Provvedimento del 29 gennaio 2026 [10222864]

[doc. web n. 10222864]

Provvedimento del 29 gennaio 2026

Registro dei provvedimenti
n. 42 del 29 gennaio 2026

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia, componente, e il dott. Luigi Montuori, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE" (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore il Prof. Pasquale Stanzione;

PREMESSO

1. Introduzione.

Con reclamo presentato ai sensi dell'art. 77 del Regolamento, i sig.ri XX e XX, per il tramite del proprio avvocato, in qualità di esercenti la responsabilità genitoriale sul minore XX, frequentante l'Istituto San Giuseppe La Salle di Milano (di seguito, l'"Istituto"), la cui attività è riconducibile alla Provincia della Congregazione dei Fratelli delle Scuole Cristiane (di seguito, il "Titolare"), hanno

lamentato una presunta violazione della disciplina in materia di protezione dei dati personali.

In particolare, il predetto minore avrebbe subito un infortunio durante l'orario scolastico e, nell'ambito dell'azione promossa dai genitori ai fini della richiesta di risarcimento del danno alla società assicuratrice, è emerso che l'Istituto sarebbe in possesso di una registrazione video dell'episodio. I genitori avrebbero, inoltre, appreso che il filmato in questione non sarebbe stato acquisito direttamente dal sistema di videosorveglianza, bensì mediante un telefono cellulare, che avrebbe ripreso lo schermo di un computer al momento della riproduzione del video. Tale filmato sarebbe stato, inoltre, consegnato a un investigatore privato, incaricato dalla compagnia assicuratrice ai fini della gestione della richiesta di risarcimento.

2. L'attività istruttoria.

Nel corso dell'istruttoria, l'Autorità ha rivolto al Titolare una richiesta d'informazioni formulata ai sensi dell'art. 157 del Codice (v. nota prot. n. XX del XX). Il Titolare ha fornito riscontro con note del XX e XX (prot. Garante nn. XX e XX), i cui passaggi salienti sono ripresi in prosieguo nella parte motiva del presente provvedimento.

Con nota del XX (prot. n. XX), l'Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell'attività istruttoria, ha notificato al Titolare, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, per aver posto in essere un trattamento dei dati personali degli studenti, dei lavoratori e degli altri soggetti ripresi, mediante un sistema di videosorveglianza, in maniera non conforme al principio di "liceità, correttezza e trasparenza", nonché in assenza di un idoneo presupposto di liceità, in violazione degli artt. 5, par. 1, lett. a), 6 e 88 del Regolamento, e 2-ter e 114 del Codice (in riferimento all'art. 4 della l. n. 300/1970); per aver posto in essere un ulteriore trattamento dei dati personali del figlio minore dei reclamanti e degli altri soggetti ripresi (mediante una ripresa, effettuata da una docente, tramite il proprio telefono cellulare, del video in esame), in maniera non conforme ai principi di "liceità, correttezza e trasparenza" e "limitazione della finalità", nonché in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a) e b), e 6 del Regolamento, nonché 2-ter del Codice; per non aver assicurato un sufficiente livello di trasparenza del trattamento nei confronti degli interessati, in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento; per non aver svolto una valutazione di impatto sulla protezione dei dati prima di dare avvio al trattamento, in violazione dell'art. 35 del Regolamento. Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota del XX, il Titolare, per il tramite del proprio avvocato, ha presentato una memoria difensiva e, ai sensi dell'art. 166, comma 6, del Codice, ha chiesto di essere audito (v. il verbale dell'audizione tenutasi in data XX, acquisito al prot. del Garante n. XX della medesima data, e la nota del Titolare del XX, acquisita al prot. del Garante n. XX della medesima data, con la quale il Titolare ha attestato la correttezza del verbale, così formalizzando lo stesso), prospettando taluni argomenti difensivi, il cui contenuto, per le parti d'interesse, viene ripreso nel successivo par. 3 del presente provvedimento.

3. Esito dell'attività istruttoria.

3.1 La liceità del trattamento.

Con riguardo al trattamento di dati personali oggetto di reclamo e ai presupposti di liceità dello stesso, il Titolare, nel corso dell'istruttoria, ha dichiarato, in particolare, che:

- "l'Istituto è un ente privato fondato e diretto dalla congregazione religiosa dei Fratelli delle

Scuole Cristiane";

- "l'area su cui sorge l'istituto si trova nel territorio del Municipio 2 […] che risulta tra le più critiche di Milano […per quanto attiene alla pubblica sicurezza, tanto che] lo stesso istituto è stato soventemente oggetto di accessi non autorizzati anche durante gli orari scolastici, con episodi di furti, anche in danno di soggetti terzi ed atti di vandalismo", da cui "la necessità degli impianti di video sorveglianza, volti esclusivamente ad assolvere, anche in orari diurni, la precipua funzione di sicurezza […]";

- "il sistema di video sorveglianza è costituito da 2 apparati di registrazione, denominati DVR1 e NVR2, per un totale di 24 TVCC. Il DVR1 gestisce 10 TVCC e la data di installazione, stimata […], risale al 2019. L'NVR2 gestisce 14 TVCC e la data di installazione, stimata […], risale al Settembre del XX";

- "presso l'Istituto vengono svolte diverse attività: 1) […] scolastica; 2) Centro sportivo, anche diurno, gestito da un ente terzo; 3) Ospitalità e foresteria, non accessibile a studenti e insegnanti; 4) Affitto posti auto. In tale contesto i siti di installazione esterni all'Istituto sono i seguenti: Accessi in corrispondenza dei 2 cancelli carrai […]; Parcheggio esterno e box dedicati al deposito materiali; Scale esterne e portoni di ingresso/uscita all'Istituto […]; Area sport e infanzia";

- "i siti di installazione interni riguardano esclusivamente gli atri di accesso ai piani (0, 1, 2, 3), non sono riprese classi, corridoio di accesso alle classi o altre aree in cui si svolge in via continuativa attività didattica […]. Al quarto piano, dedicato all'ospitalità/foresteria sono ripresi l'atrio di sbarco dall'ascensore, il corridoio e l'area antistante all'accesso alla cucina";

- "la telecamera che ha ripreso l'episodio oggetto del reclamo è una di quelle ubicate all'esterno ed è la n. 2 del sistema DVR1 ed è posta a tutela dell'accesso carraio di Via Riccardi e del percorso che effettuano le automobili in una zona dove tra l'altro si verifica, in contestualità, anche il passaggio pedonale, rendendo, pertanto, opportuna la videosorveglianza al fine di poter verificare determinate condotte che possano mettere a rischio l'incolumità delle persone";

- "[…detta] telecamera, caso ha voluto, che abbia ripreso l'episodio occorso al bambino […] che si trovava, dopo il pranzo, insieme ad altri compagni […]";

- "le telecamere che inquadrano l'interno, numericamente limitate, non sono state attivate solo negli orari di chiusura poiché nell'area in cui sorge l'Istituto non sono svolte unicamente attività scolastiche ed extrascolastiche ma altresì attività sportive gestite da un ente terzo, ospitalità/foresteria e affitto di posti auto";

- "la base giuridica ritenuta applicabile è dunque il legittimo interesse (art. 6.1 lettera f) del [Regolamento]). Ciò bilanciando il rispetto dei diritti e delle libertà fondamentali degli interessati […]";

- "non è possibile utilizzare mezzi meno intrusivi per raggiungere gli obiettivi di sicurezza e protezione dell'Istituto considerando anche gli orari limitati dell'operatore della reception e la vasta area da presidiare";

- "il suddetto sistema di videosorveglianza non ha mai avuto una finalità di controllo a distanza dell'attività lavorativa dei dipendenti […;] "la […] installazione [del sistema di videosorveglianza] è sempre stata nota ai lavoratori fin dall'assunzione (Rif. documento "SC02-Assunzione-a-tempo-determinato") […]" e "[…] mai nessuna contestazione disciplinare è stata elevata sulla scorta delle immagini"; in ogni caso, "l'Istituto ritiene opportuno procedere con l'esperire le formalità relative alle procedure di garanzia di cui

all’art. 4 della l. 300/1970”;

- “il DVR1 conserva le immagini per 8 giorni, l'NVR2 conserva le immagini per 14 giorni. Entrambi i dispositivi non sono stati impostati per sovrascrivere le immagini [;] i tempi di conservazione dipendono dalla capacità di memoria del disco di archiviazione”;

- “successivamente al notificato reclamo […], si è provveduto [… alla] disattivazione delle telecamere dei due impianti di videosorveglianza, ad esclusione solamente di due telecamere posizionate su due varchi di accesso in sola rilevazione, senza, pertanto, registrazione […;] l’impianto è stato spento e i due DVR disconnessi dalla rete”.

Risulta, pertanto, accertato che, a partire dal 2019, il Titolare aveva attivato nell’Istituto un sistema di videosorveglianza, che poteva raccogliere immagini di studenti, anche minorenni, del personale scolastico, nonché di soggetti terzi (fornitori, ospiti foresteria, genitori, etc.). Le telecamere erano, infatti, attive anche durante l’orario diurno e in diversi locali interni (negli atri di accesso ai piani dell’Istituto, nell’atrio di sbarco dall’ascensore, corridoio e nell’area antistante all’accesso alla cucina al quarto piano, dedicato all’ospitalità/foresteria) e anche nella parte esterna dello stesso (in corrispondenza dei due cancelli carrai e dell’entrata principale, nel parcheggio esterno, nelle scale esterne e nei portoni di ingresso e uscita, nell’area “sport e infanzia”).

L’impiego dei predetti dispositivi video non risulta, tuttavia, conforme alla disciplina in materia di protezione dei dati personali.

Deve, infatti, osservarsi che il quadro giuridico in materia di protezione dei dati non prevede un diverso regime applicabile ai soggetti pubblici e a quelli privati ma tiene conto del solo profilo funzionale nel trattamento dei dati. Pertanto, stante il perseguimento di un medesimo interesse pubblico sotteso all’offerta formativa, da parte degli istituti scolastici pubblici e privati, i relativi trattamenti di dati personali possono considerarsi leciti se essi sono necessari “per adempiere un obbligo legale al quale è soggetto il titolare del trattamento” o “per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri” (art. 6, par. 1, lett. c) ed e), e parr. 2 e 3 del Regolamento; v. anche art. 2-ter del Codice); tale base giuridica, perimetrando l’ambito del trattamento consentito, stabilisce presupposti, limiti e condizioni dello stesso, e deve essere idonea in termini di qualità di fonte, contenuto essenziale del diritto e di proporzionalità dell’“obiettivo di interesse pubblico [perseguito]” (art. 6, par. 3, del Regolamento; cfr. provv. 10 luglio 2025, n. 410, doc. web n. 10162731).

Nel caso di specie, l’impiego da parte del Titolare di un sistema di videosorveglianza nell’Istituto ha comportato il trattamento di dati personali appartenenti anche a “persone fisiche vulnerabili”, ovvero sia gli studenti minorenni frequentanti l’Istituto - che meritano “una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali” (cons. n. 38 del Regolamento; cfr. provv.ti 25 febbraio 2021, n. 74, doc. web n. 9710177; 13 marzo 2025 n. 134, doc. web n. 10127792; 27 novembre 2025 n. 725, doc. web n. 10211243) - sia i lavoratori in servizio presso lo stesso (v. cons. 75 e art. 88 del Regolamento).

Al riguardo, occorre evidenziare che non si rinvengono, allo stato, disposizioni dell’ordinamento nazionale che contemplino la possibilità di impiegare sistemi di videosorveglianza negli istituti scolastici durante lo svolgimento di attività scolastiche ed extrascolastiche (cfr. l’audizione in Parlamento del Presidente del Garante del 2 ottobre 2018, in relazione a un disegno di legge - poi non approvato - in materia di videosorveglianza negli asili nido e nelle scuole dell'infanzia, nonché nelle strutture socio-sanitarie e socio-assistenziali per anziani e persone con disabilità, ove è stata evidenziata la necessità di tutelare “il diritto alla protezione dei dati personali dei vari soggetti ripresi dal sistema di videosorveglianza. Non solo i lavoratori, dunque, ma anche gli stessi ospiti

delle strutture educative o di cura […]").

Pertanto, come in più occasioni evidenziato dal Garante, "l'eventuale installazione di sistemi di videosorveglianza presso le scuole deve garantire il diritto dello studente alla riservatezza. Può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio e i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate. È inoltre necessario segnalare la presenza degli impianti con cartelli. Le telecamere che inquadrano l'interno degli istituti possono essere attivate solo negli orari di chiusura, quindi non in coincidenza con lo svolgimento di attività scolastiche ed extrascolastiche. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato" ("Scuola e privacy - Le FAQ del Garante", FAQ n. 14, in www.gpdp.it; v. anche il vademecum "La scuola a prova di privacy", da ultimo aggiornato il 12 novembre 2025, doc. web n. 10190259).

Non rileva, pertanto che, come dichiarato in sede di memoria difensiva, si debba tener conto "della circostanza […che] non sono presenti telecamere all'interno degli ambienti scolastici, classi, corridoi ecc.", atteso che la vita di relazione degli studenti, e tra questi e gli insegnanti e altro personale in servizio, si svolge in tutti i luoghi della realtà scolastica, comprese le aree di transito, passaggio o stazionamento temporaneo.

Né è possibile invocare nel caso di specie la base giuridica del legittimo interesse per le seguenti ragioni. Il trattamento di dati personali relativi a lavoratori, mediante telecamere di videosorveglianza idonee a riprendere anche il personale che transita o sosta nei luoghi di lavoro, può essere, infatti, effettuato dal datore di lavoro se esso è necessario per la gestione del rapporto di lavoro, nel rispetto del quadro giuridico applicabile, definito dalla normativa nazionale ed eurounitaria, da regolamenti o da contratti collettivi (artt. 6, par. 1, lett. c), e 88 del Regolamento). In tale quadro, il datore di lavoro deve rispettare le norme nazionali di maggior tutela che regolano i trattamenti di dati personali nel contesto lavorativo (88, par. 2, del Regolamento, a cui fa rinvio l'art. 6, par. 2, del Regolamento). In secondo luogo, sempre con riguardo all'impossibilità di invocare il legittimo interesse, occorre considerare l'effettiva natura d'interesse pubblico dell'attività educativa svolta dal Titolare (cfr. l'art. 6, par. 1, lett. f), ultimo periodo), in un contesto caratterizzato, peraltro, dalla presenza di minori, che, per le ragioni sopra esposte, rende più radicalmente illecito il trattamento in questione, avendo il Titolare utilizzato il sistema di videosorveglianza anche in orario diurno, allorquando sono presenti minori all'interno dell'Istituto.

In ogni caso, l'installazione di telecamere di videosorveglianza all'interno dell'Istituto, anche in orari in cui non sono presenti minori, avrebbe comunque comportato la necessità di assicurare il rispetto della disciplina in materia di controllo indiretto dell'attività lavorativa, stante la perdurate presenza di personale in servizio anche durante tali orari.

Come, infatti, costantemente ribadito nei provvedimenti del Garante, i trattamenti conseguenti all'impiego degli strumenti tecnologici nei luoghi ove si svolge anche l'attività lavorativa trovano la propria base giuridica nella disciplina di settore di cui all'art. 4 della l. n. 300/1970. Tale disposizione perimetra, infatti, in modo uniforme a livello nazionale, l'ambito del trattamento consentito in ogni contesto lavorativo (pubblico e privato) e costituisce nell'ordinamento interno una disposizione più specifica e di maggiore garanzia di cui all'art. 88 del Regolamento, la cui osservanza è condizione di liceità del trattamento (v. art. 5, par.1, lett. a) e 6, par. 1, lett. c) del Regolamento; v., a livello europeo, le indicazioni contenute nelle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video", adottate dal Comitato europeo per la protezione dei dati il 29 gennaio 2020, par. 11, nonché le precedenti indicazioni del Gruppo di Lavoro Articolo 29 nel "Parere 2/2017 sul trattamento dei dati sul posto di lavoro", WP 249; cfr. par. 4.1 del "Provvedimento in materia di videosorveglianza" dell'8 aprile 2010, doc. web n. 1712680, e, da ultimo, la FAQ n. 9 del Garante in materia di videosorveglianza, del dicembre 2020, doc. web 9496574, e le numerose decisioni del Garante riferite a casi concreti, tra cui, con specifico riguardo al ricorso alla videosorveglianza sui luoghi di lavoro, provv.ti 23 ottobre 2025, n.

628, doc. web n. 10196164; 10 luglio 2025, n. 410, cit.; 10 aprile 2025, n. 201, doc. web n. 10139433; 11 aprile 2024, n. 234, doc. web n. 10013356; 16 novembre 2023, n. 578, doc. web n. 9963486; 16 settembre 2021, n. 331, doc. web n. 9719768; 11 marzo 2021, n. 90, doc. web n. 9582791; 5 marzo 2020, n. 53, doc. web n. 9433080; 19 settembre 2019, n. 167, doc. web n. 9147290).

Anche la giurisprudenza della Corte europea dei diritti dell'uomo, nel caso Antovic e Mirkovic v. Montenegro (Application n. 70838/13 del 28.11.2017), ha stabilito che il rispetto della "vita privata" deve essere esteso anche ai luoghi di lavoro pubblici (nel caso di specie, le aule universitarie), evidenziando che la videosorveglianza sul posto di lavoro pubblico può essere giustificata solo nel rispetto delle garanzie previste dalla legge nazionale applicabile, in mancanza delle quali costituisce un'interferenza illecita nella vita privata del dipendente, ai sensi dell'art. 8, par. 2, della CEDU.

Ciò comporta, pertanto, che il datore di lavoro deve rispettare le procedure di garanzia previste dall'art. 4, comma 1, della l. n. 300/1970 (accordo sindacale o, in alternativa, autorizzazione pubblica) allorquando ricorra a sistemi di videosorveglianza per il perseguimento delle finalità tassativamente ivi indicate.

Le pur legittime esigenze di tutela del patrimonio e dell'incolumità delle persone, invocate anche del Titolare nel corso dell'istruttoria, non possono, infatti, di per sé sole, in base al quadro normativo sopra delineato, legittimare il trattamento dei dati personali mediante strumenti dai quali può derivare anche la possibilità di controllo a distanza dei lavoratori, come il sistema di videosorveglianza in questione, in assenza delle predette garanzie previste dalla legge.

Nel caso di specie, il Titolare non ha esperito dette garanzie, sul presupposto che il sistema di videosorveglianza non sarebbe stato preordinato al controllo dell'attività lavorativa e che i lavoratori sarebbero stati a conoscenza dell'utilizzo dello stesso fin dalla loro assunzione, considerazioni queste che, diversamente da quanto prospettato nel corso del procedimento, non rilevano ai fini della possibilità di escludere l'applicabilità delle predette tutele stabilite dalla legge.

Ciò fermo restando che, stante quanto sopra detto in merito alla sproporzione dell'impiego della videosorveglianza all'interno degli istituti scolastici, un eventuale accordo sindacale stipulato ai sensi dell'art. 4 della l. 300/1970 non potrebbe comunque legittimare un siffatto trattamento di dati personali, non potendo le parti assumere impegni e disciplinare la materia dei controlli indiretti sull'attività lavorativa in contrasto con i principi di base di protezione dei dati, con particolare riguardo ai canoni di necessità e proporzionalità del trattamento (v. art. 5 del Regolamento; cfr. Corte di giustizia dell'Unione europea, sentenza C65/23, K GmbH (Traitement de données personnelles des employés), del 19 dicembre 2024, par. 59).

Né rileva la circostanza che i lavoratori in servizio presso l'Istituto siano stati ripresi soltanto incidentalmente e occasionalmente in aree di solo transito. Il sistema di protezione dei dati, integrato con l'art. 4 della l. n. 300/1970, tutela, infatti, la persona che lavora non solo quando i dispositivi di sorveglianza siano posti all'interno dei locali di lavoro - essendo irrilevante la circostanza che l'accesso a detti locali da parte dei lavoratori avvenga in maniera discontinua e per brevi archi temporali - ma anche nel caso in cui siano sottoposte a videosorveglianza aree di pertinenza della sede datoriale, anche esterne o perimetrali, in cui comunque transitano i lavoratori, stante la possibilità, come nel caso di specie, di riprendere la loro immagine e le attività da essi svolte (cfr. provv.ti 23 ottobre 2025, n. 628, cit., relativo all'impiego di una telecamera collocata sulla pubblica via per finalità di sicurezza urbana e inquadrante l'ingresso della casa comunale utilizzato anche dai dipendenti; 10 aprile 2025, n. 201, cit., sull'impiego di una telecamera di videosorveglianza inquadrante l'ingresso esterno di una sede di Polizia locale e parte del parcheggio delle auto di servizio; 11 marzo 2021, n. 90, doc. web n. 9582791, riguardante l'impiego di telecamere di videosorveglianza nei corridoi di un edificio ospitante un

Dipartimento di un Ateneo; 9 maggio 2018, n. 277, doc. web n. 8998303, riguardante un sistema di videosorveglianza installato in aree interne ed aree esterne a un edificio della sede di un ente pubblico, inclusi gli accessi; 18 aprile 2013, n. 200, doc. web n. 2483269, riguardante le riprese che interessavano in particolare gli accessi, i corridoi e alcuni ambienti aperti all'utenza di un Archivio di Stato; 9 febbraio 2012, n. 56, doc. web n. 1886999, nel quale le riprese riguardavano gli accessi ai garage di un Comando di polizia locale, nonché il corridoio interno di accesso ai locali dell'armeria; 17 novembre 2011, n. 434, doc. web n. 1859558, nel quale le riprese interessavano gli ingressi principali e di emergenza, i corridoi posti ai diversi piani, nonché le aree di accesso a talune zone degli uffici).

In ogni caso, nella vicenda in questione, erano sottoposte a videosorveglianza aree in cui potevano transitare o sostare gli alunni, con la conseguenza che necessariamente anche i docenti e il personale amministrativo, chiamati alla vigilanza sugli stessi, svolgevano la propria attività lavorativa in tali aree.

Alla luce delle considerazioni che precedono, deve ritenersi che il trattamento dei dati personali degli studenti, dei lavoratori e degli altri soggetti ripresi all'interno e all'esterno dell'Istituto, è stato posto in essere posto in essere dal Titolare, mediante il sistema di videosorveglianza in questione, in maniera non conforme ai principi di "liceità, correttezza e trasparenza", nonché in assenza di un idoneo presupposto di liceità, in violazione degli artt. 5, par. 1, lett. a), 6 e 88 del Regolamento, e 2-ter e 114 del Codice (in riferimento all'art. 4 della l. 300/1970).

Quanto alle aree esterne all'Istituto, si prende atto di quanto rappresentato dal Titolare sia sede di memoria difensiva, in merito alla circostanza che "in realtà è stato il […] Comune di Milano ad aver sottoposto per questioni di ordine pubblico a videosorveglianza la pubblica via", sia in sede di audizione, confermando che "le telecamere […] riprendevano esclusivamente aree interne (all'aperto) e di proprietà dell'Istituto, non essendo in alcun modo interessata la pubblica via", dovendosi, pertanto, considerare superate le contestazioni mosse al Titolare a tal riguardo.

3.2. L'ulteriore trattamento dei dati personali contenuti nel filmato in cui è ripreso il figlio minore dei reclamanti

Nel corso dell'istruttoria, il Titolare, con riguardo allo specifico episodio che ha interessato il figlio minore dei reclamanti e che è stato ripreso dal sistema di videosorveglianza, ha dichiarato che:

- "non è stato possibile estrarre il filmato direttamente dal DVR […] poiché [l'addetto] non era presente nell'Istituto e […] così [una docente] ha effettuato la ripresa dello schermo del computer tramite il proprio telefono cellulare in collaborazione con il custode […]";

- "i soggetti terzi che hanno visionato il filmato sono i genitori dell'alunno oggetto del video, [un'altra docente] e la […] coordinatrice della scuola primaria, in occasione dell'incontro con la famiglia [del minore], convocat[a] per chiarire la ricostruzione dell'evento";

- "la base giuridica è rappresentata dal legittimo interesse di dimostrare la buona fede e la correttezza dell'operato dell'Istituto".

Nel corso dell'audizione, il Titolare ha poi dichiarato che "il filmato in questione non è mai stato condiviso con compagnie assicurative o investigatori privati nominati dalle stesse" e che "l'Ente detiene ancora il filmato, essendo stata presentata dalla famiglia del minore una denuncia all'Autorità giudiziaria contro ignoti ed, essendo, pertanto possibile che il filmato possa essere richiesto nell'ambito delle attività di indagine".

Al riguardo si evidenzia che la normativa europea prevede che i dati personali devono essere trattati "in modo lecito, corretto e trasparente nei confronti dell'interessato" e "raccolti per finalità determinate, esplicite e legittime" (principio di limitazione della finalità), ammettendo la possibilità

di successivi trattamenti ma solo “in modo che non sia incompatibile con [le] finalità” iniziali del trattamento (art. 5, par. 1, lett. a) e b), del Regolamento).

In tale quadro, pertanto, il titolare può utilizzare per ulteriori trattamenti i soli dati personali lecitamente raccolti in presenza di un’idonea base giuridica, avendo previamente “soddisfatto tutti i requisiti per la liceità del trattamento originario” (cfr. cons. n. 50 del Regolamento), e dunque nei limiti in cui l’originaria raccolta sia stata lecitamente effettuata, avuto riguardo alla finalità principale e nel rispetto dei principi generali di protezione dei dati. Tenuto conto dell’illiceità del trattamento effettuato a monte mediante le telecamere di videosorveglianza in questione (v. il precedente par. 3.1), e stante l’inutilizzabilità dei “dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati” (art. 2-decies del Codice), si ritiene che anche i successivi trattamenti dei dati personali in questione devono essere considerati illeciti. Il trattamento di dati personali per una finalità ulteriore rispetto a quella per i quali sono stati raccolti presuppone, infatti, che la finalità di trattamento originaria sia lecita, circostanza, questa, che non ricorre nel caso di specie (cfr. artt. 5, par. 1, lett. b), e 6, par. 4, del Regolamento).

Deve, pertanto, concludersi che anche tali ulteriori trattamenti dei dati personali del figlio minore dei reclamanti e degli altri soggetti ripresi è stato posto in essere dal Titolare in maniera non conforme ai principi di “liceità, correttezza e trasparenza” e “limitazione della finalità”, nonché in assenza di base giuridica, in violazione degli artt. 5, par. 1, lett. a) e b), e 6 del Regolamento, nonché 2-ter del Codice.

3.3. La trasparenza nei confronti degli interessati.

Per quanto attiene alla trasparenza del trattamento, il Titolare, nel corso dell’istruttoria, ha dichiarato che:

> - “gli impianti sono segnalati dalla presenza di alcuni cartelli […;] è in corso un’attività di sostituzione degli stessi con il modello previsto dalle linee guida dell’EDPB 03/2019, l’ubicazione in più punti in modo che siano visibili anche in orari notturni e la predisposizione di un’informativa integrativa”;
>
> - “sono disponibili diversi cartelli informativi di primo livello apposti in concomitanza con l’installazione del primo impianto di videosorveglianza nell’anno 2019 […]”;
>
> - “l’informativa ai lavoratori è stata fornita attraverso il documento “SC02-Assunzione-a-tempo-determinato” [;] è in corso la predisposizione di un’informativa completa […]”.

Al riguardo, deve farsi presente che, allorquando siano impiegati dispositivi video, il titolare del trattamento, oltre a rendere l’informativa di primo livello mediante apposizione di segnaletica di avvertimento in prossimità della zona sottoposta a videosorveglianza, deve fornire agli interessati anche delle “informazioni di secondo livello”, che devono “contenere tutti gli elementi obbligatori a norma dell’articolo 13 del [Regolamento]” ed “essere facilmente accessibili per l’interessato, ad esempio attraverso un pagina informativa completa messa a disposizione in uno snodo centrale […] o affissa in un luogo di facile accesso” (“Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, cit., in particolare par. 7; ma si veda già il “Provvedimento in materia di videosorveglianza” del Garante dell’8 aprile 2010, cit., in particolare par. 3.1; da ultimo, v. la FAQ n. 4 del Garante in materia di videosorveglianza, cit.).

Le informazioni di primo livello (cartello di avvertimento) “dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l’identità del titolare del trattamento e l’esistenza dei diritti dell’interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento” (Linee guida del Comitato, cit., par. 114). Inoltre, la segnaletica deve contenere anche quelle informazioni che potrebbero risultare inaspettate per l’interessato. Potrebbe trattarsi, ad esempio,

della trasmissione di dati a terzi, in particolare se ubicati al di fuori dell'UE, e del periodo di conservazione dei dati. Se tali informazioni non sono indicate, l'interessato dovrebbe poter confidare nel fatto che vi sia solo una sorveglianza in tempo reale, senza alcuna registrazione di dati o trasmissione a soggetti terzi (ibidem, par. 115). La segnaletica di avvertimento di primo livello deve contenere un chiaro riferimento al secondo livello di informazioni, ad esempio indicando un sito web sul quale è possibile consultare il testo dell'informativa estesa.

Ciò premesso, in merito all'informativa di primo livello conferita mediante apposita cartellonistica allegata al riscontro del XX (all. XX) e tenuto conto di quanto previsto dagli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento, si osserva che essa indica riferimenti non aggiornati in merito alla normativa sulla protezione dei dati personali; non specifica l'identità del titolare del trattamento (v. art. 13, par. 1, lett. a), del Regolamento); non indica le finalità di trattamento perseguite e la base giuridica del trattamento (v. art. 13, par. 1, lett. c), del Regolamento); non specifica i tempi di conservazione delle immagini (v. art. 13, par. 2, lett. a), del Regolamento); non menziona compiutamente i diritti degli interessati di cui agli artt. 15 e seg. del Regolamento e le modalità di esercizio degli stessi (v. art. 13, par. 2, lett. b), del Regolamento); non specifica le modalità attraverso le quali gli interessati possono accedere ad un'informativa completa di "secondo livello" nella quale poter reperire gli ulteriori e completi elementi informativi.

Non si risulta, inoltre, comprovato che il Titolare abbia reso disponibile agli interessati un'informativa completa di secondo livello, risultando, pertanto, in ogni caso compromesso il meccanismo di informativa stratificata basata su un'informativa di primo livello che rimanda un'informativa completa, di secondo livello, messa dal titolare a disposizione degli interessati.

Inoltre, quanto alla specifica informativa sul trattamento dei dati che avrebbe dovuto essere fornita ai lavoratori in relazione al trattamento dei dati mediante il medesimo sistema di videosorveglianza, deve rilevarsi che il Titolare si è limitato a produrre in atti copia di un mero modello d'informativa (all. XX alla nota del XX, in atti), sprovvisto di data certa e sottoscrizione dei lavoratori interessati, per presa visione, nel relativo campo in calce allo stesso. Non risulta, pertanto, sufficientemente comprovato che il Titolare abbia fornito detta informativa ai lavoratori prima di avviare il trattamento in questione.

Alla luce delle considerazioni che precedono, deve concludersi che il Titolare ha effettuato un trattamento di dati personali, mediante dispositivi video, in maniera non conforme al principio di "liceità, correttezza e trasparenza", in violazione degli artt. 5, par. 1, lett. a), 12, par. 1, e 13 del Regolamento.

3.4 La valutazione di impatto sulla protezione dei dati.

Nel corso dell'istruttoria, il Titolare ha dichiarato che "lo svolgimento della [valutazione di impatto sulla protezione dei dati] non è stato ritenuto necessario", in quanto "il trattamento non presenta […] rischi elevati nonostante la presenza di minori poiché le aree riprese sono soprattutto esterne e dedicate ai varchi di accesso".

Al riguardo, si osserva che quando un tipo di trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e, in ogni caso, al ricorrere delle ipotesi tassativamente previste (incluso il caso di "sorveglianza sistematica su larga scala di una zona accessibile al pubblico"), il titolare del trattamento, prima di porre in essere lo stesso, deve svolgere una valutazione di impatto sulla protezione dei dati, al fine di adottare, in particolare, le misure adeguate ad affrontare tali rischi, consultando preventivamente il Garante, ove ne ricorrano i presupposti (v. artt. 35 e 36, par. 1, del Regolamento).

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si ritiene che, nel caso specie, il Titolare avrebbe dovuto svolgere una valutazione di impatto sulla protezione dei dati

prima di avviare il trattamento, atteso che lo stesso, oltre a risolversi in una “sorveglianza sistematica su larga scala di una zona accessibile al pubblico”, comporta rischi specifici per i diritti e le libertà degli interessati, ovvero sia per i lavoratori sia per gli studenti anche minorenni frequentanti. Ciò, tanto in considerazione della particolare “vulnerabilità” degli interessati (cfr. cons. 75 e art. 88 del Regolamento e le “Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679”, WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menzionano espressamente “i dipendenti” e i “minori”) quanto del fatto che sono impiegati sistemi che comportano il “monitoraggio sistematico” in ambito lavorativo, inteso come “trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti” (cfr. criterio n. 3 indicato nelle Linee guida, cit., ma vedi anche criteri 4 e 7; v. artt. 35 e 88, par. 2, del Regolamento; v. anche provv. 11 ottobre 2018, n. 467, doc. web n. 9058979, all. n. 1, che espressamente menziona i “trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici […] dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti”). La mancata esecuzione di una valutazione di impatto sulla protezione dei dati in relazione a sistemi di videosorveglianza impiegati nel contesto lavorativo è stata, per tali motivi, oggetto di recenti provvedimenti anche correttivi e sanzionatori del Garante (v. in particolare, provv.ti 10 luglio 2025, n. 410, cit.; 10 aprile 2025, n. 201, cit.; 13 marzo 2025, n.135, doc. web n. 10128005; 16 novembre 2023, n. 578, doc. web n. 9963486; 1° dicembre 2022, n. 409, doc. web n. 9833530).

Nel caso di specie, il Titolare ha, invece, trattato i dati personali dei propri lavoratori e degli studenti, nonché di terze persone, mediante il sistema di videosorveglianza in questione, in assenza di una preliminare valutazione di impatto sulla protezione dei dati e, pertanto, in violazione dell’art. 35 del Regolamento.

Deve, peraltro, osservarsi, quanto ai tempi di conservazione dei filmati di videosorveglianza (nel caso di specie 8/14 giorni, fino a esaurimento dello spazio di archiviazione, senza meccanismi di cancellazione automatica delle immagini), che le citate “Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video”, adottate dal Comitato europeo per la protezione dei dati, par. 121, ove si evidenzia che “nella maggior parte dei casi (ad esempio se la videosorveglianza serve allo scopo di rilevare atti vandalici) – cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici. Quanto più prolungato è il periodo di conservazione previsto (soprattutto se superiore a 72 ore), tanto più argomentata deve essere l’analisi riferita alla legittimità dello scopo e alla necessità della conservazione”). Lo svolgimento di una valutazione di impatto sulla protezione dei dati, prima di dare avvio al trattamento, avrebbe consentito al titolare anche di effettuare le opportune valutazioni anche con riguardo a tale profilo, come elemento che concorre a definire la complessiva “necessità e proporzionalità dei trattamenti in relazione alle finalità” (art. 35, par. 7, lett. b), del Regolamento).

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell’istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell’art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall’Ufficio con l’atto di avvio del procedimento e risultano insufficienti a consentire l’archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall’art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell’Ufficio e si rileva l’illiceità del trattamento di dati personali effettuato dal Titolare, per aver trattato dati personali mediante un sistema di videosorveglianza, in violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, par. 1, 13, 35 e 88 del Regolamento, nonché 2-ter e 114 del Codice.

Tenuto conto che la violazione delle predette disposizioni ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, le violazioni più gravi, relative agli artt. 5, par. 1, lett. a) e b), 6, 12, par. 1, 13, e 88 del Regolamento, nonché 2-ter e 114 del Codice, sono soggette alla sanzione prevista dall'art. 83, par. 5, del Regolamento, come richiamato anche dall'art. 166, comma 2, del Codice, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti - atteso che, come dichiarato in sede di memoria difensiva, è stato disposto lo "spegnimento di tutte le telecamere" - non ricorrono i presupposti per l'adozione di ulteriori misure correttive di cui all'art. 58, par. 2, del Regolamento. Per quanto riguarda, invece, lo specifico filmato relativo all'infortunio occorso al figlio minore dei reclamanti, si ritiene, altresì, di non potersi adottare le predette misure correttive, atteso che dalla documentazione in atti emerge una situazione di contenzioso tra il Titolare, la famiglia del minore e terzi, in relazione a diversi profili astrattamente riconducibili sia all'ambito civile che a quello penale, anche con interessamento dell'Autorità giudiziaria (cfr. art. 160-bis del Codice).

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

Tenuto conto che:

- il trattamento ha avuto luogo per un esteso arco temporale (dal 2019), avendo, pertanto, riguardato lo stesso un elevato numero di interessati, anche minorenni, ed è stato posto in essere in modo non conforme alla disciplina di settore in materia di impiego di strumenti tecnologici sul luogo di lavoro e alle puntuali indicazioni fornite nel tempo dal Garante sia con provvedimenti a carattere generale sia con decisioni su casi specifici (art. 83, par. 2, lett. a), del Regolamento);

- sebbene il trattamento non abbia riguardato dati particolari appartenenti alle categorie particolari di cui all'art. 9 del Regolamento, hanno formato oggetto di trattamento dati personali relativi a soggetti vulnerabili, tra cui minori e lavoratori, sebbene, in relazione a questi ultimi, il Titolare abbia dichiarato di non aver mai utilizzato le immagini di videosorveglianza a fini disciplinari (cfr. art. 83, par. 2, lett. a) e g), del Regolamento);

la violazione ha carattere colposo (art. 83, par. 2, lett. b), del Regolamento);

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia alto (cfr. Comitato europeo per la protezione dei dati, “Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR” del 24 maggio 2023, punto 60).

Ciò premesso, nel considerare che il titolare del trattamento è un ente ecclesiastico civilmente riconosciuto, e tenuto conto anche del volume d’affari IVA dello stesso relativo all’anno XX, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

non risultano precedenti violazioni pertinenti commesse dal Titolare (art. 83, par. 2, lett. e), del Regolamento);

il Titolare ha offerto una buona cooperazione con l’Autorità nel corso dell’istruttoria (art. 83, par. 2, lett. f), del Regolamento);

la violazione ha riguardato una singola struttura scolastica gestita dal Titolare (art. 83, par. 2, lett. k), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l’ammontare della sanzione pecuniaria nella misura di euro 12.000 (dodicimila) per la violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, par. 1, 13, 35 e 88 del Regolamento, nonché 2-ter e 114 del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell’art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell’art. 166, comma 7, del Codice e dell’art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che, come sopra evidenziato, il trattamento ha avuto luogo per un esteso arco temporale e ha riguardato anche dati personali relativi a soggetti vulnerabili.

Si rileva, infine, che ricorrono i presupposti di cui all’art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell’art. 57, par. 1, lett. f), del Regolamento, l’illiceità del trattamento effettuato dalla Provincia della Congregazione dei Fratelli delle Suore Cristiane per la violazione degli artt. 5, par. 1, lett. a) e b), 6, 12, par. 1, 13, 35 e 88 del Regolamento, nonché 2-ter e 114 del Codice, nei termini di cui in motivazione;

ORDINA

alla Provincia della Congregazione dei Fratelli delle Suore Cristiane, in persona del legale rappresentante pro-tempore, con sede legale in Viale del Vignola, 56 - 00196 Roma (RM), P. IVA 02113801001, di pagare la somma di euro 12.000 (dodicimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell’art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al predetto titolare, in caso di mancata definizione della controversia ai sensi dell’art. 166,

comma 8, del Codice, di pagare la somma di euro 12.000 (dodicimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito internet dell'Autorità;

- ai sensi dell'art. 17 del Regolamento del Garante n. 1/2019, l'annotazione delle violazioni e delle misure adottate in conformità all'art. 58, par. 2 del Regolamento, nel registro interno dell'Autorità previsto dall'art. 57, par. 1, lett. u) del Regolamento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 29 gennaio 2026

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Montuori