

# Sommario

<b>CENNI STORICI SU PRIVACY E PROTEZIONE DEI DATI</b>	<b>3</b>
<b>DALLA DIRETTIVA 95/46 AL REGOLAMENTO 2016/679</b>	<b>4</b>
<b>IL REGOLAMENTO EUROPEO: ASPETTI FONDAMENTALI</b>	<b>5</b>
IL GLOSSARIO	5
I PRINCIPI APPLICATI AL TRATTAMENTO DATI	5
LE BASI DI LICEITÀ DEL TRATTAMENTO	6
LE FIGURE DI SISTEMA (TITOLARE, RESPONSABILE, RPD, AUTORIZZATI)	7
I DIRITTI DELL'INTERESSATO	8
L'atto di informazione	8
Il diritto di accesso	8
Il diritto all'oblio	8
I diritti alla limitazione e altri diritti	10
GLI OBBLIGHI GENERALI: PRIVACY BY DESIGN E PRIVACY BY DEFAULT	10
GLI OBBLIGHI SPECIFICI PER IL TITOLARE E IL RESPONSABILE DEL TRATTAMENTO	11
La formazione	11
I registri obbligatori	11
<i>Il registro dei trattamenti</i>	11
<i>Il registro delle violazioni</i>	12
La violazione dei dati - Data Breach	12
La valutazione di impatto privacy (DPIA - Data Protection Impact Assessment)	13
<b>IL DECRETO DI ARMONIZZAZIONE ALLA NORMATIVA EUROPEA D.LGS. 101/2018</b>	<b>15</b>
<b>L'AUTORITÀ GARANTE</b>	<b>17</b>
I POTERI DI INDAGINE	18
I POTERI CORETTIVI	18
I POTERI AUTORIZZATIVI E CONSULTIVI	18
<b>GLI STRUMENTI GIURISDIZIONALI: I MEZZI DI RICORSO</b>	<b>20</b>
IL RECLAMO	20
LA SEGNALAZIONE	20
IL RICORSO GIURISDIZIONALE EFFETTIVO	20
Avverso il garante	21
Avverso il titolare o il responsabile del trattamento	21
<b>LE DOMANDE DI RISARCIMENTO DEL DANNO (ART. 82 REG.)</b>	<b>22</b>
<b>IL QUADRO SANZIONATORIO</b>	<b>23</b>
GLI ILLECITI AMMINISTRATIVI	23
GLI ILLECITI PENALI	26

<b>GLI ASPETTI RIGUARDANTI LE PUBBLICHE AMMINISTRAZIONI: ACCESSO AGLI ATTI</b>	<b>28</b>
<b>I TRATTAMENTI SPECIFICI RIGUARDANDI LE ISTITUZIONI SCOLASTICHE</b>	<b>30</b>
GLI ESITI SCOLASTICI	30
IL REGISTRO ELETTRONICO	30
I DATI BIOMETRICI	30
I TEMI IN CLASSE	30
LE PUBBLICAZIONI DELLE FOTO DEGLI ALUNNI	30
LE COMUNICAZIONI SCUOLA FAMIGLIA	30
LA SITUAZIONE GENITORIALE	30
L'ALTERNANZA SCUOLA-LAVORO	31
GLI SCUOLABUS E LA MENSA SCOLASTICA	31
LA VIDEOSORVEGLIANZA	31

## IL REGOLAMENTO EUROPEO SULLA PROTEZIONE DEI DATI 2016/679 E IL CODICE DELLA PRIVACY 196/2003 NOVELLATO DAL D.LGS. 101/2018

*Pubblichiamo, a valere come contributo professionale, un pregevole lavoro redatto da due colleghi DSGA, nonché Dirigenti Territoriali Anquap (A. Foti e C. Odoardi).*

*Dalla semplice lettura dell'indice (vedi sotto) risulta evidente quanto il lavoro prodotto dai colleghi sia stato impegnativo e corposo.*

*Sull'argomento, l'Anquap è disponibile a svolgere specifiche attività formative (alcune sono già state fatte nello scorso anno scolastico con l'avv. Zampetti, mentre due iniziative si sono tenute lo scorso settembre a Catania ed Enna con il collega Foti).*

### Cenni storici su privacy e protezione dei dati

L'intento di questo contributo è quello di delineare il percorso storico, sociale e poi giuridico che ha portato alla promulgazione dell'attuale Regolamento Comunitario sul trattamento dei dati personali. Con l'ambizione di cercare di trasmettere un seme culturale tra coloro che con i dati ci lavorano tutti i giorni. Sì, perché è proprio questo il cuore della questione. Non di semplici adempimenti formali e/o tecnici si alimenta un sistema Privacy, ma della consapevolezza che la protezione dei dati è un percorso che si costruisce attraverso una conoscenza ed una prassi in cui l'elemento umano è imprescindibile. Oggi più che mai questo Regolamento mette al centro dell'azione di tutela il Titolare (ed il Responsabile) senza

che vi sia più quella rete di protezione definita dal vecchio codice nostrano di "misure minime". Da qui l'approccio non può che essere inevitabilmente di tipo culturale prima ancora che tecnico. Il contributo si divide in due parti secondo l'indice proposto in ragione della complessità della materia.

Il concetto di Privacy appare all'orizzonte giuridico per la prima volta nel 1890 grazie ad una pubblicazione di Samuel Warren e Louis Brandeis giovani avvocati americani che definiscono il "right to be left alone", diritto ad essere lasciato solo, come contrapposizione ad un nascente giornalismo di gossip nella Boston di fine XIX secolo. Definizione che però non varcò l'oceano almeno fino al secondo dopoguerra quando la

Dichiarazione Universale dei Diritti Umani all'articolo 12 sancì il diritto inviolabile di tutti gli uomini alla propria riservatezza come antidoto a ciò che era accaduto con i regimi totalitari e con la loro invasione nella vita privata degli individui. In Italia, invece, si deve aspettare il 1975 per trovare nella giurisprudenza una pronuncia che elevasse a diritto la protezione della vita privata. La Cassazione per la prima volta individuava e descriveva un vero e proprio diritto alla riservatezza che consisteva nella tutela di quelle situazioni e vicende strettamente familiari che ancorché avvenute "al di fuori del proprio domicilio domestico non avevano per i terzi un interesse socialmente apprezzabile". Fin qui la storia.

## *Dalla Direttiva 95/46 al Regolamento 2016/679*

Dopo la promulgazione della Direttiva comunitaria 95/46 che apre la strada alle normative nazionali, in Italia accogliamo nel nostro ordinamento la Legge n. 675/96 con la quale per la prima volta si riconosce, anche in ragione del mutato quadro tecnologico, un diritto alla tutela dei dati. Viene introdotto, cioè, un diritto parallelo alla riservatezza che tutela l'individuo in quanto persona. Il dato personale, strumento e benzina di una nuova economia, deve essere trattato in maniera adeguata. E dalla tutela della riservatezza il concetto di Privacy si sposta sul potere, da parte dell'interessato, ad avere il pieno controllo sulle informazioni che lo riguardano, a prescindere dal fatto che queste informazioni possano ledere in qualche modo la sua riservatezza. Da qui il passo successivo è il D.Lgs. n. 196 del 30 giugno 2003 atto normativo comunque collegato alla Direttiva Comunitaria 95/46. Viene, in buona sostanza, parametrato un nuovo diritto da cui a cascata ne discende un altro. La protezione del dato opera tout court, a monte, ma è indispensabile perché questa si rifletta sulla nostra riservatezza. Un concetto ribadito con forza all'interno della Carta dei Diritti Fondamentali dell'Unione Europea (Carta di Nizza del 2001) che tra i diritti inviolabili della personalità all'art. 8 cita: "1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica." Da segnalare che, come già enunciato all'interno della Direttiva 95/46, il principio di lealtà può considerarsi un refuso da

traduzione che in lingua italiana è diventato principio di correttezza. Inizia da questo momento un nuovo percorso normativo che pone al centro della tutela il dato, come detto, e che crea attorno ad esso una rete di protezione costruita attorno a figure di sistema che ne assumono le responsabilità. E il diritto alla protezione dei dati acquisisce il rango di tutela costituzionale (art. 2 della Costituzione).

L'ultimo passaggio storico è l'approvazione e la promulgazione del Regolamento relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - GDPR (General Data Protection Regulation), esattamente il 25 maggio 2016 che rappresenta uno scatto in avanti del legislatore europeo. Innanzitutto, la scelta regolamentare rappresenta la decisione di uniformare la normativa su tutto il territorio dell'Unione sulla base del principio "One Continent, One law". A onor di verità non sono esenti da questo tipo di intervento normativo le pressioni esercitate dai numerosi soggetti che oggi si nutrono di dati per la propria sopravvivenza e che da una normativa uniformata avrebbero tutto da guadagnare non fosse altro che per l'abbattimento delle spese degli uffici legali che farebbero riferimento ad un unico testo anziché a 27. Perché un regolamento, quindi? I motivi sono diversi. Innanzitutto, la formula giuridica ha il vantaggio dell'immediata applicabilità su tutto il territorio comunitario. In Italia la questione del recepimento era stata risolta da diverse sentenze della Corte Costituzionale che avevano riconosciuto la diretta applicabilità dei regolamenti comunitari (Sentenze 183/1973 e 170/1984) nell'ordinamento italiano, grazie alla copertura fornita dall'art. 11 della Costituzione, che giustifica le limitazioni di sovranità derivanti dall'ade-

sione dell'Italia all'ordinamento delle Comunità Europee (ora dell'Unione Europea). Ciò marca una netta differenza dallo strumento della Direttiva, atto astratto e generale che avrebbe necessitato di una conversione in norma nazionale disperdendo il potere unificante. In secondo luogo vi era la necessità, in ragione del mutato quadro tecnologico, sociale ed economico di sottolineare che la protezione dei dati non è prerogativa assoluta ma un obbligo relazionale ad altri diritti in base ad un principio di proporzionalità (considerando 4). Ed è per questo motivo che la responsabilità del trattamento non poteva essere rinchiusa in una norma statica ma doveva essere esercitata all'interno di una autonoma valutazione del rischio. In conseguenza di ciò, oggi la norma di riferimento in materia di protezione dei dati personali è senza alcun dubbio il GDPR. E lo sarebbe stata comunque anche nel caso in cui il D.Lgs 196 non avesse subito quell'opera di maquillage di cui parleremo più avanti.

Il Regolamento, composto da 167 considerando (premesse) e da 99 articoli, ha fissato una nuova frontiera della protezione dei dati. In un'epoca segnata dalla terza rivoluzione informatica, il web 3.0 meglio conosciuto come IoT (Internet of Things) la necessità era di coniugare la capacità di far circolare i dati, divenuti il nuovo petrolio, fattore economico al pari di materie prime e forza lavoro, garantendo al tempo stesso la massima sicurezza degli stessi. Creare fiducia nel cittadino per consentire una libera circolazione dei dati. Ed il fattore di protezione si sposta dal dato alla procedura, al trattamento. È il trattamento l'oggetto principale di cui il GDPR detta le regole.

La struttura della norma è molto simile al nostro vecchio codice ed ora ci apprestiamo ad analizzarlo.

## Il Regolamento europeo: aspetti fondamentali

### IL GLOSSARIO

Come prassi consolidata ormai da tempo, negli atti legislativi il primo approccio della norma è di tipo nozionistico e ci consegna il glossario delle definizioni che qui riportiamo nei suoi termini salienti:

– *dato personale*: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

– *trattamento*: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

– *profilazione*: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

– *pseudonimizzazione*: il trattamen-

to dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

– *archivio*: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

– *titolare del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

– *responsabile del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il glossario non menziona i Dati Particolari che sono una categoria al quale il Regolamento dedica un intero articolo, il 9. Essi ricomprendono la vecchia definizione di dato sensibile (dato idoneo a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, alla salute o alla vita sessuale o all'orientamento sessuale della persona) a cui vengono aggiunti ed affiancati i dati biometrici e quelli genetici. Per que-

sta particolare categoria di dati è vietata la diffusione, ma ancor prima è vietato il trattamento, a meno che non ricorrano le eccezioni elencate nel secondo paragrafo dell'articolo nelle lettere da a) a j). Per quello che ci riguarda, rientriamo nella lettera g) che ci autorizza a trattare i dati particolari nell'esercizio di un pubblico potere e per motivi di interesse pubblico.

Così pure per gli ex Dati Giudiziari catalogati all'art. 10 come Dati Personali relativi a condanne penali e reati.

Sia per i Dati Particolari che per i Dati Giudiziari è vietata la diffusione e il loro trattamento è legato alle eccezioni previste dal Regolamento.

### I PRINCIPI APPLICATI AL TRATTAMENTO DATI

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'art. 5 del Regolamento UE che di seguito vengono riportati:

1. *Liceità*: il trattamento deve rispettare le norme e non deve violare disposizioni generali o speciali dell'ordinamento;
2. *Correttezza*: il trattamento deve rispettare le norme etiche e deontologiche anche se non codificate;
3. *Trasparenza*: il contenuto dell'informazione deve essere accessibile, comprensibile (linguaggio semplice) e corrispondente alla modalità con cui il trattamento è formulato e veicolato (chiarezza, uso di formati intellegibili, ecc.);
4. *Limitazione della finalità*: lo scopo del trattamento deve essere determinato, esplicito e legittimo: eventuali trattamenti successivi non devono essere incompatibili con le finalità originarie della raccolta dei dati;

5. *Minimizzazione dei dati*: i dati devono essere adeguati, pertinenti e limitati alle finalità del trattamento; tale principio si identifica con il principio di necessità: l'identificabilità dell'interessato deve essere ridotta al minimo;
6. *Esattezza e aggiornamento dei dati*: la cancellazione o la rettifica dei dati che risultino inesatti rispetto alle finalità del trattamento deve essere tempestiva;
7. *Limitazione della conservazione*: è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
8. *Integrità e riservatezza*: occorre garantire la sicurezza (con misure tecniche e organizzative adeguate) per evitare trattamenti non autorizzati o illeciti, perdite, distruzione o danni accidentali. Il dato va protetto perché solo così si proteggono le persone fisiche cui il dato si riferisce.

Il Regolamento UE sempre all'art. 5 paragrafo 2, richiede al Titolare di rispettare tutti questi principi e di essere "in grado di provarlo". Questo è il principio detto di "responsabilizzazione" (o accountability) che viene poi esplicitato ulteriormente dall'art. 24, paragrafo 1, del Regolamento UE, in cui si afferma che "il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento".

L'adeguatezza implica che il Titolare deve sostenere oneri formali e sostanziali sulla base del contesto in cui opera, della natura dei dati trattati, delle finalità e della valutazione dei rischi.

Il Titolare è l'unico soggetto che risponde delle conseguenze dei trattamenti non conformi alle norme perché unico soggetto decisore.

## LE BASI DI LICEITÀ DEL TRATTAMENTO

Le condizioni di liceità del trattamento rappresentano la base giuridica del trattamento dei dati personali, ossia le condizioni che rendono lecito un trattamento. L'art. 6 del Regolamento UE 2016/679 prevede una serie di presupposti di liceità senza distinzione tra Titolari del trattamento, siano essi soggetti pubblici o privati, perché quel che interessa al legislatore europeo è esclusivamente la natura dell'attività che genera il trattamento dei dati, non la condizione pubblica o privata del Titolare. Prima di ogni trattamento di dati personali è indispensabile individuare su quale fondamento giuridico il Titolare tratta il dato. È possibile individuare due macro categorie:

1) la prima categoria di condizioni si basa sul consenso dell'interessato e evidenzia una struttura "contrattuale" costituita dall'incontro di due volontà. Il che fa pensare alla dimensione di "proprietà" dei dati personali e, appunto, riguarda esclusivamente il settore privato concernendo:

- il consenso per una o più specifiche finalità ed espresso in modo libero. Con esso l'interessato manifesta l'intenzione inequivocabile e specifica di accettare il trattamento dei dati che lo riguardano. Non è ammesso il consenso tacito o presunto; tuttavia il consenso non necessariamente deve essere documentato per iscritto né è richiesta la forma scritta. Piuttosto, graverà sul Titolare del trattamento l'onere della prova della sua acquisizione;
- l'esecuzione di un'obbligazione contrattuale o precontrattuale. In questo caso, il consenso al trattamento è considerato implicito nel rapporto contrattuale nei limiti delle prestazioni dedotte nel contratto;

2) la seconda categoria prescinde dal

consenso ed ha come fondamento una previsione normativa, cioè un obbligo di legge e può riguardare Titolari pubblici o privati. Essa fa riferimento alle seguenti situazioni giuridiche:

- obbligo di legge: ciò si verifica quando un Titolare privato è per legge, nazionale o comunitaria, obbligato a raccogliere e trattare dati sulla base di una previsione normativa al fine di tutelare un interesse pubblico;
- salvaguardia di interessi vitali di una persona fisica: ciò accade nei casi in cui la priorità è costituita dalla protezione di un bene supremo quale la vita dell'interessato o di un'altra persona fisica (ad esempio nelle situazioni di rischio per l'incolumità fisica o la salute);
- esecuzione di compiti di interesse pubblico o connesso all'esercizio di pubblici poteri: in questo caso, il trattamento è svolto da soggetti pubblici, il cui interesse è per definizione "prevalente" su quello individuale, sicché l'interessato, se un potere pubblico tratta i dati della sua vita, può solo esercitare un diritto di opposizione;
- legittimo interesse del titolare o di terzi: in questo caso, il trattamento può avvenire legittimamente se risulta necessario al perseguimento di determinate finalità, che però non devono mettere a rischio la salvaguardia della sfera giuridica fondamentale degli individui; nella fattispecie, il titolare ha il compito di effettuare il bilanciamento tra tutti gli interessi (soprattutto se vengono trattati dati di un minore).

Per le Istituzioni Scolastiche è da sottolineare che l'unico fondamento giuridico della liceità del trattamento è quello della lettera e) del paragrafo 2 dell'art. 6, cioè l'esecuzione di compiti di interesse pubblico o connesso all'esercizio di pubblici poteri. In ragione di ciò, le Istituzioni

Scolastiche, e più in generale tutte le Pubbliche Amministrazioni, non devono chiedere mai il consenso ma trattano dati in forza di una norma di legge o regolamentare. In assenza di queste condizioni, il dato non può essere trattato.

Per il trattamento dei dati particolari, la liceità è invece garantita solo se ricorrono le condizioni di cui al paragrafo 2 dell'art. 9 del Regolamento 2016/679/UE.

### **LE FIGURE DI SISTEMA (TITOLARE, RESPONSABILE, RPD, AUTORIZZATI)**

La figura del Titolare è il *deus ex machina* del Trattamento dei Dati; attorno a lui ruotano tutte le azioni di protezione, trattamento, organizzazione dell'intero sistema di sicurezza dei dati. È il responsabile quasi unico di ogni operazione e ne risponde in caso di contenzioso. Nella Pubblica Amministrazione si identifica nell'Amministrazione stessa, quindi il Titolare del Trattamento dati di un'Istituzione Scolastica è l'Istituzione rappresentata organicamente dal suo Dirigente Scolastico. Cosa cambia? Molto! In caso di contenzioso amministrativo, infatti, è l'Amministrazione che va in giudizio e non la persona fisica. Accanto al Titolare, il legislatore europeo ha disegnato una figura, per certi versi nuova, che non pochi problemi interpretativi sta creando specialmente in ambito scolastico: il Responsabile del Trattamento dati. La presenza di una figura simile all'interno del codice nazionale (al medesimo articolo, tra l'altro, il 28) ha creato una sorta di ambigua traslazione sul nuovo profilo. Come invece affermato da illustri giuristi (cfr Prof. Pizzetti – 6° Privacy Day 2016) ci troviamo di fronte alla correzione di un errore giuridico che aveva commesso il nostro legislatore all'interno del D.Lgs. 196. Tale soggetto, infatti, non trovava riscontro all'interno della Direttiva 95/46, che già allora aveva descritto un profilo

diverso da quello che poi aveva visto la luce all'interno del codice (soggetto facoltativo, che agiva su incarico etc.). Il Responsabile tratteggiato nel GDPR corrisponde senza ombra di dubbio ad un soggetto esterno all'organizzazione (Istituzione Scolastica) che tratta dati per conto del Titolare sulla base di un contratto di servizi. L'incipit dell'art. 28 è sintomatico per svelare l'arcano: "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate..." Sono due le cose da sottolineare e che sembrano marcare le caratteristiche del profilo; il qualora ed il per conto che escludono a priori che possa essere un qualsivoglia dipendente interno a svolgere questa mansione. Un dipendente, infatti, tratta dati per dovere d'ufficio e sulla base di un rapporto gerarchico. In aggiunta a ciò, la lettura coordinata degli artt. 28, 30 e 32 ci fa concludere che il Titolare ed il Responsabile del trattamento dati non possono essere che soggetti autonomi e indipendenti, dovendo soggiacere ai medesimi oneri (tenuta del registro dei trattamenti, nomina del DPO etc.) cosa che, qualora fosse erroneamente imputata ad un soggetto interno, porterebbe ad una confusione burocratica. Da non sottovalutare, infine, la responsabilità in solido che investe i due soggetti in caso di patologie del trattamento. Quindi, per sintetizzare: chi sono questi Responsabili del Trattamento dati? La risposta sta nell'evoluzione tecnologica dell'ultimo decennio quando è nato il cloud computing ovvero la possibilità di servirsi di risorse software ed hardware in remoto, delocalizzando anche le banche dati. E di conseguenza, con l'introduzione di un soggetto che si assume la responsabilità di trattare dei dati

per conto di un titolare al quale è legato da un contratto di servizi. Nelle Istituzioni Scolastiche possiamo facilmente individuare queste figure nelle software house che forniscono i gestionali, nelle Imprese assicuratrici, negli Istituti Cassieri etc.

Figura assolutamente nuova per la nostra legislazione (ma non per il resto d'Europa) è invece il Responsabile della Protezione dei Dati (in inglese abbreviato DPO), il quale rappresenta una sorta di figura di garanzia per l'intero sistema. Obbligatorio per ogni Pubblica Amministrazione nel Regolamento, è delineato attraverso i compiti per i quali viene individuato; in particolare il DPO deve:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del

caso, consultazioni relativamente a qualunque altra questione.

Come si evince dai compiti assegnati, il DPO è un consulente che coadiuva, ove richiesto, e controlla il sistema di protezione dati senza alcuna responsabilità diretta riguardo le patologie del trattamento dati. La responsabilità in ogni caso e come già affermato, resta in capo al Titolare e/o al Responsabile del trattamento dati.

Scivolata via tra le righe del Regolamento è invece la vecchia figura dell'incaricato al trattamento dati. Una superficiale lettura non lo individuerebbe. Ma leggendo con attenzione l'art. 29 ritorna a galla sotto la definizione di "persona autorizzata al trattamento dati" che ci riporta immediatamente alla responsabilità del Titolare nell'individuare, formare ed istruire adeguatamente tutti coloro che avranno a che fare con il trattamento dei dati. Per inciso, e a scanso di equivoci, si elencano non esaustivamente i soggetti che in una Istituzione Scolastica trattano dati:

1. Docenti
2. Direttore s.g.a.
3. Assistenti Amministrativi
4. Collaboratori Scolastici
5. Revisori dei Conti
6. Rappresentanti negli organi collegiali (genitori ed alunni)
7. Fornitori
8. Esperti Esterni

## **I DIRITTI DELL'INTERESSATO**

### **L'atto di informazione**

L'interessato, ovvero il proprietario dei dati, ha il diritto di ottenere le informazioni che riguardano il trattamento dei propri dati. Gli articoli 13 e 14 si occupano di ciò a seconda che i dati siano raccolti presso l'interessato o meno. L'elenco tassativo delle informazioni da fornire deve essere contenuto in apposito documento da rilasciare all'interessato (anche previa indicazione del link al sito web dove è pubblicato) e che qui

riassumiamo:

- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del responsabile della protezione dei dati, ove applicabile;
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

Al paragrafo 2:

- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano, o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsia-

si momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

- d) il diritto di proporre reclamo a un'autorità di controllo;
- e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Inoltre, qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2.

### **Il diritto di accesso**

L'interessato, inoltre, conserva il diritto di accesso ai propri dati (art. 15) per avere conoscenze dei trattamenti avvenuti e verso chi, i suoi dati sono o possono essere trasferiti. L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo (art. 16).

### **Il diritto all'oblio**

L'istituto del diritto all'oblio presenta un significato differente da quello accolto nel Regolamento UE 2016/679 sulla protezione e sul trattamento dei dati personali.

Il diritto all'oblio può essere definito come la pretesa di un soggetto di ottenere la rimozione di informa-

zioni personali che lo riguardano, dalla circolazione pubblica nel caso in cui il loro rilievo, in termini di interesse del pubblico, sia ridotto in funzione del tempo trascorso o per altre ragioni. Il metro di valutazione deve essere non puramente cronologico ma logico-funzionale, cioè occorre tenere conto di molteplici fattori come la tassatività, la gravità della notizia, il peso sociale degli eventi, il ruolo e la posizione pubblica dell'interessato.

Immediatamente il diritto all'oblio viene definito come il processo di deindicizzazione totale o parziale dei risultati di un motore di ricerca. Quando tra le prime pagine del risultato appaiono notizie attinenti ad un soggetto, persona fisica superate o inesatte, non aggiornate, decontestualizzate e non anonimizzate se dovuto, ci troviamo di fronte ad una lesione del diritto all'oblio con conseguente danno alla reputazione.

In un'altra definizione di origine giurisprudenziale il diritto all'oblio (CGUE del 13/05/2014 Costeja-Google) si collega al ruolo che assume un soggetto come "figura pubblica", quando l'informazione su tale persona fisica sia "divenuta ormai non più di interesse apprezzabile per la collettività". In tal caso il diritto all'oblio prevale sul diritto della collettività di accedere alla notizia ripescata. I parametri per definire un'informazione non più rilevante per il pubblico sono i seguenti:

- la notizia non contribuisce al dibattito di interesse pubblico;
- la notizia non attiene a ragioni di giustizia, di polizia, a scopi scientifici, didattici e culturali;
- la notizia non attiene ad un soggetto con un grado di notorietà tale da essere definita appunto "figura pubblica";
- la notizia non deve risultare di "interesse apprezzabile per la collettività" (CGUE del 9/03/2017 Manni); è ad esempio il caso del

mantenimento di una informazione nei registri pubblici per tutelare gli interessi dei terzi e garantire la certezza del diritto, la lealtà delle transazioni commerciali e, quindi il buon funzionamento del mercato interno (ragioni di pubblicità legale).

Per altro, in relazione al diritto di cronaca, il diritto all'oblio può essere sacrificato, a seguito di un'adeguata operazione di bilanciamento, in presenza dei seguenti parametri aggiuntivi rispetto a quelli sopra indicati:

- la notizia deve essere veritiera, di attualità e contingente;
- il diritto di replica deve essere concesso prima della diffusione della notizia.

In relazione alla satira, il diritto all'oblio può essere esercitato (Cass. 21235/12 e Cass. 28411/08) solo se la satira non si riduce ad una lesione gratuita e ingiustificata della reputazione di una persona ma è collegata ad una manifestazione di dissenso ragionato nell'ambito di una denuncia sociale o politica logicamente argomentata.

Nell'art. 17 del Regolamento UE, la nozione di diritto all'oblio è riferita espressamente alla cancellazione dei dati personali senza che la norma abbia formalizzato gli schemi di ragionamento maturati dal pensiero giuridico nonostante il titolo dell'articolo che si rubrica "Diritto alla cancellazione (diritto all'oblio)".

L'art. 17 riproduce testualmente con qualche precisazione e puntualizzazione il consolidato diritto alla cancellazione disciplinato nell'abrogata direttiva 95/46. La sovrapposizione dei termini "cancellazione" e "oblio" del titolo è impropria, in quanto trattasi di due istituti giuridici distinti. Precisamente, la cancellazione si pone in un rapporto di conseguenza rispetto alla pretesa di oblio. Il comma 1 recita: "L'interessato ha diritto di ottenere dal titolare del trattamento la cancellazione dei dati

personali che lo riguardano senza giustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: ..." Sicché la pretesa alla cancellazione è prefigurata come una conseguenza di determinate situazioni che determinano l'obbligo per il titolare di procedere alla suddetta cancellazione. L'esercizio del diritto alla cancellazione non si concretizza dunque con la semplice richiesta, ma solo alla verifica dei presupposti elencati al comma 1 da cui deriva l'obbligo del titolare. I motivi di cui sopra, che sono presupposti alla cancellazione, sono i seguenti:

- a) esaurimento della finalità del trattamento dei dati: i dati non sono più necessari rispetto alle finalità per cui sono stati raccolti;
- b) revoca del consenso: l'assenza di una base giuridica, già di per sé, obbliga il titolare a cancellare i dati;
- c) opposizione riuscita: l'interessato si oppone al trattamento dei dati e quindi non sussiste alcun motivo legittimo per procedere con il trattamento. Si esercita qui l'azione congiunta di due diritti: il diritto di opposizione e quello di oblio;
- d) illiceità del trattamento: il principio della liceità sancito dall'art. 5, se non rispettato, consente all'interessato, con la cancellazione, il ripristino della liceità, salvo la possibilità di esperire un'azione civile per il risarcimento del danno;
- e) obbligo di legge: vi è un obbligo legale previsto dal diritto UE o dalla normativa nazionale che prevale sugli interessi del titolare;
- f) illiceità del trattamento per offerta a minore sotto i sedici anni: il diritto alla cancellazione sussiste anche se l'interessato non è attualmente minore ma lo era quando aveva prestato il consenso per cui non era pienamente consapevole dei rischi derivanti dal trattamento.

La norma UE individua però anche le eccezioni relativamente alle quali il diritto all'oblio non può essere esercitato. Queste sono rappresentate dai seguenti casi di deroga:

- se il trattamento è effettuato per l'esercizio del diritto alla libertà di espressione e di informazione;
- se il trattamento è effettuato per l'adempimento di un obbligo di legge;
- se il trattamento riguarda un interesse pubblico nel settore della sanità;
- se il trattamento obbedisce a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- se il trattamento è effettuato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria (ad esempio un responsabile non ha diritto alla cancellazione delle prove della sua colpevolezza).

Agli Stati membri è demandata l'introduzione di ulteriori deroghe laddove è necessario il bilanciamento con la libertà di espressione e di informazione di cui all'art. 85 del Regolamento nel rispetto, in ogni caso, delle garanzie previste a tutela degli interessati.

Da quanto sopra esposto si evince che il diritto all'oblio coesiste ma non si identifica con gli altri diritti quali la limitazione del trattamento (perché prevede comunque la conservazione), l'opposizione al trattamento (perché non determina la cancellazione), la portabilità dei dati (perché si muovono su spazi diversi).

Deve inoltre ritenersi che il diritto all'oblio assume rilievo di rango costituzionale in quanto declinazione del diritto alla protezione dei dati personali alla stessa stregua degli altri diritti dell'interessato indicati nel Capo III del Regolamento: rispetto della vita privata e familiare, del domicilio e delle comunicazioni, libertà di pensiero, di coscienza e di

religione, libertà di espressione e d'informazione, libertà di impresa, diritto ad un ricorso effettivo e a un giudice imparziale, diversità culturali, religiosa e linguistica.

In definitiva la mancata tipizzazione del diritto all'oblio nel Regolamento, alla luce delle pronunce giurisprudenziali, ha rappresentato un'occasione perduta di definizione di parametri per procedere al bilanciamento degli interessi e dei diritti costituzionali in gioco.

### ***I diritti alla limitazione e altri diritti***

L'interessato ha il diritto ad ottenere la limitazione del trattamento quando ricorrano le seguenti condizioni:

- a) l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
- d) l'interessato si è opposto al trattamento ai sensi dell'articolo 21, paragrafo 1, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

L'art. 19 impone infine al Titolare del trattamento la notifica ai destinatari dei dati personali trasmessi di eventuali correzioni, integrazioni, cancellazioni operate ai sensi degli articoli 16, 17 e 18.

Gli articoli da 20 a 22 riguardano casistiche ricadenti in ambito privato (e su questi non ci soffermiamo).

### ***GLI OBBLIGHI GENERALI: PRIVACY BY DESIGN E PRIVACY BY DEFAULT***

Con gli articoli 24 e 25 ci troviamo nel cuore del Regolamento Europeo sulla protezione dei dati personali. Il Primo sancisce la responsabilità posta in capo al Titolare del trattamento senza che questa possa essere tralasciata su altri soggetti per atto organizzativo o via amministrativa; vale a dire che non esiste altro soggetto a cui può essere delegata una qualsiasi forma di responsabilità. L'articolo, inoltre, amplia e traduce il concetto di "accountability" riguardo al trattamento dei dati. "Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento". Ciò significa che finisce l'era delle misure minime dettagliate da una norma (nel nostro caso era l'allegato B del codice nazionale) per entrare in un territorio dove la valutazione del rischio diventa la regola. "Deve essere in grado di dimostrare..." vuol dire che non basta correre ai ripari nell'imminenza di una ispezione, ma occorre documentare di aver proceduto per tempo alla realizzazione di un adeguato sistema di protezione dei dati.

L'articolo 25 è forse l'articolo più importante, quello che rappresenta meglio lo spirito della norma e raffigura i due profili di responsabilizzazione del Titolare. Privacy by design significa protezione dei dati sin dalla progettazione del processo di trattamento. Il primo paragrafo dell'art. 25 coinvolge direttamente il Titolare nella scelta delle misure sia tecniche (software e strumenti) che organizzative (disposizioni di accesso limitato a determinate aree, pseudonimizzazione, minimizzazione etc.) tenendo conto sia dello stato dell'organizzazione che delle risorse (anche economiche) necessarie, in rapporto ad una valutazione di impatto che lo stesso

deve fare. In altre parole, il Titolare ha la responsabilità di progettare i trattamenti fin dall'origine approntando le misure adeguate alla protezione dei dati. In questo, la sua valutazione e la scelta devono riguardare, per esempio, anche le risorse tecnologiche (software, hardware) che ove carenti in tema di privacy by design dovranno essere integrate da misure organizzative, così da costruire un'originale combinazione che possa contemperare sia le esigenze normative che la sostenibilità in termini economici del sistema di protezione.

Il concetto di privacy by default significa invece che la protezione del dato deve diventare l'impostazione predefinita. Il sistema di protezione dei dati deve essere organizzato in modo da dover trattare esclusivamente i dati necessari. Ad esempio, con l'impostazione predefinita si deve forzare il sistema per inserire ulteriori dati; si deve forzare il sistema per conservare per un periodo eccedente quello preimpostato; non deve consentirsi l'accesso ai dati ad un numero indefinito di persone senza la presenza della persona fisica, individuata dal Titolare, autorizzata al trattamento.

### **GLI OBBLIGHI SPECIFICI PER IL TITOLARE E IL RESPONSABILE DEL TRATTAMENTO**

#### **La formazione**

Il Titolare del trattamento ai sensi dell'art. 29 del Regolamento UE è obbligato ad istruire il Responsabile del trattamento e il soggetto che ha accesso ai dati. Si tratta di un obbligo rivolto agli autorizzati al trattamento che si sostanzia in un ordine di servizio nel quale vengono fornite le necessarie informazioni tecniche per il trattamento dei dati. L'ottemperanza a questo obbligo, unitamente alla predisposizione di un piano di formazione per il personale dipendente che faccia com-

prendere la cultura e i principi cardine dei diritti fondamentali della persona, tra cui la protezione dei dati, rappresenta un importante tassello nella dimostrazione di aver messo in atto le c.d. misure di sicurezza organizzative adeguate, nel rispetto del principio di responsabilizzazione. Infatti l'art. 32, paragrafo 1, del Regolamento UE, dice testualmente: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" e poi successivamente il paragrafo 4 "Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento". In ragione di ciò, incrementare la consapevolezza del fattore rischio, mediante la conoscenza della normativa, rappresenta un'opportunità da condividere con il Responsabile della Protezione Dati il quale è tenuto a "informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati" ai sensi dell'art. 39, paragrafo 1 lett. a) del Regolamento UE. Sicché il Titolare e il Responsabile della Protezione Dati avranno un ruolo decisivo nella diffusione della cultura privacy all'interno dell'organizzazione attraverso la formazione che realizzeran-

no per tutti i soggetti coinvolti nel trattamento.

#### **I registri obbligatori**

Nel Regolamento UE gli unici obblighi di tenuta della documentazione si sostanziano nella tenuta dei seguenti registri:

1. IL REGISTRO DEI TRATTAMENTI previsto dall'art. 30.

2. IL REGISTRO DELLE VIOLAZIONI DEI DATI previsto dall'art. 33.

#### *Il registro dei trattamenti*

Il Titolare, sotto la propria responsabilità, è obbligato alla tenuta del Registro dei trattamenti, salvo i casi previsti dal paragrafo 5 dell'art. 30. Tale Registro rappresenta un utile strumento operativo ex ante in quanto il Titolare censisce tutti i trattamenti e il loro ciclo di gestione. Rappresenta altresì uno documento probatorio ex post degli adempimenti messi in atto, indispensabile per dimostrare la conformità del trattamento ai principi del Regolamento UE in caso di controllo da parte del Garante. L'obbligo della tenuta del Registro vale anche per il Responsabile del Trattamento in ordine ai trattamenti effettuati per conto del Titolare. Il contenuto del Registro dei trattamenti, tenuto dal Titolare, è così stabilito nel paragrafo 1:

- a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- b) le finalità del trattamento;
- c) una descrizione delle categorie di interessati e delle categorie di dati personali;
- d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- e) ove applicabile, i trasferimenti di

dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;

- f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32.

Mentre per il Responsabile del trattamento in luogo dei punti b) c) e d) è previsto che il Registro (denominato anche Registro delle categorie delle attività riferito al Responsabile) contenga:

- a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
- b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32.

Nei predetti testi l'“ove possibile” si riferisce a contenuti residuali che impongono tuttavia al Titolare, o al Responsabile, di dimostrare le ragioni per cui è impossibile descrivere quanto richiesto.

Il contenuto del Registro, che deve essere tenuto in forma scritta anche in modalità elettronica, può tuttavia prevedere ulteriori informazioni ritenute opportune nell'ottica di una

gestione complessiva del rischio e della valutazione di impatto.

La deroga all'obbligo della tenuta del Registro è contenuta nel paragrafo 5 dell'art. 30 e riguarda i casi in cui l'organizzazione del Titolare abbia meno di 250 dipendenti. Tale deroga non si applica tuttavia nei casi in cui il trattamento presenti un rischio per i diritti e le libertà degli interessati, non sia occasionale e non includa un trattamento di dati particolari o giudiziari. In sostanza significa che, ancorché un trattamento si presenti come occasionale, se concerne dati particolari o giudiziari, deve essere sempre riportato obbligatoriamente in un Registro dei trattamenti. Il Garante raccomanda comunque la tenuta di siffatto registro, anche per i Titolari che non sono obbligati, in quanto rappresenta un adempimento inserito in un quadro di una corretta gestione del trattamento dei dati.

Il MIUR con la comunicazione prot. n. 877 del 3 agosto 2018 ha fornito alle scuole uno schema di Registro delle attività di trattamento unitamente ad una guida per la compilazione. In tale Registro vengono evidenziate le seguenti informazioni: le attività di trattamento; la descrizione dell'attività di trattamento; la modalità di trattamento; la finalità; la tipologia di trattamento; la base giuridica del trattamento; l'informativa; la categoria di interessati; le categorie di dati trattati (dati comuni, categorie particolari di dati personali, dati personali relativi a condanne penali); i termini di cancellazione; i destinatari esterni dei dati; i trasferimenti all'estero; i paesi extra-UE o organizzazioni internazionali verso i quali vengono trasferiti i dati; le misure di sicurezza di cui all' art. 32; il contitolare del trattamento; il Responsabile esterno del trattamento.

È da ritenere utile nella gestione

dell'adeguamento alle norme privacy considerare il Registro dei trattamenti come punto di partenza.

### *Il registro delle violazioni*

Al solo Titolare del trattamento è fatto obbligo della tenuta di un Registro, ai sensi del paragrafo 4 dell'art. 33 del Regolamento UE che documenta qualsiasi violazione dei dati personali, le circostanze che le hanno originate, le conseguenze e i rimedi adottati per la rimozione. Attraverso tale registro, il Garante potrà verificare il rispetto delle norme. Il Registro costituisce onere della prova della capacità del Titolare di provvedere alla gestione dei rischi.

Tali registri vanno continuamente aggiornati e, naturalmente, vanno coordinati con gli altri adempimenti documentali, come le informazioni da rilasciare all'interessato (ex informativa), le autorizzazioni al trattamento, nonché le analisi sulla valutazione di impatto.

### **La violazione dei dati - Data Breach**

La violazione dei dati personali definita dall'art. 2, punto 12, del Regolamento UE, si sostanzia nella violazione della sicurezza del sistema di protezione. L'incidente, che comporta casualmente o illecitamente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, può avvenire in vari modi: per furto, per infedeltà aziendale, per perdita accidentale, per accesso abusivo da parte di terzi. In pratica, i dati personali degli interessati, gestiti dal Titolare, vengono in possesso di soggetti non autorizzati al trattamento. In proposito, il Titolare, oltre a documentare nel Registro delle violazioni i fatti avvenuti, è tenuto a notificare al Garante, senza ingiustificato ritardo e comunque entro le 72 ore dal momento in cui ne è venuto a conoscenza, salvo docu-

mentare le ragioni del ritardo, i casi probabili di violazione dei dati personali che presentano un rischio per i diritti e le libertà delle persone fisiche. Nel caso in cui è certo che la violazione comporti un elevato rischio per i diritti individuali e le libertà allora la comunicazione del data breach va effettuata anche nei confronti dell'interessato. L'evento della violazione dei dati va gestito e affrontato immediatamente senza indugio per evitare l'insorgenza o l'aggravamento di eventuali danni alla persona, come ad esempio il furto di identità, la perdita di riservatezza dei dati coperti da segreto professionale, la decifrazione non autorizzata della pseudonimizzazione o altre perdite di natura economica o sociale significative per la persona.

La notifica al Garante quindi è subordinata alla valutazione del probabile rischio per gli interessati e, se questo è elevato, occorrerà informare quest'ultimi sempre senza indugio, su ordine del Garante medesimo, ai sensi del paragrafo 4 dell'art. 34.

Il contenuto della notifica al Garante è riportato nel paragrafo 3 dell'art. 33:

- a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- c) descrivere le probabili conseguenze della violazione dei dati personali;
- d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamen-

to per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Invece, il contenuto della notifica agli interessati, che deve essere esposta in forma scritta con un linguaggio immediatamente comprensibile, deve contenere almeno i punti b), c) e d) della notifica di cui sopra. È possibile non procedere alla notifica agli interessati nel caso il Titolare abbia adottato misure tecniche e organizzative in modo adeguato, quali ad esempio la cifratura, oppure nel caso in cui dimostri di aver adottato successivamente le misure atte a scongiurare il rischio elevato e, infine, nel caso in cui la comunicazione richieda uno sforzo talmente sproporzionato a causa dell'elevato numero degli interessati. In quest'ultimo caso la comunicazione va resa in forma pubblica.

Da sottolineare che il Garante potrà sempre autonomamente valutare se richiedere al Titolare la notifica agli interessati dopo aver valutato la probabilità del rischio della violazione come sopra indicato ai sensi del paragrafo 4 dell'art. 34.

La previsione della comunicazione agli interessati di un data breach, solo in casi certi e a fronte di elevati pericoli, è stata voluta dal legislatore europeo per evitare all'organizzazione un danno reputazionale e perdite economiche anche in termini di diminuzione di credibilità nei casi in cui il rischio della violazione era solo probabile e incerto.

#### ***La valutazione di impatto privacy (DPIA - Data Protection Impact Assessment)***

L'oggetto della normativa privacy non è il dato in se stesso, bensì il trattamento con il quale il dato entra a far parte del ciclo di gestio-

ne di un processo produttivo con finalità private o pubbliche. Sicché, prima di considerare gli interessati, è necessario procedere ad una analisi preliminare, ad una valutazione ex ante di ciò che potrebbe accadere nel caso di un'eventuale violazione delle misure di protezione poste a garanzia dei proprietari dei dati personali, particolari o giudiziari.

Quindi, in sostanza, prima del trattamento, anche e soprattutto quando si utilizzino nuove tecnologie, considerando la natura, l'oggetto, il contesto e le finalità proprie del trattamento, se c'è un rischio elevato per i diritti e le libertà, si deve procedere ad una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati. Per trattamenti simili con rischi elevati analoghi è possibile effettuare una singola valutazione.

In questa importante attività di valutazione, il Titolare si deve consultare con il Responsabile della Protezione dei Dati.

I casi in cui la VIP è necessaria sono quelli riportati nel paragrafo 3 dell'art. 35 del Regolamento UE e sono i seguenti:

- a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

In aggiunta a ciò, il Garante dovrà individuare un elenco di tipologie

di trattamenti soggetti all'obbligo della VIP e un altro elenco dei trattamenti sottratti all'obbligo.

La valutazione deve necessariamente contenere, ai sensi del paragrafo 7 dell'art. 35:

- a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
- c) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i mecca-

nismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Le Istituzioni Scolastiche non trattano dati particolari in larga scala (la definizione di *larga scala* si trova nel Considerando 91 "i trattamenti su larga scala [...] mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze

tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti"). Sicché non vi è obbligo di redigere la VIP. Tuttavia, la predisposizione di questa misura risponde alla logica del principio di responsabilizzazione e soddisfa pienamente l'adeguamento a tutto il sistema della privacy. La conoscenza delle misure, delle garanzie e dei procedimenti per eliminare o attenuare i rischi permette di conformare il trattamento dei dati agli standard normativi europei e nazionali.

## *Il Decreto di armonizzazione alla normativa europea D.Lgs. 101/2018*

Il Decreto Legislativo n. 101 del 10 agosto 2018 ha visto la luce con la sua pubblicazione sulla Gazzetta Ufficiale del 4 settembre 2018 con oltre tre mesi di ritardo rispetto alla scadenza fissata dalla Legge Delega n. 163 del 25 ottobre 2017. Ad onor del vero tale scadenza è scivolata al 21 agosto successivo in forza di un meccanismo legislativo (legge Moavero del 2012) che, in caso di mutamento delle maggioranze parlamentari a seguito di elezioni (cosa effettivamente accaduta), impedisce al governo uscente di operare una forzatura sulle nuove camere e, quindi, prevede una proroga automatica di 90 giorni del limite per adempiere alle prescrizioni della delega.

Il Decreto si compone di 27 articoli che operano fondamentalmente una sorta di maquillage tecnico rispetto al quale, anche in ragione del tempo trascorso per la sua gestazione, non si può che rimanere sconcertati. Del nostro 196 rimangono in piedi 81 articoli a cui il legislatore nazionale ne aggiunge 16 da 2-bis a 2-septiesdecies e ulteriori 10 sparsi per tutto il restante testo.

Come si diceva, una sorta di rivisitazione terminologica del codice adeguata alla nuova nomenclatura del regolamento.

Nel dettaglio, per quel che riguarda le Istituzioni Scolastiche, oltre all'abrogazione dell'art. 95 che definiva l'interesse pubblico delle operazioni di trattamento dei dati da parte delle scuole (disposizione attratta negli articoli 2-ter e 2-sexies) vi è l'adeguamento dell'art. 96 riguardante la possibilità di comunicare, su richiesta dell'interessato, i dati relativi agli esiti scolastici [...] al fine di age-

volare l'orientamento, la formazione e l'inserimento professionale [...]. Il novellato coinvolge in questa modalità di trattamento dei dati degli studenti "le istituzioni del sistema nazionale di istruzione, i centri formazione professionale regionale, le scuole private non paritarie, nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute" con un ampliamento del campo di applicazione prima non previsto.

Per il resto il legislatore utilizza la tecnica del rinvio a futuri decreti ministeriali e linee guida da parte del Garante (ben 11 rinvii); fa salve tutte le precedenti decisioni del Garante (art. 20) nell'attesa di nuove linee guida e codici deontologici; prevede la definizione agevolata delle controversie nate da violazione in materia di protezione dei dati: l'art. 18, infatti, stabilisce che "[...] per i procedimenti sanzionatori riguardanti le violazioni di cui agli articoli 161, 162, 162-bis, 162-ter, 163, 164, 164-bis, comma 2, [...] e le violazioni delle misure di cui all'articolo 33 e 162, comma 2-bis, del medesimo Codice, che, alla data di applicazione del Regolamento, risultino non ancora definiti con l'adozione dell'ordinanza-ingiunzione, è ammesso il pagamento in misura ridotta di una somma pari a due quinti del minimo edittale".

All'art. 2-septies comma 7 si segnala l'apertura del legislatore circa l'utilizzo dei dati biometrici con riguardo alle procedure di accesso fisico ai dati. Resta comunque una disposizione condizionata dall'emanazione da parte del Garante delle misure di garanzia previste nello stesso articolo al comma 1.

All'art. 2-quaterdecies troviamo una disposizione di carattere organizzativo che consente al Titolare e/o al Responsabile del Trattamento di nominare sotto la propria responsabilità una o più figure organizzative dedicate a compiti specifici connessi al trattamento dati. È una ovvietà che all'interno di un'organizzazione si possano prevedere figure intermedie rispetto al vertice per la gestione dei sistemi. Anche nelle Istituzioni Scolastiche, ad esempio, potremmo trovare un supervisore al trattamento dati che si occupa del sistema di protezione per una determinata area di trattamento.

Di rilievo l'art. 140-bis che sancisce l'alternatività delle forme di tutela. In sostanza, il ricorso all'Autorità Garante è alternativo al ricorso al Giudice Ordinario.

Il legislatore nazionale, inoltre, ha scelto di non intervenire sulle sanzioni amministrative, lasciando a scienza e coscienza del Garante o del Giudice Ordinario, la graduazione delle sanzioni pecuniarie, sulla base dei parametri fissati dall'art. 83 del Regolamento.

Un aspetto inquietante di questa norma è contenuto nell'art. 2-quinquies dove il legislatore si occupa del consenso dei minori per il trattamento dei dati in relazione all'offerta di servizi della società dell'informazione. Una disposizione che scavalca il GDPR che già aveva disposto una barriera al di sotto della maggiore età (16 anni). In Italia sarà possibile chiedere il consenso per il trattamento evidenziato a minori che avranno compiuto i 14 anni. Per la funzione sociale ed educativa della Scuola questa deve essere una sfida contro gli abusi che potranno nascere su questo versante.

In ultimo, una curiosità: nel Regolamento, il Considerando 27 stabilisce che le norme sulla protezione dei dati non si applicano alle persone decedute. Al tempo stesso rilascia agli Stati membri la facoltà di prevedere all'interno della legislazione nazionale norme di tutela dei dati di questi soggetti. Il legislatore italiano ha prov-

veduto a ciò con l'art. 2-terdecies con il quale vengono individuati i soggetti che possono esercitare la tutela dei diritti di cui agli articoli da 15 a 22 del GDPR per le persone decedute.

Sinteticamente sono:

- coloro che hanno un interesse proprio;
- coloro che agiscono a tutela

dell'interessato come mandatario;

- coloro che per ragioni familiari chiedono la tutela del diritto meritevole di protezione.

Lo stesso articolo limita tale protezione per il diritto di cronaca e negli altri casi previsti dalla legge.

## L'Autorità Garante

L'organo di controllo che sovrain-tende 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;

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 di seguito sintetizzati:

### ***I 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;
- 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.

### ***I POTERI CORRETTIVI***

- a. rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le dispo-

sizioni del presente regolamento;

b. rivolgere ammonimenti al titolare 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;

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

### ***I 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, attraverso la quale ogni Stato può prevedere ulteriori poteri. Nel D.Lgs. 101 ciò è accaduto con l'in-

roduzione dell'art. 154 bis che autorizza il Garante ad 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

scientifico-storico-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 4 il legislatore ha infine dato possibilità al Garante di avviare d'Ufficio, in base ai poteri di indagine sanciti all'art. 58, paragrafo 1, 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)

### **IL 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 e 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 preve-

de 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).

### **LA 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.

### **IL 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:

#### **Avverso il garante**

Sono impugnabili:

- le decisioni giuridicamente vin-

colanti 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.

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

#### **Avverso il titolare o il responsabile del trattamento**

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’authority pubblica, il foro esclusivo è il luogo di stabilimento del pubblico potere.

È 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.

## *Le domande di risarcimento del danno (art. 82 Reg.)*

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, decifrazione 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 riguar-

dano; 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.

L'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.

## Il quadro sanzionatorio

### GLI ILLECITI AMMINISTRATIVI

Il nuovo quadro sanzionatorio amministrativo pecuniario direttamente applicabile è delineato esativamente 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 la 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 vio-

- lazione; 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

si 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:

<b>Violazione dei seguenti obblighi</b>	<b>Norme del Regolamento o del Codice Privacy</b>
In materia di trattamento dati che non richiedono l'identificazione	Art. 11Reg.
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-quaterdecies 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-ter 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:

<b>Violazione dei seguenti obblighi</b>	<b>Norme del Regolamento o del Codice Privacy</b>
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 effettuano 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-quinquies Codice
Delle norme sul trattamento di particolari categorie di dati personali per rilevanti motivi di interesse pubblico rilevante	Art. 2-sexies Codice
Delle norme sulla diffusione in dati genetici, biometrici e relativi alla salute	Art. 2-septies Codice
Delle norme sul trattamento dei dati relativi a condanne penali	Art. 2-octies Codice
Delle disposizioni sul trattamento dei dati personali relativi a persone decedute	Art. 2-duodecies 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 sul 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. 11-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. 12 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. 2-quater 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:

<b>Violazione dei seguenti obblighi</b>	<b>Norme del Regolamento o del Codice Privacy</b>
Inosservanza di un ordine da parte del Garante nell'esercizio del potere correttivo	Art. 58 par. 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 particolare 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. È 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.

**GLI 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 (violazione degli art. 2-ter: nell'esercizio di pubblici poteri);	Art. 167-bis	Reclusione da uno a sei anni	Dolo di profitto e dolo di danno
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 raccol-

ta 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.

## *Gli 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 e 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 at-

tuale 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 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.

## *I trattamenti specifici riguardanti le Istituzioni Scolastiche*

### **GLI ESITI SCOLASTICI**

Fin dal 1999 l'Autorità Garante ha espresso il suo giudizio sul tema: "la pubblicità degli esiti scolastici è invece la regola in generale: non può infatti dimenticarsi che vi sono essenziali esigenze di controllo sociale e professionale che dipendono proprio dalle conoscibilità delle valutazioni finali". Tale pronuncia è stata ribadita nel tempo e nella documentazione prodotta dall'Autorità Garante in particolare nelle Linee Guida per le Istituzioni Scolastiche del 2012 e nel Vademecum "La scuola a prova di privacy" del 2016 che così recita "Gli esiti degli scrutini o degli esami di Stato sono pubblici.

Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal Ministero dell'Istruzione dell'Università e della Ricerca.

È necessario però che, nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti, o altri dati personali".

### **IL REGISTRO ELETTRONICO**

Con il Registro elettronico si attua il processo di trasparenza dell'attività didattica e delle procedure seguite per pervenire agli esiti scolastici. I genitori, infatti, possono controllare il percorso formativo dei propri figli e partecipare alla vita della scuola ricevendo le comunicazioni tramite il suddetto registro.

Non si può non evidenziare il problema della sicurezza del sistema informatico in relazione alla protezione dei dati degli alunni e dei genitori. Basti pensare ai rischi correlati all'eventuale diffusione delle anagrafiche degli studenti e

dei genitori visibili, in alcune piattaforme, ai docenti della classe e via web anche dalla propria abitazione con le credenziali all'uopo fornite dal Titolare, cioè dalla scuola. Poiché ci si riferisce ad un trattamento dati in outsourcing, il Titolare dovrà, con il gestore del Registro Elettronico, stipulare un contratto di servizi in cui viene designato Responsabile del trattamento il Gestore stesso.

Questo Gestore tratterà i dati degli alunni, dei genitori e dei docenti per conto del Titolare e per questo sarà sottoposto alle norme e alle responsabilità del Regolamento UE. Senza entrare in questioni tecnico-informatiche, basti pensare che la principale vulnerabilità del Registro elettronico è rappresentata dall'uso delle credenziali per accedervi in classe nel corso della lezione, oppure nell'aula docenti, e risulta evidente che altri potrebbero facilmente individuare l'account.

### **I DATI BIOMETRICI**

Il trattamento di dati biometrici, in particolar modo per la rilevazione delle presenze sul posto di lavoro, rimane ad oggi vietata. Alcune eccezioni sono state ammesse dal Garante previa una verifica preliminare per rilevare l'accesso da parte di persone a siti o zone la cui protezione deve prevedere forme più elevate di sicurezza (siti ospedalieri, siti militari, banche).

Alla data del 26 ottobre 2018 è stato esitato dal Consiglio dei Ministri il DDL cosiddetto "Concretezza" che al suo interno prevede, al fine di combattere il fenomeno dell'assenteismo dei dipendenti pubblici, l'utilizzo della rilevazione delle presenze attraverso l'identificazione tramite dati biometrici (impronte digitali, iride etc..) abbinata

ad uno strumento di videosorveglianza. Tale provvedimento, a dire il vero, è accompagnato, per la parte in esame, dal parere dell'Autorità Garante che, pur se favorevole, pone delle condizioni precise e severe all'utilizzo.

In primo luogo, limitando la scelta ad un solo strumento di verifica e poi ancorandone l'utilizzo alla sussistenza di specifici fattori di rischio, ovvero a particolari presupposti, quali ad esempio le dimensioni dell'ente, il numero dei dipendenti coinvolti, la ricorrenza di situazioni di criticità che potrebbero essere anche influenzate dal contesto ambientale. In ultimo, tutto sarebbe demandato a specifici regolamenti attuativi a cura della stessa Autorità. Inoltre, per il personale docente e educativo le modalità attuative saranno stabilite dal MIUR di concerto con il Ministero della pubblica amministrazione sentito il Garante.

### **I TEMI IN CLASSE**

Anche qui una pronuncia del Garante datata 1999 ma rimasta immutata nel tempo e puntualmente ribadita nelle successive pubblicazioni dedicate alla scuola è inequivocabile. "L'assegnazione da parte degli insegnanti di temi in classe, anche se attinenti alla sfera personale o familiare degli alunni, è del tutto lecita e rispondente alle funzioni attribuite all'Istituzione Scolastica".

### **LE PUBBLICAZIONI DELLE FOTO DEGLI ALUNNI**

Non esiste un divieto alla pubblicazione di foto di alunni sul sito dell'Istituzione Scolastica. In diversi interventi il Garante ha ribadito la necessità di indicare nell'informativa la possibilità che le foto di alunni in situazioni didattiche e in atteggiamenti propositivi possano essere

pubblicate al fine di fornire dimostrazione dell'azione educativa svolta dalla scuola. Tutto ciò ancorato anche ad una base di liceità che deve essere contenuta all'interno del PTOF.

### **LE 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".

### **LA 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:

- inoltre, 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, 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".

### **L'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".

### **GLI SCUOLABUS E LA 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 online, 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".

## **LA 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.