REGOLAMENTO PRIVACY E DECRETO DI ARMONIZZAZIONE - INDICE

PARTE PRIMA

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. Si, 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 delle 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 questa 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'adesione dell'Italia all'ordinamento delle Comunità Europee (ora dell'Unione Europea). Ciò marca una netta differenza dallo strumento delle 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 relazionato 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.

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 trattamento 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 questo 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.

PRINCIPI DEL TRATTAMENTO

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 rettificazione 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 comprovarlo*". 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.

BASI DI LICEITA′

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 assenze 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.

FIGURE DI SISTEMA (TITOLARE, RESPONSABILE, DPO, INCARICATI)

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 stessa rappresentata organicamente dal suo Dirigente Scolastico. Che 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 ed 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, e 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 quindi 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, invece, 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 ed 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 (artt. Da 13 a 22)

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 qualsiasi 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.

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).

Diritto alla cancellazione (diritto all'oblio) (art. 17)

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 informazioni 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 demandato 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 la limitazione prevede comunque la conservazione), l'opposizione al trattamento (perché l'opposizione non determina la cancellazione), la portabilità dei dati (perché i dati 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 culturale, 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.

Diritto alla limitazione (art. 18) 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.

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 traslata 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 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.

OBBLIGHI SPECIFICI PER IL TITOLARE ED IL RESPONSABILE DEL TRATTIAMENTO - 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 comprendere 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 realizzeranno per tutti i soggetti coinvolti nel trattamento.

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 DELLA VIOLAZIONE 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.

Nel 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 DELLA VIOLAZIONE DEI DATI

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 documenti qualsiasi violazione dei dati personali, le circostanze che le hanno originato, 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 continuamenti 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.

DATA BREACH – VIOLAZIONE DEI DATI

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 documentare 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 ed 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 decifratura 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 e certo 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 trattamento 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 ed 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.

VALUTAZIONE DI IMPATTO PRIVACY – VIP (DPIA – Data Protection Impact Assessment)

L'oggetto della normativa privacy non è il dato in sé stesso bensì il trattamento con il quale il dato entra a fa parte del ciclo di gestione 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 e considerando la natura, l'oggetto, il contesto e le finalità proprie del trattamento, infine 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; c) 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 meccanismi 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 agevolare 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, e' ammesso il pagamento in misura ridotta di un 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. Così 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 alla 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). Ebbene 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 provveduto 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.

TRATTAMENTI SPECIFICI DELLE ISTITUZIONI SCOLASTICHE

1. 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".

2. 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 alla 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.
3. 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.

4. 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."
5. Pubblicazione foto di 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 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.

Antonino Foti