lungo periodo effettivamente modificare situazioni che allo attuale paiono cristallizzate, che deve però porsi un interrogativo fondamentale: "*veramente vogliamo una società in cui si è sempre ripresi, in cui si vive sotto i riflettori?*"[21].

Avv. Marco Fusari

20 Vantaggi tutti da dimostrare, peraltro, con riguardo a scuole dove non risulta si siano mai verificati in precedenza eventi criminosi.

21 Garante della Privacy, Intervista pubblicata su *La Repubblica* del 18 aprile 2013.