

INFORMAZIONI CIOFS E CNOS/SCUOLA

17/2021

A cura di d. Bruno Bordignon

479/21 Scuole che pubblicano foto, video e audio di minori: non basta il consenso dei genitori. Una proposta di check list privacy per essere sicuri

di Avv. Bruno Cantarone

Uno dei quesiti che più frequentemente mi viene rivolto quale Responsabile della Protezione dei Dati in ambito scolastico, riguarda la possibilità di raccogliere ed utilizzare, nei modi e per le finalità più disparate, immagini e video di studenti. Nello specifico, i dubbi di Dirigenti Scolastici e docenti attengono non tanto alle condizioni che legittimano la pubblicazione da parte della Scuola di dati personali relativi ai propri studenti, operazione spesso data (a torto) per scontata, quanto piuttosto alla necessità o meno di acquisire il consenso dei loro genitori, quasi sempre ritenuto (nuovamente a torto) “salvifico” e dirimente. La questione è assai delicata e merita di essere attentamente vagliata ed approfondita. In via preliminare va precisato che ai fini dell’applicazione della vigente normativa in materia di protezione dei dati personali (Regolamento UE 2016/679 – GDPR e D. Lgs. 196/2003 – Codice Privacy):

1. le immagini e la voce sono informazioni che permettono l’identificazione diretta della persona interessata e sono pertanto da considerare “dati personali” a tutti gli effetti;
2. costituisce “trattamento di dati” qualsiasi operazione compiuta con o sui dati personali (come ad esempio la raccolta, la conservazione, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, ecc.);
3. anche la sola registrazione di video o foto che riprendono persone identificabili si configura come un “trattamento di dati personali”, come tale assoggettabile alla citata normativa.

La questione relativa alla raccolta ed eventuale pubblicazione di foto e video in ambito scolastico è stata da tempo affrontata (e risolta) dall’Autorità Garante nei seguenti termini, con riguardo ad una ben definita fattispecie.

Alla FAQ: “*Violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici?*” (<https://www.garanteprivacy.it/home/faq/scuola-e-privacy>), la risposta fornita dal Garante è negativa, perché “*Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale.*” Il “via libera” che ne discende risulta subordinato al sussistere di queste **quattro condizioni** (enucleabili dalla stessa formulazione della domanda e della risposta): **I**) deve evidentemente trattarsi di un evento in ambito scolastico che è aperto alla partecipazione dei genitori; **II**) i soggetti autorizzati ad effettuare tali riprese sono i genitori; **III**) la finalità da essi perseguita deve essere personale; **IV**) l’ambito di circolazione dei dati personali raccolti (foto e video) deve limitarsi a quello familiare o amicale. La risposta del Garante precisa inoltre che: “*Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet e sui social network. In caso di diffusione di immagini dei minori diventa infatti indispensabile ottenere il consenso da parte degli esercenti la potestà genitoriale*”. In pratica, ferme le prime tre condizioni, se la quarta non è rispettata perché l’ambito di circolazione delle riprese si estende ad una platea più ampia di destinatari mediante pubblicazione via internet, è necessario acquisire il preventivo consenso dei genitori dei minori coinvolti. Rispetto a questa indicazione fornita dal Garante, cosa cambia se – in diversa fattispecie – a fare le riprese video o raccogliere le fotografie degli alunni è il **personale scolastico**? Lo scenario è completamente diverso perché:

- le riprese vengono verosimilmente effettuate in un contesto “chiuso”, che cioè non prevede la presenza di soggetti esterni all’amministrazione scolastica (genitori e parenti degli alunni, visitatori, ecc.);
- è cambiata la qualità del soggetto che effettua le riprese (egli ha responsabilità del tutto diverse da quella genitoriale e quindi non può decidere per il minore);
- è cambiata la finalità perseguita (non è più di tipo “personale” ma è semmai configurabile come “istituzionale”, “professionale”, “promozionale”, “motivazionale”, ecc.);
- i dati personali raccolti non sono destinati a circolare in un ambito “familiare o amicale” (con ogni probabilità, essi costituiranno oggetto di comunicazione o diffusione mediante trasmissione telematica).

Date tali profonde differenze, non è possibile, in questa mutata prospettiva, continuare a fare affidamento sulla risposta del Garante che legittima (solo) il comportamento dei genitori.

In questo diverso caso, allo scopo di verificare la liceità del trattamento di dati che intende effettuare attraverso la ripresa di fotografie, audio o video di alunni, l’operatore scolastico dovrebbe porsi una serie di **interrogativi preliminari progressivi**:

1. La finalità del trattamento consiste nella esecuzione di un **compito di interesse pubblico** (o nell’adempimento di un **obbligo legale**)?
2. Il trattamento è **funzionale** al raggiungimento della finalità perseguita? (serve, ad esempio, per documentare l’attività formativa svolta nell’ambito di un P.O.N., o di un progetto didattico previsto nel P.T.O.F.)
3. Quel trattamento è l’**unico modo** per raggiungere la finalità perseguita? (non è possibile documentare diversamente l’attività svolta, ad esempio attraverso gli elaborati prodotti dagli alunni)
4. Il trattamento è **proporzionato** rispetto alla finalità perseguita? (i dati personali trattati sono ridotti al minimo indispensabile per il raggiungimento dello scopo)
5. La eventuale adozione di **cautele particolari** nel trattamento dei dati personali, tali da precludere la riconoscibilità dell’interessato (ad esempio riprendendo i soggetti di spalle o da lontano, evitando i primi piani, o pixellando i volti, ecc.), impedisce di raggiungere la finalità perseguita?

Se le risposte alle domande precedenti sono tutte affermative il trattamento può essere certamente considerato legittimo in sé, e non richiede la raccolta del preventivo consenso dei genitori.

Il consenso è invece assolutamente indispensabile se:

- le domande precedenti hanno ricevuto **risposte dubbie o addirittura negative** (maggiore è il loro numero, maggiori possono essere le responsabilità che assume il titolare del trattamento);
- i dati trattati sono destinati alla **pubblicazione**, cioè verranno messi a disposizione di soggetti indeterminati, ad esempio attraverso i canali social o il sito web (beninteso, al di fuori di circuiti protetti come può essere la piattaforma GPU per la gestione, il monitoraggio e la documentazione delle attività del Programma Operativo Nazionale, ed esclusi i casi in cui, per le particolari cautele adottate nel trattamento (vedi sopra *sub 5*) è stato spezzato il collegamento tra l’informazione personale pubblicata (immagine o voce) e l’interessato al quale essa appartiene).

In simili ipotesi, poiché il consenso dei genitori diventa la (necessaria e sufficiente) condizione di liceità del trattamento, è quanto mai opportuno che la questione venga attentamente ponderata dal titolare del trattamento (l’istituzione scolastica, in persona del suo Dirigente), effettuando di volta in volta un prudente bilanciamento di tutti gli interessi in gioco e dei potenziali rischi per l’interessato, tenendo in debito conto le considerazioni che seguono. Per il principio di **accountability** stabilito dall’art. 24 del GDPR, il titolare del trattamento deve “garantire, ed essere in grado di dimostrare” la conformità del trattamento rispetto alla normativa vigente.

Il puntuale rispetto di tale obbligo di “rendicontazione” grava inevitabilmente la Scuola – nel caso dei trattamenti basati sul consenso – di oneri documentali, procedurali e di conservazione a causa della necessità di dover correttamente:

1. elaborare la formula *ad hoc* da sottoporre ai genitori, osservando i principi che presidiano la validità del consenso (adeguata informazione, anche in ordine alla revocabilità; forma “comprensibile e facilmente accessibile”; linguaggio semplice e chiaro; “granularità”; “chiara distinguibilità” da altre materie; ecc.);
2. gestire la fase della raccolta delle loro manifestazioni di volontà (verificandone in qualche modo la autenticità);
3. conservarle per il futuro, nell’evenienza di contestazioni;
4. procedere alla tempestiva cancellazione dei dati trattati qualora un genitore revochi il consenso in precedenza rilasciato (art. 17, par. 1, lett. b) del GDPR).

Laddove tali oneri vengano ritenuti accettabili (nell’interesse della Scuola), prima di procedere alla eventuale pubblicazione delle immagini di minori resta ancora da valutare se – stabilito l’interesse superiore del fanciullo quale considerazione preminente (come prescrive la relativa Convenzione di New York del 1989) – i potenziali rischi che ne derivano risultano comunque giustificati. Allo scopo di fornire un utile elemento di valutazione per la prudente decisione che, al riguardo, il titolare del trattamento è chiamato ad assumere, riporto gli esiti di una recente analisi condotta dall’Eurispes (Istituto di Studi Politici, Economici e Sociali, ente privato che dal 1986 è iscritto all’Anagrafe Nazionale degli enti di ricerca del MIUR) e riguardante il fenomeno sociale dello *sharenting*, ossia dell’esposizione dei figli attraverso i post sui social e la condivisione di immagini e video che li riguardano. “L’Eurispes.it” (il magazine online del medesimo Istituto di ricerca) ha messo in guardia i genitori (auspicandone una “educazione al digitale” che li renda più consapevoli dei meccanismi alla base delle piattaforme di condivisione sociale) dai **rischi tecnologici** che incombono sulla esposizione mediatica di immagini di minori ([Foto e video dei figli sui social: quali regole? – L’Eurispes](#)). Il primo è dato dalla possibilità che tramite fotomontaggi o, addirittura, video di tipo *deep fake* le immagini pubblicate possano entrare nei circuiti frequentati da pedofili. La definizione che il vocabolario Treccani fornisce del sostantivo *deep fake* (o *deepfake*) è quella di “Filmato che presenta immagini corporee e facciali catturate in Internet, rielaborate e adattate a un contesto diverso da quello originario tramite un sofisticato algoritmo. Un altro genere di rischio attiene alla possibilità che le immagini del minore finiscano, come peraltro avviene anche per le nostre, all’interno di piattaforme di riconoscimento facciale che utilizzano una mole impressionante di dati per poter affinare i loro sistemi di Intelligenza Artificiale basati sul *machine learning*. Tenuto conto di tutto ciò, le aspettative, le aspirazioni e i desideri ancorché comprensibili di genitori e docenti che attraverso la pubblicazione delle foto dei minori vedono appagati i loro sforzi educativi, meritano soddisfazione e preferenza rispetto agli obblighi legali di massima protezione nei confronti di soggetti vulnerabili? In altri termini: il gioco vale la candela? In conclusione, è mio auspicio che la Scuola pubblica avverta il segnale di allarme trasmesso dalla indagine Eurispes, prima ed anche più forte rispetto ai genitori ai quali esso è direttamente rivolto, e che la prima contribuisca con il proprio esempio all’educazione digitale non solo degli studenti ma anche delle loro famiglie, limitando – in ciò è la mia risposta all’ultima domanda – la pubblicazione di foto e video di minori ai soli casi in cui, per le circostanze che lo connotano (vedi quanto sopra esposto e numerato da 1 a 5), il trattamento di dati personali rispetta per impostazione predefinita (*by default*) la protezione dei dati personali, abbandonando definitivamente la ormai superata logica “consensocentrica” che ispirava la previgente normativa in materia e che per le ragioni sopra illustrate potrebbe creare, nella prassi applicativa delle variopinte formule “liberatorie” che ancora circolano nelle Scuole, più problemi di quanti è in grado di risolvere.

[Scuole che pubblicano foto, video e audio di minori: non basta il consenso dei genitori. Una proposta di check list privacy per essere sicuri - Orizzonte Scuola Notizie](#)

