

PARTE SECONDA

1. L'AUTORITA' GARANTE
2. GLI STRUMENTI GIURISDIZIONALI: I MEZZI DI RICORSO©
3. IL QUADRO SANZIONATORIO ©
4. ASPETTI RIGUARDANTI LE PUBBLICHE AMMINISTRAZIONI: ACCESSO AGLI ATTI
5. TRATTAMENTI SPECIFICI RIGUARDANDI LE ISTITUZIONI SCOLASTICHE
 - a) Comunicazioni scuola famiglia
 - b) Situazione genitoriale
 - c) Alternanza scuola lavoro
 - d) Scuolabus e mensa scolastica
 - e) Videosorveglianza

L'AUTORITA' GARANTE

L'organo di controllo che sovrintende al rispetto della normativa sulla protezione dei dati è il Garante per la protezione dei dati personali meglio conosciuto come Garante Privacy, figura introdotta già dalla Legge 675/96. L'Ufficio del Garante Privacy è un'Autorità amministrativa indipendente e secondo l'ordinamento ha natura giuridica di Ente Pubblico non economico. Nell'arco di vigenza delle normative che si sono succedute in materia di protezione di dati personali ha accresciuto i suoi poteri ed il suo sindacato giurisdizionale fino alle ultime novità apportate dal d.lgs. 101 del 10 agosto 2018. Tralasciando il percorso storico scopriamo quale ruolo ha ritagliato il Regolamento per l'Organo di controllo. Della materia si occupa il Capo VI in particolare negli articoli da 53 a 59. Da sottolineare che l'art. 53 rilascia agli Stati Membri il compito di regolamentare la nomina del proprio organo. L'articolo 57 elenca i compiti così riassunti:

- a) sorveglia e assicura l'applicazione del presente regolamento;*
- b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento. Sono oggetto di particolare attenzione le attività destinate specificamente ai minori;*
- c) fornisce consulenza, a norma del diritto degli Stati membri, al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;*
- d) promuove la consapevolezza dei titolari del trattamento e dei responsabili del trattamento riguardo agli obblighi imposti loro dal presente regolamento;*
- e) su richiesta, fornisce informazioni all'interessato in merito all'esercizio dei propri diritti*

derivanti dal presente regolamento e, se del caso, coopera a tal fine con le autorità di controllo di altri Stati membri;

f) tratta i reclami proposti da un interessato, o da un organismo, un'organizzazione o un'associazione ai sensi dell'articolo 80, e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole, in particolare ove siano necessarie ulteriori indagini o un coordinamento con un'altra autorità di controllo;

g) collabora, anche tramite scambi di informazioni, con le altre autorità di controllo e presta assistenza reciproca al fine di garantire l'applicazione e l'attuazione coerente del presente regolamento;

h) svolge indagini sull'applicazione del presente regolamento, anche sulla base di informazioni ricevute da un'altra autorità di controllo o da un'altra autorità pubblica;

i) sorveglia gli sviluppi che presentano un interesse, se e in quanto incidenti sulla protezione dei dati personali, in particolare l'evoluzione delle tecnologie dell'informazione e della comunicazione e le prassi commerciali;

j) adotta le clausole contrattuali tipo di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d);

k) redige e tiene un elenco in relazione al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35, paragrafo 4;

l) offre consulenza sui trattamenti di cui all'articolo 36, paragrafo 2;

m) incoraggia l'elaborazione di codici di condotta ai sensi dell'articolo 40, paragrafo 1, e fornisce un parere su tali codici di condotta e approva quelli che forniscono garanzie sufficienti, a norma dell'articolo 40, paragrafo 5;

n) incoraggia l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati a norma dell'articolo 42, paragrafo 1, e approva i criteri di certificazione a norma dell'articolo 42, paragrafo 5;

o) ove applicabile, effettua un riesame periodico delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;

p) definisce e pubblica i criteri per l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;

q) effettua l'accreditamento di un organismo per il controllo dei codici di condotta ai sensi dell'articolo 41 e di un organismo di certificazione ai sensi dell'articolo 43;

r) autorizza le clausole contrattuali e le altre disposizioni di cui all'articolo 46, paragrafo 3;

- s) approva le norme vincolanti d'impresa ai sensi dell'articolo 47;*
- t) contribuisce alle attività del comitato;*
- u) tiene registri interni delle violazioni del presente regolamento e delle misure adottate in conformità dell'articolo 58, paragrafo 2; e*
- v) svolge qualsiasi altro compito legato alla protezione dei dati personali.*

Il successivo art. 58 invece delinea i poteri dell'Autorità che sono suddivisi in poteri di indagine, poteri correttivi, poteri autorizzativi e consultivi così a seguito sintetizzati:

POTERI DI INDAGINE:

- a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti;
- b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati;
- c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7;
- d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento;
- e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e
- f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.

POTERI CORRETTIVI:

- a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento;
- b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento;
- c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento;
- d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata

maniera ed entro un determinato termine;

e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali;

f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento;

g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19;

h) revocare la certificazione o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti;

i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e

j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.

POTERI AUTORIZZATIVI E CONSULTIVI:

a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36;

b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali;

c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare;

d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5;

e) accreditare gli organismi di certificazione a norma dell'articolo 43;

f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5;

g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e

all'articolo 46, paragrafo 2, lettera d);

h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a);

i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b);

j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47.

All'interno dello stesso articolo troviamo al paragrafo 4, inoltre, le modalità di esercizio del potere da parte dell'Autorità. Il paragrafo 5 invita gli Stati Membri a regolamentare l'intervento autonomo in sede giudiziale o extragiudiziale per far rispettare il Regolamento. Il paragrafo 6 invece rappresenta una delle clausole di apertura che il GDPR ha rilasciato agli Stati membri e attraverso la quale ogni Stato può prevedere ulteriori poteri. Nel d.lgs. 101 ciò è accaduto con l'introduzione dell'art. 154 bis che autorizza il Garante a adottare Linee Guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione del regolamento e approvare le regole deontologiche previste per il trattamento da parte di pubblici poteri, per i trattamenti di dati particolari e per i trattamenti nell'ambito dell'informazione, del rapporto di lavoro, e della ricerca scientifica – storica - statistica ; l'art. 154 ter che autorizza il Garante ad agire in giudizio in caso di violazione in materia di protezione dei dati personali; con l'art. 166 comma quattro il legislatore ha infine dato possibilità al Garante di avviare d'Ufficio in base ai poteri di indagine sanciti all'art. 58 paragrafo 1 e di cui si parlerà più approfonditamente nelle prossime pagine.

GLI STRUMENTI GIURISDIZIONALI: I MEZZI DI RICORSO

- 1. Reclamo al Garante (art. 77 Regolamento UE, artt. 141-142-143 Codice Privacy)**
- 2. Segnalazioni al garante (art. 144 Codice Privacy)**
- 3. Ricorso giurisdizionale (artt. 78-79-80-81 Regolamento UE e art. 152 Codice Privacy)**

RECLAMO

Il reclamo è l'unico strumento amministrativo che consente all'interessato di rivolgersi direttamente al Garante dello Stato dove risiede abitualmente oppure dove si è verificata la violazione per denunciare una qualsiasi inosservanza della disciplina in materia di protezione dei dati personali e di richiedere pertanto una verifica ai sensi dell'art. 77 del Regolamento e degli artt. da 140-bis a 143 del Codice Privacy.

Legittimati attivi ad una tale azione sono gli interessati o le associazioni che li rappresentano. Mentre legittimati passivi sono i Titolari e i Responsabili.

Il Regolamento non fissa un termine per la conclusione della procedura in quanto la normativa nazionale vi dovrà provvedere. Tuttavia, il Garante deve comunque informare il reclamante dello

stato o dell'esito del reclamo e dare la comunicazione della possibilità di un ricorso giurisdizionale (art. 77 paragrafo 2).

La proposizione del reclamo avviene secondo le regole procedurali dell'art. 142 del Codice Privacy; precisamente la norma dispone che esso debba riportare in modo dettagliato e circostanziato i fatti violati nonché le disposizioni non rispettate unitamente agli estremi identificativi del Titolare o del Responsabile del trattamento. Dovrà essere allegata la documentazione utile al riguardo. Il reclamo è gratuito e deve essere predisposto utilizzando la modulistica messa a disposizione del Garante sul proprio sito web. La sottoscrizione del reclamo può essere apposta anche da parte di enti ed associazioni rappresentative dei diritti degli interessati. Il Garante disciplina con proprio regolamento il procedimento per l'esame dei reclami e le modalità semplificate nonché i termini abbreviati per la loro trattazione se relativi alla violazione dei diritti degli interessati.

La decisione sul reclamo avviene, ai sensi dell'art. 143 Codice Privacy, nel termine massimo di nove mesi dalla data di presentazione; comunque entro tre mesi da questa data, il Garante deve informare l'interessato sullo stato del procedimento. Il termine può dilazionarsi a dodici mesi (in luogo di nove) solo per motivate esigenze istruttorie che vanno comunicate all'interessato. Tuttavia, il Garante ancor prima di decidere sul reclamo, non appena terminata l'istruttoria oppure quando il reclamo risulta non manifestamente infondato e ne sussistono i presupposti, può adottare i provvedimenti indicati dall'art. 58 del Regolamento (in virtù dei suoi poteri di indagine, correttivi e autorizzativi). La decisione del Garante è pubblicata sulla Gazzetta Ufficiale se i destinatari non sono facilmente identificabili per numero o per la complessità degli accertamenti. La decisione sul reclamo oppure il silenzio del Garante il quale non abbia comunicato nei termini le informazioni circa lo stato del procedimento (entro i tre mesi dalla data di presentazione del reclamo) può essere impugnata mediante ricorso giurisdizionale davanti al giudice ordinario.

L'art. 140-bis introdotto dal D.Lgs. 101/2018 nel Codice privacy prevede espressamente la tutela del doppio binario (amministrativo e giurisprudenziale) nel senso che la proposizione del reclamo è inibita se per la medesima fattispecie concreta è stata già stata adita l'autorità giurisdizionale. Altresì la proposizione della domanda dinanzi all'autorità giudiziaria è improponibile nel caso in cui sia stato già proposto reclamo al Garante (salvo il caso in cui il Garante non abbia deciso entro i termini previsti).

SEGNALAZIONE

Ai sensi dell'art. 144 del Codice Privacy chiunque può segnalare al Garante possibili violazioni sull'applicazione della normativa privacy in modo che il Garante possa adottare un provvedimento di

cui all'art. 58 del Regolamento. Si tratta di una semplice forma di interlocuzione con il Garante che non implica un procedimento istruttorio.

Le misure di competenza del Garante (conseguenti ai poteri di indagine, correttivi, autorizzativi e consultivi) possono essere adottate anche d'ufficio a prescindere dal reclamo o dalla segnalazione: in tal modo viene ampliata la gamma dei provvedimenti che possono essere adottati ancor prima che inizi l'istruttoria preliminare della violazione.

RICORSO GIURISDIZIONALE EFFETTIVO

L'autorità competente è il giudice ordinario in funzione di giudice del lavoro e, all'uopo, ai sensi del Codice Privacy all'art. 152 comma 2 per le controversie in materia di protezione dei dati personali deve essere seguita la procedura giuslavoristica (D.Lgs. 150/2011 art. 10).

Il diritto al ricorso giurisdizionale di cui agli artt. 78 e 79 del Regolamento deve essere “*effettivo*”. Il riferimento al concetto di “rimedio effettivo” si collega al principio fondamentale dell'UE (art. 47 Carta UE): *«Ogni persona i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni persona ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato, qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia.»*

La competenza del giudice ordinario riguarda tre tipologie di tutele:

1. AVVERSO IL GARANTE art. 78 del Regolamento

Sono impugnabili:

- le decisioni giuridicamente vincolanti del Garante assunte in sede di reclamo o nell'esercizio dei poteri di indagine, correttivi e autorizzativi;
- la mancata trattazione del reclamo nel termine di nove mesi dalla presentazione della domanda;
- il mancato riscontro entro il primo trimestre dalla presentazione della domanda;
- l'archiviazione, il rigetto o l'inattività del garante o le decisioni ritenute insoddisfacenti

Non sono impugnabili i pareri o la consulenza in quanto non giuridicamente vincolati.

Sono soggetti attivi dell'impugnazione: i Titolari, i Responsabili, gli interessati e gli enti rappresentativi dei diritti degli interessati. Mentre sono soggetti passivi le parti del procedimento impugnato.

E' possibile per il giudice ordinario investire la Corte di giustizia europea in via pregiudiziale per questioni interpretative necessarie alla soluzione del caso.

2. AVVERSO IL TITOLARE O IL RESPONSABILE DEL TRATTAMENTO art. 79 del Regolamento

Sono impugnabili:

- ogni violazione delle norme del Regolamento integrate dalle norme nazionali del Codice della Privacy.

Sono soggetti attivi dell'impugnazione: gli interessati e gli enti rappresentativi dei diritti degli interessati. Mentre i soggetti passivi sono il Titolare del Trattamento e il Responsabile.

Il foro competente è quello dove risiede lo stabilimento del Titolare o del Responsabile oppure in alternativa quello della residenza abituale dell'interessato. Se il Titolare è un'autorità pubblica il foro esclusivo è il luogo di stabilimento del pubblico potere.

E' possibile anche in questo caso per il giudice ordinario investire la Corte di giustizia europea in via pregiudiziale di questioni interpretative necessarie per la soluzione del caso.

3. DOMANDE DI RISARCIMENTO DEL DANNO art. 82 del Regolamento

Il risarcimento del danno per fatto illecito causato da qualsiasi violazione del Regolamento o del Codice Privacy può essere richiesto da chiunque sia nei confronti del Titolare sia nei confronti del Responsabile.

Per danno deve intendersi quello materiale e quello immateriale. Dal Considerando 75 le conseguenze del danno possono essere così enunciate: *“discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti*

riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali”.

L'interessato dovrà dimostrare con prove l'esistenza di un trattamento dei suoi dati, la violazione delle norme e il danno subito.

La imputabilità del danno è sempre in capo al Titolare. Tuttavia nel caso in cui il Responsabile non abbia adempiuto in modo corretto alle istruzioni del Titolare oppure abbia disatteso le disposizioni regolamentari risponderà personalmente del danno cagionato.

La responsabilità si basa sulla presunzione di colpa del Titolare o del Responsabile (inversione dell'onere della prova): ai sensi del comma 3 essi dovranno dimostrare di aver messo in campo tutte le misure adeguate per evitare il fatto illecito dannoso e che il danno quindi è dovuto al caso fortuito o a forza maggiore. La ragione di ciò è data dal fatto che l'attività del trattamento dati è caratterizzata da un rischio socialmente elevato.

QUADRO SANZIONATORIO

ILLECITI AMMINISTRATIVI

Il nuovo quadro sanzionatorio amministrativo pecuniario direttamente applicabile è delineato esaustivamente dall' art. 83 del Regolamento UE che fissa i principi nonché i limiti massimi delle sanzioni; sono invece rimesse alla libera determinazione delle autorità preposte in sede giurisdizionale le sanzioni per ulteriori violazioni rispetto a quelle previste dal suddetto articolo.

Nel Considerando 11 viene rafforzata la necessità di un'azione sanzionatoria equivalente per tutti gli Stati membri unitamente a poteri di controllo che possano assicurare in modo uniforme la tutela in caso di violazioni. Si tratta del principio generale di armonizzazione il quale, unitamente al principio di coerenza di cui all'art. 63, mira ad evitare squilibri tra gli Stati membri (il Comitato europeo per la protezione dei dati elabora linee guida per le autorità relativamente a controlli riguardanti le violazioni che ricadono nelle sanzioni amministrative pecuniarie art. 70 paragrafo 1 lett. k).

Inoltre la regolamentazione sanzionatoria deve garantire “*certezza del diritto e trasparenza*” offrendo agli interessati gli stessi livelli di protezione e imponendo a titolari e responsabili identici vincoli e responsabilità (Considerando 13).

Le sanzioni amministrative pecuniarie vengono inflitte dal Garante in alternativa o in aggiunta ad altri poteri correttivi di cui all'art. 58 paragrafo 2 (avvertimenti, ammonimenti, ingiunzioni, imposizioni di limitazioni, ordini di rettifica e cancellazione, revoca delle certificazioni) sulla base di principi comuni fissati dal legislatore europeo che devono tener conto degli elementi di cui all'art. 83 paragrafo 2 che sono:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;

b) il carattere doloso o colposo della violazione; si tratta quindi di valutare l'elemento soggettivo dell'azione;

c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati; si tratta quindi di valutare le modalità della condotta;

d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32; si tratta quindi di valutare il rispetto dei principi nel caso di applicazione delle misure di sicurezza;

e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;

f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi; si tratta del c.d. ravvedimento operoso;

g) le categorie di dati personali interessate dalla violazione; si tratta quindi di considerare una violazione dei dati particolari e dei dati sui minori in modo più stringente rispetto a dati di altre categorie;

h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione; si tratta quindi di commisurare tale indicazione con il principio di responsabilizzazione;

i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2 (azioni correttive del garante), nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;

j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; si tratta di tenere presente l'eventuale violazione dei codici di condotta in quanto aggravante dell'azione illecita;

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione; si tratta di valutare altri elementi tra cui la buona fede nelle azioni commesse, ad esempio quando la finalità perseguita non è legata alla violazione commessa;

Oltre a quanto sopra riportato il Garante assume il potere di irrogare le sanzioni amministrative pecuniarie che devono in ogni caso essere “*effettive, proporzionate e dissuasive*”; in particolare, la sanzione ha il duplice scopo di reprimere gli illeciti avvenuti e di prevenire gli illeciti futuri. L’applicazione della sanzione non può dunque essere meccanica e automatica ma dovrà essere ponderata cioè dovrà essere valutata caso per caso affinché sia il più possibile equa.

Qualora, per un singolo trattamento o più trattamenti collegati, un titolare o responsabile violi, con dolo o colpa, più disposizioni si applica la sanzione per la violazione più grave (c.d. limite al cumulo sanzionatorio).

Inoltre nell’infliggere una sanzione ad una persona fisica occorre tener presente, nel determinare l’importo della sanzione amministrativa, il livello generale di reddito e della situazione economica della persona stessa sicché, se il reddito è insufficiente, potrebbe essere ragionevolmente prescritto dal Garante un semplice ammonimento. L’ammonimento può essere più efficiente perché consente di prevenire le possibili conseguenze che potrebbero verificarsi con il prolungarsi della violazione medesima o di ulteriori infrazioni.

Da sottolineare che ai soggetti a cui è addebitata la violazione vanno assicurati i principi costituzionali delle garanzie procedurali adeguate ai principi UE e nazionali compreso il giusto processo.

In Italia il D.lgs. 101/2018 ha novellato l’adeguamento sanzionatorio alle disposizioni regolamentari. Premesso che nel determinare l’importo della sanzione si deve far sì che questa rispetti in ogni singolo caso l’effettività, la proporzionalità in riferimento alla gravità e l’efficacia, gli illeciti amministrativi vengono suddivisi in base alla gravità della sanzione.

A titolo esemplificativo vengono riportate le fattispecie che possono verificarsi sulla base delle violazioni e inosservanze delle disposizioni regolamentari e nazionali.

Le sanzioni amministrative pecuniarie sono di tre tipologie che corrispondono a due livelli di importi massimi predefiniti.

PRIMA TIPOLOGIA DI SANZIONE Art. 83 paragrafo 4 e art. 166 Codice Privacy

Fino a 10 milioni di Euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell’esercizio precedente, se superiore

Violazione dei seguenti obblighi	Norme del Regolamento o del Codice privacy
In materia di trattamento dati che non richiedono l'identificazione	Art. 11 Reg.
In materia di privacy by design e privacy by default	Art. 25 Reg.
In materia di contitolari e rappresentanti di titolari	Artt. 26-27 Reg.
In materia di Responsabile del trattamento e degli autorizzati al trattamento	Artt. 28-29 Reg
Degli obblighi inerenti la tenuta del Registro dei trattamenti e del registro delle violazioni;	Artt. 30 e 33 c. 5 Reg.
Degli obblighi sulla sicurezza; data breach; registro delle violazioni	Artt. 32-33-34 Reg.
In materia di Valutazione di Impatto Privacy e consultazione preventiva	Artt. 35 -36 Reg.
In materia di nomina del Responsabile della Protezione dei dati	Art. 37-38-39
In materia di obblighi dell' organo di controllo	Art. 41 par. 4 Reg.
In materia di obblighi dell' organismo di certificazione	Artt. 42-43 del Reg.
Di fornire al minore di anni quattordici un'informativa chiara e semplice con un linguaggio comprensibile;	Art. 166 c. 1 Codice
Delle misure a garanzia dell'interessato per i trattamenti che presentano rischi elevati per l'esecuzione di un compito di interesse pubblico;	Art. 2- <i>quaterdecies</i> Codice
Violazione delle modalità di redazione e conservazione di cartelle cliniche	Art. 92 c. 1 Codice
Delle disposizioni sulla redazione del certificato di assistenza al parto	Art. 93 c. 1 Codice
Violazione, da parte del titolare, degli obblighi di informativa all'utente sulla natura dei dati di traffico telefonico e telematico e sulla durata del trattamento	Art. 123 c. 4 Codice
Violazione, da parte del fornitore del servizio di comunicazione elettronica, degli obblighi relativi alla fatturazione dettagliata dei dati di traffico, al trasferimento automatico della chiamata e violazione degli obblighi relativi alla sicurezza del trattamento	Artt. 124-128-132- <i>ter</i> Codice
Violazione del provvedimento del Garante di individuazione delle modalità di manifestazione del consenso all'inclusione negli elenchi telefonici cartacei e elettronici e all'utilizzo dei relativi dati per marketing	Art. 129 c. 2 Codice

SECONDA TIPOLOGIA DI SANZIONE Art. 83 paragrafo 5 e art. 166 Codice Privacy

Fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Violazione dei seguenti obblighi	Norme del Regolamento o del Codice Privacy
Principi base del trattamento e condizioni di liceità, comprese le condizioni del consenso	Artt. 5-6-7-9 Reg.
Diritti degli interessati (informativa, diritto di accesso, diritto di rettifica e cancellazione, diritto alla limitazione del trattamento, diritto alla portabilità del dato, diritto di opposizione, diritto a non essere profilati in modo automatizzato)	Da artt. 12 a 22 Reg.
Trasferimenti di dati personali a un destinatario in un paese terzo o un'organizzazione internazionale	Da artt. 44 a 49 Reg.
Qualsiasi violazione inerente altre fattispecie di cui al capo IX del Regolamento UE relativi a peculiari situazioni di trattamento (come libertà di espressione e di informazione, rapporti di lavoro, ricerca scientifica, statistica e storica, sanità, accesso ai documenti delle pubbliche amministrazioni)	Da artt. 85 a 89 Reg.
Inosservanza di un ordine di limitazione o di sospensione nell'ambito dei poteri correttivi del Garante	Art. 58 par. 2 Reg.
Diniego di accesso del garante mentre svolge poteri di indagine	Art. 58 par. 1
Disposizioni relative alla comunicazione e diffusione di dati personali da parte di titolari che effettuato il trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri	Art. 2-ter Codice
Consenso del minore per i servizi della società dell'informazione	Art. 2- <i>quinqies</i> Codice
Delle norme sul trattamento di particolari categorie di dati personali per rilevanti motivi di interesse pubblico rilevante	Art. 2- <i>sexies</i> Codice
Delle norme sulla diffusione in dati genetici, biometrici e relativi alla salute	Art. 2- <i>septies</i> Codice
Delle norme sul trattamento dei dati relativi a condanne penali	Art. 2- <i>octies</i> Codice
Delle disposizioni sul trattamento dei dati personali relativi a persone decedute	Art. 2- <i>duodecies</i> Codice
Delle norme sull'indicazione dei dati identificativi degli interessati in provvedimenti giurisdizionali in violazione della disciplina che consente all'interessato di precludere tale indicazione nella riproduzione dei provvedimenti	Art. 52 Codice
Della disciplina sul trattamento dei dati sanitari	Art. 75 Codice
Delle disposizioni sull'informativa da fornire all'interessato nell'ambito dei trattamenti sanitari, anche d'emergenza	Artt. 78-80-82 Codice
Delle disposizioni sulla presa visione e il rilascio di cartella clinica a soggetto diverso dall'interessato	Art. 92 c. 2 Codice
Delle norme sulle rilascio a terzi di certificato di assistenza al parto	Art. 93 c. 2 3 Codice

Delle disposizioni sulla comunicazione e diffusione di dati relativi a studenti	Art. 96 Codice
Delle disposizioni sulla durata del trattamento in caso di trattamento a fini di archiviazione nel pubblico interesse o di ricerca scientifica	Art. 99 Codice
Diffusione di dati per fini di studio da parte di università ed enti di ricerca	Art. 100 c. 1,2-4 Codice
Modalità di trattamento di dati per scopi storici, per scopi statistici e scientifici	Art. 101-105 c. 1,2-4 Codice
Delle disposizioni sul diritto di rettifica in relazione al trattamento dei dati relativi alla salute per fini di ricerca medica, biomedica ed epidemiologica	Art. 110 c. 2 Codice
Delle regole deontologiche nei trattamenti in materia di lavoro e previdenza	Art. 111 Codice
Della disciplina sull'informativa all'interessato nel primo contatto dopo la ricezione del curriculum	Art. 111-bis Codice
Delle disposizioni sul trattamento dei dati da parte degli istituti di patronato	Art. 116 c. 1 Codice
Delle norme sul trattamento e comunicazione di dati all'istituto di vigilanza sulle assicurazioni a fini di contrasto delle frodi assicurative	Art. 120 c. 2 Codice
Delle disposizioni sul trattamento di informazioni nell'apparecchio terminale del contraente o utente di servizi di comunicazione elettronica	Art. 122 Codice
Mancata cancellazione di dati relativi al traffico telefonico e telematico, conservazione degli stessi a fini di fatturazione oltre i sei mesi, mancato consenso al trattamento dei dati a fini di commercializzazione di servizi e trattamento da parte di soggetti diversi dal delegato	Art. 123 c. 1,2,3 e 5 Codice
Violazione, da parte del fornitore del servizio di comunicazione elettronica, degli obblighi relativi alla fatturazione dettagliata dei dati di traffico	Art. 124 Codice
Violazione dell'obbligo, a richiesta, di impedire l'identificazione della linea	Art. 125 Codice
Delle disposizioni sui dati relativi all'ubicazione diversi dai dati del traffico	Art. 126 Codice
Delle disposizioni sulle comunicazioni indesiderate	Art. 130 da c. 1 a c.4 Codice
Delle disposizioni su informazioni a contraenti e utenti	Art. 131 Codice
Delle disposizioni sulla conservazione dei dati di traffico telefonico e telematico	Art. 132 Codice
Violazione degli obblighi per i fornitori dei servizi di comunicazione elettronica di fornire al Garante le informazioni sulle procedure interne	Art. 132-bis c. 2 Codice
Delle disposizioni sulle informazioni del fornitore ad abbonati e utenti sui rischi di violazioni della sicurezza	Art. 132-quater Codice
Violazione delle regole deontologiche	Art. 132-quinquies Codice

Violazione delle misure di garanzia e delle misure tecniche introdotte dal Garante in relazione ai dati genetici, biometrici e relativi alla salute	Art. 2-septies Codice
La comunicazione a terzi, il trasferimento e la diffusione di dati personali degli interessati iscritti al registro delle opposizioni da parte del titolare del trattamento, per fini di pubblicità o di vendita ovvero per il compimento di ricerche di mercato o di comunicazione commerciale non riferibili alle attività, ai prodotti o ai servizi offerti dal titolare del trattamento	Legge n. 5/2018 art. 1 c. 9
La violazione del diritto di opposizione al trattamento di dati per fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale, mediante l'impiego del telefono	Legge n. 5/2018 art. 1 c. 10

TERZA TIPOLOGIA DI SANZIONE Art. 83 paragrafo 6

Fino a 20 milioni di Euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

Violazione dei seguenti obblighi	Norme del Regolamento o del Codice Privacy
Inosservanza di un ordine da parte del Garante nell'esercizio del potere correttivo	Art. 58 parg. 2 Reg.

L'irrogazione della sanzione è effettuata dal Garante nei confronti sia di soggetti privati sia di autorità pubbliche a seguito di:

- reclamo;
- attività istruttoria e di indagine del Garante;
- ispezioni, verifiche e accessi disposti dal Garante (anche delegabili);
- attività di accertamento.

Il Garante avvia il procedimento notificando al Titolare o al Responsabile le presunte violazioni; questi entro trenta giorni possono inviare memorie difensive oppure chiedere di essere ascoltati in audizione. Per l'adozione dei provvedimenti sanzionatori il Garante deve far riferimento alla L. n. 689 del 1981; in particolar modo deve applicare i principi generali sulle sanzioni amministrative, la disciplina del procedimento applicativo (ordinanza, ingiunzione e eventuale opposizione) e dell'eventuale esecuzione forzata, del possibile pagamento rateale della sanzione e della prescrizione

dell'illecito. E' prevista la possibilità per il garante di applicare come sanzione amministrativa accessoria la pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito del Garante. Il 50% delle sanzioni riscosse annualmente sono riassegnate al Fondo presso il Ministero dell'economia per le spese di funzionamento del Garante. Al trasgressore è offerta la possibilità del pagamento della sanzione in misura ridotta se esercita tale possibilità "entro il termine previsto per la proposizione del ricorso» e se si adegua alle prescrizioni del Garante.

ILLECITI PENALI

L'impianto sanzionatorio degli illeciti penali è stato ridisegnato dal D.Lgs. 101/2018 che modifica il Codice Privacy D.Lgs. 196/2003. Il Regolamento UE prevede esclusivamente gli illeciti amministrativi mentre la definizione degli illeciti penali è stata demandata, ai sensi dell'art. 84 del Regolamento UE, alle singole legislazioni nazionali. Nel rispetto del principio del *ne bis in idem*, la scelta del nostro legislatore è stata quella di non prevedere per un illecito amministrativo anche una corrispondente sanzione penale. Pertanto, il D.Lgs. 101/2018 ha operato un processo di depenalizzazione attraverso l'abrogazione di alcune fattispecie penali che prima erano previste negli articoli 169 e 170 del vecchio Codice Privacy. Tanto premesso, nel nuovo Codice della Privacy si rilevano le seguenti nove diverse ipotesi di reati penali nei seguenti casi:

Violazione penale	Articolo del Codice	Pena prevista	Condizione per sanzionare
Trattamento illecito dei dati personali. Reato base.	Art. 167 comma 1	Reclusione da sei mesi ad un anno e sei mesi	Dolo di profitto e dolo di danno; nocumento all'interessato
Trattamento illecito dei dati particolari e giudiziari nonché le violazioni delle misure di garanzia, delle regole deontologiche per i trattamenti con rischi specifici. Reato aggravato.	Art. 167 comma 2	Reclusione da uno a tre anni	Dolo di profitto e dolo di danno
Trasferimento illecito di dati personali verso paesi terzi o organizzazione internazionale (al di fuori dei casi consentiti)	Art. 167 comma 3	Reclusione da uno a tre anni	Dolo di profitto e dolo di danno; nocumento all'interessato
Comunicazione e diffusione illecita di dati personali riferibili a un rilevante numero di persone	Art. 167-bis	Reclusione da uno a sei anni	Dolo di profitto e dolo di danno

(violazione degli art. 2-ter: nell'esercizio di pubblici poteri;			
Acquisizione fraudolenta di dati personali contenenti in un archivio automatizzato o parte di esso oggetto di trattamento su larga scala	Art. 167-ter	Reclusione da uno a quattro anni	Dolo di profitto e dolo di danno
Falsità nelle dichiarazioni al Garante in un procedimento o in corso di accertamenti	Art. 168 comma 1	Reclusione da sei mesi a tre anni	Mera condotta oggettiva
Interruzione intenzionale o turbativa della regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti	Art. 168 comma 2	Reclusione sino ad un anno	Dolo di profitto e dolo di danno
Inosservanza dei provvedimenti del Garante	Art. 170	Reclusione da tre mesi a due anni	Mera condotta oggettiva
Violazione delle disposizioni in materia di controlli a distanza e indagini sulle opinioni politiche, religiose, sindacali dei lavoratori	Art. 171	Ammenda da € 154,00 ad € 1.549,00 o con l'arresto da 15 giorni ad un anno	Mera condotta oggettiva

Il Procedimento di collegamento tra Garante e autorità giudiziaria è caratterizzato dalla cooperazione. Infatti, il Pubblico Ministero quando ha notizia del reato deve informare senza indugio il Garante. Successivamente il Garante dovrà trasmettere al Pubblico Ministero una relazione motivata di accompagnamento alla documentazione raccolta durante l'attività istruttoria di accertamento. La relazione motivata rappresenta una novità per il nostro sistema normativo e comporterà probabilmente un incremento dei procedimenti penali in materia.

Potrebbe tuttavia accadere che per una medesima fattispecie di violazione sia stata già applicata dal Garante una sanzione amministrativa pecuniaria. In tal caso la pena è diminuita.

Come pena accessoria l'art. 172 prevede per tutti i reati la pubblicazione della sentenza sul sito del ministero di giustizia a spese del condannato per non più di trenta giorni.

ASPETTI RIGUARDANTI LE PUBBLICHE AMMINISTRAZIONI: ACCESSO AGLI ATTI

Su questo versante né il Regolamento né tanto meno il novellato Codice hanno introdotto novità rimettendo, anzi, la materia alle normative nazionali. Recita l'art. 86 del Regolamento "I dati personali contenuti in documenti ufficiali in possesso di un'autorità pubblica o di un organismo

pubblico o privato per l'esecuzione di un compito svolto nell'interesse pubblico possono essere comunicati da tale autorità o organismo conformemente al diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti, al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali ai sensi del presente regolamento."

Il discorso si sposta quindi sulla normativa italiana che riguarda l'accesso agli atti. Normativa che nel corso degli ultimi 25 anni ha subito notevoli evoluzioni ed ampliamenti culminati con l'emanazione del d.lgs. 97 del 2016 meglio conosciuto come F.O.I.A. italiano. Ma andiamo con ordine. Questo aspetto è quello che ci interessa più da vicino in quanto le Pubbliche Amministrazioni trattano dati in forza di una norma di legge. Trattamento che a differenza di quanto avviene in ambito privato deve soggiacere anche a requisiti di trasparenza. Tali obblighi sono enunciati all'interno del d.lgs. 33/2013 (novellato dal d.lgs 97/2016). Queste normative si sono sommate alla legge 241 del 1990 che per la prima volta aveva ammesso a determinate condizioni (interesse legittimo concreto e attuale) una forma di accessibilità ai dati contenuti all'interno di un procedimento amministrativo. Questo il quadro normativo di fonte primaria. Sulla scorta di quanto prodotto dal legislatore l'ANAC ha emanato apposite linee guida (1309 e 1310 del 28 dicembre 2016) che dovevano rappresentare la linea di indirizzo per la corretta applicazione di tutte le norme sopramenzionate. In realtà quando il tema si è spostato sulla tutela dei dati l'Autorità ha tirato il freno a mano ed ha concluso pilatescamente che il bilanciamento tra diritto alla trasparenza e diritto alla tutela dei dati va valutato caso per caso, senza fornire tra l'altro parametri idonei a misurare il peso degli interessi in campo. Il cerino resta in mano alla singola amministrazione che sulla base della propria discrezionalità stabilisce la qualità e la quantità dei dati da ostendere sulla base della valutazione operata.

Ma di che tipo di valutazione parliamo? Questo passaggio è fondamentale per una Pubblica Amministrazione. I casi possono essere svariati. Proviamo a fare un'elencazione di certo non esaustiva ma verosimile.

Partiamo dall'accesso documentale quello previsto dall'art. 22 della legge 241/90. In questo caso parliamo di un tipo di accessibilità profonda e mirata. Vale a dire che i dati rilasciabili possono essere molteplici e anche di tipo particolare proprio perché l'interesse che si intende tutelare da parte di colui che attiva il procedimento deve essere di almeno pari dignità se non superiore. Rileviamo quindi che il diritto alla tutela dei propri dati non è un diritto assoluto e non è opponibile nei confronti di chiunque ma può soggiacere, in determinati casi, ad un diritto di pari o superiore rango. In questo caso diventa fondamentale un'adeguata valutazione da parte dell'amministrazione sugli interessi in campo e sulla qualità di dati da ostendere. Tanto più peserà l'interesse legittimo concreto e attuale da parte del procedente tanto meno resistenza potrà essere opposta al rilascio di dati personali e addirittura particolari (ex sensibili) fermo restando l'obbligo da parte dell'amministrazione di interpellare il proprietario dei dati (controinteressato art. 5 DPR 184/2005).

Nessun problema particolare nel caso invece di accesso civico cosiddetto semplice previsto nel d.lgs 33/2013 in quanto la qualità e la quantità di dati sono predeterminati dalla norma. Resta fermo l'obbligo di non eccedenza della finalità rispetto a quanto prescritto dal testo legislativo.

L'attenta valutazione caso per caso è invece richiesta dall'evoluzione del d.lgs 33 come modificato dal d.lgs 97/2016: l'accesso civico generalizzato. Questo istituto giuridico così come recita la norma prevede “...la libertà di accesso di chiunque ai dati e ai documenti detenuti dalle pubbliche amministrazioni... nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti” Le linee guida ANAC hanno contribuito a disciplinare quest'ultimo aspetto e cioè i limiti imposti dalla norma per la tutela di interessi giuridicamente rilevanti. Cosa dice l'Authority? L'Anac ci ricorda che “Il richiamo espresso alla disciplina legislativa sulla protezione dei dati personali da parte dell'art. 5-bis, comma 2, lett. a), del d. lgs. n. 33/2013 comporta, quindi, che nella valutazione del pregiudizio concreto, si faccia, altresì, riferimento ai principi generali sul trattamento e, in particolare, a quelli di necessità, proporzionalità, pertinenza e non eccedenza” In altre parole l'Anac sottolinea anche in questo caso che il bilanciamento dei diritti è indispensabile per una giusta conclusione di un procedimento di accesso civico generalizzato. E ci dice tra le righe che quanto previsto dalla norma sulla trasparenza non può essere utilizzato come grimaldello alla disclosure di dati che nulla hanno a che fare con “forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e promuovere la partecipazione al dibattito pubblico”. In conclusione, il rilascio di dati personali in questo caso deve essere fortemente limitato a quanto già previsto dalla norma stessa e non può diventare un sistema di controllo individuale sulle singole attività ma rimanere nell'alveo della verifica generale della complessiva attività amministrativa e dell'utilizzo delle risorse pubbliche. Da ciò si deduce che ad oggi è ancora l'accesso documentale ai sensi dell'art. 22 della legge 241/90 la modalità operativa più penetrante in fatto di ostensione di dati.

TRATTAMENTI SPECIFICI RIGUARDANDI LE ISTITUZIONI SCOLASTICHE II PARTE

Comunicazioni scuola famiglia:

Sul tema il Garante ha specificato che “Il diritto–dovere di informare le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere sempre bilanciato con l'esigenza di tutelare la personalità dei minori. È quindi necessario evitare di inserire, nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari, dati personali che rendano identificabili, ad esempio, gli alunni coinvolti in casi di bullismo o in altre vicende particolarmente delicate”

Situazione genitoriale:

Sempre più spesso la situazione genitoriale può presentare aspetti problematici per il trattamento dei dati. A questo proposito è intervenuta la nota MIUR 2 settembre 2015 n. 5536 che ha fornito utili disposizioni sulle modalità di comportamento delle scuole nei casi di genitori separati affermando il diritto alla bigenitorialità e di conseguenza alla condivisione delle scelte educative fatta salva l'ipotesi

di decadenza dalla patria potestà decretata dal Giudice. In altre parole, devono coinvolgere , per quanto possibile, entrambe le parti onde evitare spiacevoli situazioni che potrebbero facilmente evolvere in contenziosi. Cita la nota ministeriale:

“Solo a titolo meramente esemplificativo, si ritiene opportuno segnalare alcune delle azioni amministrative che le istituzioni scolastiche possono porre in essere per favorire la piena attuazione del principio di bigenitorialità a cui ogni minore figlio di genitori separati ha diritto:

- *inoltro, da parte degli uffici di segreteria delle istituzioni scolastiche di ogni ordine e grado, di tutte le comunicazioni – didattiche, disciplinari e di qualunque altra natura- anche al genitore separato/divorziato/ non convivente, sebbene non collocatario dello studente interessato;*
- *individuazione di modalità alternative al colloquio faccia a faccia, con il docente o dirigente scolastico e/o coordinatore di classe, quando il genitore interessato risieda in altra città o sia impossibilitato a presenziare personalmente;*
- *attribuzione della password, ove la scuola si sia dotata di strumenti informatici di comunicazione scuola/famiglia, per l'accesso al registro elettronico, ed utilizzo di altre forme di informazione veloce ed immediata (sms o email).*
- *richiesta della firma di ambedue i genitori in calce ai principali documenti (in particolare la pagella), qualora non siano in uso tecnologie elettroniche ma ancora moduli cartacei.*

E in ultimo:

Si suggerisce, infine, laddove per la gestione di pratiche amministrative o didattiche concernenti l'alunno risulti impossibile acquisire il consenso scritto di entrambi i genitori, ovvero laddove un genitore sia irreperibile, di inserire nella modulistica la seguente frase:

“Il sottoscritto, consapevole delle conseguenze amministrative e penali per chi rilasci dichiarazioni non corrispondenti a verità, ai sensi del DPR 245/2000, dichiara di aver effettuato la scelta/richiesta in osservanza delle disposizioni sulla responsabilità genitoriale di cui agli artt. 316, 337 ter e 337 quater del codice civile, che richiedono il consenso di entrambi i genitori”.

Alternanza scuola lavoro

Alla privacy nelle attività di alternanza scuola lavoro è dedicata una sezione della nota 28 marzo 2017, n. 3355 del Miur. Al punto 13 che si riporta è specificato: “La Guida Operativa per le Scuole sull'alternanza scuola-lavoro prevede che l'istituzione scolastica e la struttura ospitante alleghino alla Convenzione il Patto formativo dello studente. Tale documento esplicita gli impegni dello studente, prevedendo anche che conosca e rispetti le norme comportamentali in materia di privacy. Qualora lo studente, nell'esercizio delle attività oggetto dell'alternanza scuola lavoro, entri in contatto con soggetti terzi e i loro dati, sarà cura della struttura ospitante garantire che vi sia il corretto trattamento. I dati dello studente in alternanza sono tutelati ai sensi della normativa vigente (cfr. Garante per la tutela dei dati personali). Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, le scuole possono comunicare e diffondere alle aziende private e alle pubbliche amministrazioni i dati personali degli studenti.”

Scuolabus e Mensa scolastica

La gestione dei dati riguardanti la mensa scolastica presenta due diverse problematiche; la prima relativa ad un'eventuale presenza di alunni portatori di intolleranze e/o allergie (dati relativi allo stato di salute): il Garante a tal proposito autorizza il trattamento i dati sensibili degli alunni, indispensabili per la fornitura di pasti nel caso in cui debbano rispondere a particolari richieste delle famiglie legate, ad esempio, a determinati dettami religiosi o a specifiche condizioni di salute. Da un altro punto di vista il Garante afferma che *“non si può pubblicare sul sito della scuola, o inserire in bacheca, il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa; né può essere diffuso l'elenco degli studenti, appartenenti a famiglie con reddito minimo o a fasce deboli, che usufruiscono gratuitamente di tale servizio.”* Per quanto riguarda invece il servizio di scuolabus il Garante prosegue *“Gli istituti scolastici e gli Enti locali non possono pubblicare on line, in forma accessibile a chiunque, gli elenchi dei bambini che usufruiscono dei servizi di scuolabus, indicando tra l'altro le rispettive fermate di salita-discesa o altre informazioni sul servizio.”*

Videosorveglianza

La raccolta, la registrazione e la conservazione di immagini di persone fisiche rappresenta un trattamento lecito se soddisfa i principi cardine del Regolamento tra cui la repressione dei reati nell'ambito delle funzioni istituzionali. È possibile installare un sistema di videosorveglianza negli istituti scolastici quando risulti indispensabile per tutelare l'edificio e i beni scolastici, circoscrivendo le riprese alle sole aree interessate, come ad esempio quelle soggette a furti e atti vandalici.

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. Non si realizza dunque un controllo distanza del lavoratore. Le aree perimetrali esterne, al pari di ogni altro edificio pubblico o privato, possono invece essere oggetto di ripresa, per finalità di sicurezza, anche durante l'orario di apertura dell'istituto scolastico. In questo caso, l'angolo visuale deve essere delimitato in modo da non inquadrare luoghi non strettamente pertinenti l'edificio. La presenza di telecamere deve sempre essere segnalata da appositi cartelli, visibili anche di notte qualora il sistema di videosorveglianza sia attivo in tale orario. In tal caso occorre precisare che Titolare del trattamento è il soggetto che ha installato il sistema (ente locale o la stessa istituzione scolastica) e che tratta i dati direttamente; nel caso in cui i dati vengono trattati tramite la società che gestisce l'impianto questa sarà nominata Responsabile del Trattamento.

In ultimo ricordiamo un aspetto che spesso viene trascurato all'interno delle Istituzioni Scolastiche: il trattamento dei dati di alunni divenuti maggiorenni. Allo scoccare della maggiore età, infatti, l'interessato cessa di essere il genitore o chiunque abbia la tutela del minore e diventa l'alunno stesso. Buona prassi dovrebbe essere che il Titolare fornisca al compimento del 18 anno da parte

dello studente idonea informativa ed eventualmente un'autorizzazione affinché i genitori possano continuare a ricevere le informazioni sulla vita scolastica dello stesso anche se su questo tema esiste una giurisprudenza che continua a coinvolgere i genitori dell'alunno maggiorenne ma non economicamente autonomo nel diritto/dovere sancito dall'art. 30 della Costituzione di mantenere, istruire ed educare i figli.

Antonino Foti

