REGOLAMENTO UE 679/2016

protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Dott.ssa Elisa Palermo

I TESTI NORMATIVI VIGENTI

- Il Regolamento UE 679/2016 ha abrogato la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

- IN ITALIA: D.lgs. 30 giugno 2009, n. 196 (cd. CODICE PRIVACY) modificato dal D.lgs. 10 agosto 2018, n. 101

LA STORIA…..

- **1950 - Convenzione diritti Uomo – art. 8 RIGHT TO BE ALONE** - tutela il diritto della persona alla sua riservatezza

- **1995 - Dir. 95/46/CEE - PROTEZIONE DELLA PERSONA TITOLARE DI DIRITTI SUI SUOI DATI** - tutela i dati della persona ed i diritti sui dati stessi

Cosa succede con il GDPR?

- **1. VIENE UNIFORMATA LA DISCIPLINA A LIVELLO COMUNITARIO, ATTRAVERSO UN REGOLAMENTO**

con applicazione anche extra UE ove si trattino dati dei cittadini europei

- **2. IL GDPR DISCIPLINA UN NUOVO MONDO: I DATI DIGITALI**

quindi l'architettura normativa è totalmente diversa da quella della Direttiva precedente

Cosa succede con il GDPR?

3. **IL DIRITTO ALLA PROTEZIONE DEI DATI DIVENTA DIRITTO CIVILE EUROPEO**

4. **I DATI VENGONO PROTETTI E DISCIPLINATI IN QUANTO MATERIA PRIMA DELLA NUOVA ECONOMIA (DATA ECONOMY)**

I dati hanno un valore economico e la loro circolazione non è evitabile.

Nasce così l'esigenza di proteggere i dati e darsi regole per una circolazione sicura.

Il diritto alla protezione dei dati personali

E’ un diritto alla autodeterminazione formativa, ossia il potere di una persona fisica di verificare e controllare il trattamento di dati che lo riguardano, svolto da terzi, cui corrisponde l’obbligo del titolare di adottare misure tecniche ed organizzative di sicurezza.

DATA ECONOMY

Commissione UE COM (2017)9 final – 17 gennaio 2017

“Costruire una economia dei dati europea”

Il valore dell’economia dei dati nella UE

Anno 2014

257 mld di euro (l’1,85% del PIL della UE)

Anno 2015

272 mld di euro (pari all’1,87% del PIL della UE), per un incremento annuo del 5,6%

Anno 2020

Si stimano 643 mld di euro, pari al 3,17% del PIL della UE

DATA ECONOMY

Elżbieta Bieńkowska, Commissario responsabile per il
Mercato interno, dell'industria, dell'imprenditorialità e delle PMI,
17 gennaio 2017

I dati sono il motore della nuova economia.

“Per garantire che l'Europa abbia successo nella nuova era dell'economia industriale, abbiamo bisogno di un flusso di dati solido e prevedibile all'interno del mercato unico. L’esistenza di norme chiare sull’accesso ai dati, sulla sicurezza e sulla responsabilità è fondamentale per consentire alle imprese europee, le PMI e le start-up di sfruttare appieno il potenziale di crescita di Internet delle cose.

Invece di innalzare frontiere digitali dovremmo impegnarci per costruire una economia europea dei dati che sia pienamente integrata e concorrenziale nell’economia globale dei dati ".

QUALI SONO LE NOVITA' SOSTANZIALI?

- **La forza normativa**
- **La nuova architettura giuridica**

LA FORZA NORMATIVA

E’ un Regolamento e non una Direttiva

Trova quindi diretta applicazione nei paesi membri della UE

Cosa è rimasto del Codice Privacy?

LEGGE 25 ottobre 2017, n. 163 – legge di delegazione europea - ART. 13

a**) abrogare espressamente le disposizioni del codice in materia di trattamento dei dati personali, di cui** al decreto legislativo 30 giugno 2003, n. 196, incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679;

b) **modificare il codice di cui al decreto legislativo 30 giugno 2003, n. 196, limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel regolamento** (UE) 2016/679;

c**) coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni recate** dal regolamento (UE) 2016/679;

d) prevedere, ove opportuno, il **ricorso a specifici provvedimenti attuativi e integrativi adottati dal** Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal regolamento (UE) 2016/679;

LEGGE 25 ottobre 2017, n. 163 – legge di delegazione europea - ART. 13

e) adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, **il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679, con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse.**

L'intervento del **D.lgs. 101/2018** ha abrogato buona parte del Codice Privacy nostrano, inserendo semplicemente dei rimandi al GDPR.

Ad oggi l'approccio alla normativa privacy richiede la lettura congiunta di **REGOLAMENTO EUROPEO – CODICE ITALIANO - CONSIDERANDO**

Che cosa resta dei provvedimenti del Garante?

CONSIDERANDO 171

Il presente regolamento dovrebbe abrogare la direttiva 95/46/CE. Il trattamento già in corso alla data di sua applicazione dovrebbe essere reso allo stesso conforme entro un periodo di due anni dall'entrata in vigore del regolamento.

Qualora il trattamento si basi sul consenso a norma della direttiva 95/46/CE, non occorre che l'interessato presti nuovamente il suo consenso, se questo è stato espresso secondo modalità conformi alle condizioni del presente regolamento, affinché il titolare del trattamento possa proseguire il trattamento in questione dopo la data di applicazione.

NUOVA ARCHITETTURA NORMATIVA

- **Si passa da una disciplina di “adempimenti”**

Ad una disciplina di natura molto più sostanziale.

- **E’ la fine di un modello di disciplina prescrittiva, “di adempimenti”.**

- **L’atteggiamento è meno burocratico e più sostanziale.**

I 2 CARDINI

1. **Approccio basato sul rischio**
   La *governance* del rischio

2. **ACCOUNTABILITY**

1 – APPROCCIO BASATO SUL RISCHIO

considerando 76

La PROBABILITA' e la GRAVITA' del RISCHIO per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.

considerando 77

Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento, in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, **e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante ANALISI DEL CONTESTO e ANALISI DEL RISCHIO LEGALE.**

APPROCCIO BASATO SUL RISCHIO

Il metodo di gestione del trattamento dei dati non è più standardizzato, ma viene trattato caso per caso attraverso l'**analisi del rischio**:

- Rischio di attacco **dall'esterno**
- Rischio di diffusione del dato **all'interno**

Il Rischio potrà essere basso, medio o alto e conseguentemente verrà scelto il metodo più efficace da applicare (software, formazione…) in base all'analisi del contesto

APPROCCIO BASATO SUL RISCHIO

Ad esempio:

Un Golf Club avrà maggior rischio di attacco dall'esterno (software)

Una Casa di Cura per anziani, maggior rischio di diffusione del dato internamente (formazione, sensibilizzazione)

I Principi generali sul trattamento dei dati personali

- ***Principio di Necessità***
- ***Principio di Proporzionalità -*** i dati che tratto devono essere necessari allo scopo perseguito. Bilanciamento di interessi.
- ***Principio di Pertinenza***
- ***Principio di Non Eccedenza***

Ad esempio, più sarà rilevante il motivo (perché) per cui devo trattare i dato, più il trattamento (come) sarà approfondito – esenzioni, assenze giustificate da patologie ecc.

2 - ACCOUNTABILITY
ART. 5 Regolamento

I dati personali sono:

a) trattati in modo **lecito** *(perseguimento di un interesse pubblico o connesso a pubblico potere),* **corretto** e **trasparente**

b) raccolti per **finalità determinate**, esplicite e legittime

c) adeguati, pertinenti e limitati ***(Principio di minimizzazione)***

d) **esatti**

e) **conservati**

d) trattati in maniera da garantire un'adeguata sicurezza dei dati personali ***(CONFIDENTIALY),*** compresa la protezione, mediante misure tecniche e organizzative adeguate ***(ACCOUNTABILITY).***

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

ACCOUNTABILITY

1. necessità che il responsabile **adotti misure** appropriate ed efficaci per attuare i principi di protezione dei dati.
2. necessità di dimostrare, su richiesta, che sono state adottate misure appropriate ed efficaci. Pertanto il responsabile deve **fornire la prova** di quanto esposto al punto 1.

- **Le misure non devono essere imposte dal legislatore, ma devono essere scelte dal Titolare.**
- **La norma indica gli obiettivi da raggiungere, lasciando le imprese libere di individuare le metodologie più efficaci per raggiungerli.**

ACCOUNTABILITY

IMPLEMENTAZIONE DI UN MODELLO ORGANIZZATIVO DI GESTIONE DEL DATO CHE CONSENTA:

- DI RISPETTARE I PRINCIPI DELL'**ART. 5**
- DI MANTENERE NEL TEMPO TALE RISPETTO
- DI DARE PROVA DI TALE RISPETTO

ACCOUNTABILITY

Ricapitolando….

il processo di responsabilizzazione del Titolare, tenuto non solo ad **individuare** ed **adottare** misure idonee a prevenire trattamenti illeciti, ma a **dare prova** di avere fatto tutto il possibile.

cd. Onere della prova di adeguatezza

ESEMPI DI ACCOUNTABILITY

- **LA SCELTA DELLE MISURE DI SICUREZZA**

Nell'Allegato B del **d.lgs. 196/2003** venivano indicata un'elencazione tassativa di misure di sicurezza da adottare.

Nel **GDPR** al contrario il Titolare del trattamento dei dati, valutato il caso concreto, deve:

- classificare i dati (Registro dei Trattamenti)
- Valutare i dati e misurarli in termini di sicurezza
- Operare la scelta più adeguata
- Documentarne la motivazione e le valutazioni comparative effettuate
- Adottare Regolamenti interni se necessario

ESEMPI DI ACCOUNTABILITY

- **APPLICAZIONE DELLA NORMA DEL LEGITTIMO INTERESSE**

ART. 6 GDPR – Liceità del trattamento (dei dati comuni)

Fornisce le basi giuridiche e detta le condizioni per il trattamento dei dati personali.

Comma 1 lett. F) "*il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.*"

COME E’ ORGANIZZATO IL REGOLAMENTO

a. I SOGGETTI
b. I DIRITTI DEGLI INTERESSATI
c. I PRINCIPI DEL TRATTAMENTO
d. GLI OBBLIGHI GENERALI, la sicurezza, Misure tecniche e organizzative
e. IL REGIME SANZIONATORIO

a) - I SOGGETTI

- IL TITOLARE
- IL CONTITOLARE
- IL RESPONSABILE
- IL DPO (Data Protection Officer)
- L’AUTORIZZATO

IL TITOLARE – articolo 24 GDPR

Quando si tratti di persona giuridica il Titolare del Trattamento dei Dati coincide con il Legale Rappresentante della Azienda / Società / Ente.

Stabilisce le finalità e i mezzi del 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 presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario…"

IL CONTITOLARE, articolo 25 GDPR

Si tratta di figura solo eventuale, che incontriamo allorquando più soggetti insieme decidono e gestiscono le modalità di trattamento dei dati raccolti.

La Contitolarità deve risultare da atto scritto e i soggetti sono obbligati in solido nei confronti dei soggetti interessati.

IL RESPONSABILE, articolo 28 e 39 GDPR

E’ persona fisica o giuridica che esegue dietro a delega (con atto o contratto) del Titolare, per suo conto, funzioni in materia di trattamento dei dati, stabilendo solo i mezzi per il trattamento (e non anche le finalità).

Nell’impianto del GDPR le funzioni del Responsabile vengono intensificate rispetto a quelle precedentemente fornite dalla Direttiva Europea del ’95.

Azione di responsabilità diretta.

RESPONSABILE INTERNO O ESTERNO?

Il testo originario del D.lgs. 196/2003 italiano (Codice Privacy) distinse fra le figure di:

-**Responsabile interno**

-**Responsabile esterno**

Con un diverso impianto di responsabilità (in solido, con azione di rivalsa per il primo e diretta per il secondo).

Il GDPR nella sua nuova stesura sembrerebbe col termine generico Responsabile parlare solo del secondo.

IL DPO – Data Protection Officer
Sezione IV – artt. 37-39 GDPR

Figura inserita dal GDPR, può essere sia interno che esterno alla Azienda che lo nomina.

E’ un soggetto con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all’interno di un’azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.

IL DPO – Data Protection Officer

E’ un organismo di controllo autonomo, imparziale, che svolge un ruolo di vigilanza.

Non soggiace alle azioni di responsabilità derivanti dal Codice Privacy o dal GDPR, perché non partecipa della attività di trattamento dei dati.

Risponde unicamente di inadempimento contrattuale nei confronti del Titolare che lo nomina.

L’AUTORIZZATO art. 4, n. 10 GDPR

Il regolamento europeo non prevede espressamente la figura dell'**incaricato**, ma non ne esclude la nomina, facendo riferimento a **persone autorizzate** al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile.

Incaricato, o autorizzato, è il **soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali**. L'autorizzato può operare alle dipendenze del titolare, ma anche del responsabile se nominato. Ovviamente gli autorizzati possono essere organizzati con diversi livelli di delega.

b) - I DIRITTI DEGLI INTERESSATI – CAPO III GDPR

- diritto all'informativa (ARTT. 12-14)
- diritto all'accesso (ART. 15)
- diritto di rettifica (ART. 16)
- diritto alla cancellazione (all'oblio) (ART. 17)
- diritto alla limitazione del trattamento (ART. 18)
- diritto alla portabilità (ART. 20)
- diritto all'opposizione (ART. 21)

Diritto all'informativa (ARTT. 12-14)

Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni e le comunicazioni relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato.

Diritto all’accesso (ART. 15)

1. *L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:*

a) *le finalità del trattamento;*

b) *le categorie di dati personali in questione;*

c) *i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati…..*

d) *il periodo di conservazione dei dati personali previsto….*

e) *l'esistenza del diritto di chiedere al titolare la rettifica o la cancellazione dei dati personali o la limitazione del trattamento o di opporsi al loro trattamento;*

f) *il diritto di proporre reclamo a un'autorità di controllo;*

g) *qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;*

h) *l'esistenza di un processo decisionale automatizzato, compresa la profilazione…*

Diritto di rettifica (ART. 16)

L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Diritto all’oblio (ART. 17)

In determinate circostanze *“l'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali…”*

Diritto alla limitazione del trattamento (ART. 18)

In alcuni casi *“l'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento…”*

Diritto alla portabilità (ART. 20)

“L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso o su un

b) Il trattamento sia effettuato con mezzi automatizzati.

Diritto all’opposizione (ART. 21)

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano (…) compresa la profilazione sulla base di tali disposizioni. Il titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

c) - I PRINCIPI DEL TRATTAMENTO – ART. 5 GDPR

a) **LICEITA', CORRETTEZZA, TRASPARENZA:** i dati personali di persona fisica sono trattati in modo lecito, corretto e trasparente.

b) **LIMITAZIONE DELLA FINALITA':** i dati sono raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità.

c) **MINIMIZZAZIONE DEI DATI:** i dati sono adeguati, pertinenti e limitati rispetto alle finalità per le quali sono trattati.

I PRINCIPI DEL TRATTAMENTO – ART. 5 GDPR

d) ESATTEZZA: i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

e) LIMITE DELLA CONSERVAZIONE: conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

f) INTEGRITA' E RISEVATEZZA: trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate.

2) RESPONSABILIZZAZIONE: Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo.

d) - GLI OBBLIGHI GENERALI, la Sicurezza, Misure Tecniche e Organizzative

- privacy by design e by default (art. 25)
- registro dei trattamenti (art. 30)
- data breach (art. 33 e 34)
- valutazione d’impatto (art. 35)
- nomina DPO (art. 37)
- codice di condotta (art. 40)

Privacy by design e by default art. 25

La protezione dei dati garantita sin dalla progettazione del trattamento degli stessi, ricorrendo a sistemi adeguati.

Il Regolamento europeo impone al titolare del trattamento l'adozione di misure tecniche ed organizzative adeguate al fine di tutelare i dati da trattamenti illeciti.

L'articolo 25, in particolare, introduce il principio di **privacy by design** e **privacy by default**, un approccio concettuale innovativo che impone alle aziende l'obbligo di avviare un progetto prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali.

Privacy by design e by default

Prevenire e non correggere, cioè i problemi vanno valutati nella fase di progettazione, e l'applicativo deve prevenire il verificarsi dei rischi.

- privacy come **impostazione di default** (ad esempio, non deve essere obbligatorio compilare un campo di un form il cui conferimento di dati è facoltativo);
- privacy **incorporata nel progetto** (ad esempio, l'utilizzo di tecniche di pseudonimizzazione o minimizzazione dei dati);
- massima **funzionalità**, in maniera da rispettare tutte le esigenze (rifiutando le false dicotomie quali più privacy = meno sicurezza);
- **sicurezza** durante tutto il ciclo del prodotto o servizio;
- **visibilità** e **trasparenza** del trattamento, cioè tutte le fasi operative devono essere trasparenti in modo che sia verificabile la tutela dei dati;
- **centralità dell'utente**, quindi rispetto dei diritti, tempestive e chiare risposte alle sue richieste di accesso.

Registro dei trattamenti (art. 30)

“Ogni titolare del trattamento e, ove applicabile, il suo rappresentante, tengono un registro delle attività di trattamento svolte sotto la propria responsabilità….”

Tale registro contiene tutte le informazioni tassativamente indicate all’art. 30.

Registro dei trattamenti

- **Elenca i trattamenti di dati in essere**
- **Per ogni trattamento indica:**

➢ *I soggetti* (titolare, responsabile, dpo ecc)

➢ *Quale tipologia di dati viene trattata* (particolari, comuni ecc.)

➢ *Finalità del trattamento* (perché vengono trattati ed eventuale consenso)

➢ *Dove si trovano i dati*

➢ *Tempi di conservazione dei dati*

➢ *Modalità di trattamento* (quali misure sono state adottate per proteggere i dati).

DATA BREACH – ART. 33

- *“In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza…”*
- *“Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.”*

DATA BREACH – ART. 34

“Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.”

DATA BREACH

Si profila un DATA BREACH ogni volta che avviene la distruzione, perdita, modifica, divulgazione non autorizzata o accesso a dati personali trasmessi, conservati o trattati a seguito di:

- **Accesso abusivo ai sistemi**
- **Sottrazione fraudolenta di dati**
- **Perdita accidentale di dati**

Comunicazione al Garante: entro 72 ore

Comunicazione all'interessato: tempestiva

Valutazione d’impatto (art. 35)

“Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.”

Nomina DPO (art. 37)

"Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico

b) le attività principali del titolare o del responsabile consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le attività principali del titolare o del responsabile consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10…"

Codici di condotta art. 40

Codici di condotta destinati a contribuire alla corretta applicazione del regolamento, allo scopo di precisarne l'applicazione, ad esempio relativamente a:

a) il trattamento corretto e trasparente dei dati;
b) i legittimi interessi perseguiti dal responsabile del trattamento in contesti specifici;
c) la raccolta dei dati personali;
d) la pseudonimizzazione dei dati personali;
e) l'informazione fornita al pubblico e agli interessati;
f) l'esercizio dei diritti degli interessati ecc.

e) – SANZIONI – CAPO XIII, artt. 77-83*Mezzi di ricorso, responsabilità e sanzioni*

- il **RECLAMO** alla autorità di controllo
- Il **ricorso amministrativo o extragiudiziale**
- Il **ricorso giurisdizionale** avverso una decisione giuridicamente vincolante dell'autorità di controllo o se lo stesso non tratti il reclamo
- Il **ricorso giurisdizionale** contro il Titolare o Responsabile, qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

e) – SANZIONI – art. 82-83

- Il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.
- Le sanzioni amministrative pecuniarie sono inflitte tenendo conto di alcuni elementi aggravanti e/o attenuanti
- Possono comminare sanzioni fino a 20.000 euro

Regime sanzionatorio MODULARE

Criteri per misurare la sanzione

A. la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento e il livello del danno subito;
B. il carattere doloso o colposo della violazione;
C. le misure adottate dal titolare del trattamento o dal responsabile per attenuare il danno;
D. il grado di responsabilità del titolare del trattamento, o del responsabile del trattamento, tenendo conto delle misure tecniche ed organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
E. eventuali precedenti violazioni;

Regime sanzionatorio MODULARE

F. il grado di cooperazione con l'autorità di controllo*;
G. categorie di dati personali interessate dalla violazione;
H. la maniera in cui l'autorità di controllo ha preso conoscenza della violazione;
I. l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42;
K. eventuali altri fattori aggravanti o attenuanti.

* Ogni Stato dell'Unione europea ha la sua **Autorità di controllo,** detta anche Garante della privacy, la cui competenza è quella di gestire i reclami e le violazioni del GDPR oltre alle norme nazionali vigenti per la protezione dei dati personali.

Il **Garante per la protezione dei dati personali** (Garante Privacy) è:

*"l'**autorità di controllo nazionale italiana** in materia di protezione dei dati personali, un'autorità amministrativa indipendente istituita dalla **legge sulla privacy** (legge 31 dicembre 1996, n. 675), in attuazione della direttiva comunitaria 95/46/CE. Oggi è disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196).*

REGIME SANZIONATORIO

Quanto costa rispettare il Regolamento?

- Costo consulenti
- Costo tempo
- Costo uomo

Regime sanzionatorio

Quanto costa NON rispettare il Regolamento?

- Rischio immagine
- Rischio richiesta danni utente
- Rischio sanzioni, economicamente importanti ma proporzionali alla violazione riscontrata

NUOVE DEFINIZIONI DEL GDPR

- **Dati personali (art. 4 lett. 1):** dati che rendono identificato o identificabile un soggetto
- **Dati particolari:** più tutelati (ex dati sensibili)
- **Dato Pseudomizzato:** dato in cui l'identificatore viene sostituito da indicatori fittizi o pseudonimi
- **Dato de-identificato (art. 11):** dati a cui sono stati rimossi gli identificatori diretti o indiretti, con rischio residuo di re-identificazione.

NUOVE DEFINIZIONI DEL GDPR

- **Dato anonimo:** è il dato non identificabile o re-identificabile. Esce così dalla sfera di applicazione del Regolamento, (es. quelli acquistati da altri che si vincolano contrattualmente a non cedere mai l'identificatore utile a re-identificare il dato: nelle mani del cedente saranno dati pseudonomizzati, nelle mani del cessionario saranno dati anonimi)**.**
- **Profilazione** (trattamento automatizzato di dati personali per analizzare)

Trattamento di categorie particolari di dati personali – Art. 9 GDPR

Il regolamento introduce il nuovo concetto di DATI PARTICOLARI, che sostituisce i precedenti DATI SENSIBILI, aggiungendo di fatto al vecchio impianto:

- I dati biometrici, quelli atti ad identificare in modo univoco una persona fisica
- I dati atti a rilevare l'orientamento sessuale di una persona.

Art. 9 GDPR, comma 1

1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Art. 9 GDPR, comma 2

2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:

a. *Consenso Informato.*
b. *Necessità per diritti del Titolare in materia di diritto del lavoro e della sicurezza e protezione sociale.*
c. *Per tutela di un interesse vitale dell'interessato, in stato di incapacità fisica o giuridica a prestare consenso.*
d. *Se trattati da Ass.ni o Fond.ni senza scopo di lucro, senza divulgazione esterna.*
e. *Se è l'interessato ad avere reso pubblici i propri dati.*
f. *Diritto di difesa in sede giurisdizionale.*
g. *Interesse pubblico, purchè il trattamento sia proporzionato.*
h. *Medicina preventiva – lavoro – idoneità fisica al lavoro, diagnosi, assistenza o terapia sanitaria. IN QUESTI CASI NON SERVE CONSENSO – NON C'è OBLIO*
i. *Interesse pubblico in sanità pubblica, minacc epe rla salute a carattere transfrontaliero. NO OBLIO*
j. *Archiviazione di pubblico interesse, ricerca scientifica, storica – fini statistici*

TRASPARENZA – ACCESSO E PRIVACY A CONFRONTO

- **Accesso ai documenti amministrativi - legge 241/’90**
- **Accesso ai dati - GDPR e Codice Privacy**
- **Accesso civico (Dlgs 33/2013 art. 5 comma 1) e l’accesso generalizzato (D.Lgs 33/2013 art. 5 comma 2 - Il FOIA)**
- **Considerando n. 4 GDPR. Principio di proporzionalità – contemperamento del trattamento dati con altri diritti fondamentali**

Cons. Stato Sez. IV, 14/05/2014, n. 2472

L'equilibrio tra Accesso agli atti della P.A. e Privacy è dato dal combinato disposto degli artt. 59 e 60 D.Lgs. 30 giugno 2003, n. 196 (Codice della privacy) e delle norme di cui alla legge n. 241 del 1990.

La disciplina che ne deriva delinea tre livelli di protezione dei dati dei terzi, cui corrispondono tre gradi di intensità della situazione giuridica che il richiedente intende tutelare con la richiesta di accesso:

- nel più elevato si richiede la necessità di una situazione di "pari rango" rispetto a quello dei dati richiesti;
- a livello inferiore si richiede la "stretta indispensabilità"
- infine, la "necessità"

(Parziale riforma della sentenza del T.a.r. Lazio, sez. III, 21 ottobre 2013, n. 9036).

richiesta del marito alla agenzia delle entrate per sapere i redditi della moglie, richiesta ritenuta accettabile

L’iter FOIA e la tutela della Privacy

1. Verifica di presenza di casi di esclusione ex art. 5 bis D.lgs. 33/2013
2. Verifica di presenza di controinteressati
3. Valutazione del loro pregiudizio concreto
4. Bilanciamento di interessi fra diritto di accesso e privacy
5. Valutazione di rendere l’accesso parziale

Il diritto alla privacy nel bambino

I bambini, in quanto minori, hanno bisogno della certezza che i loro genitori e gli adulti in generale si occupino e proteggano la loro privacy e si facciano quindi “garanti” dei loro diritti.

Invece non sempre le insidie che può nascondere il web sono note a chi vi naviga.

Le informazioni personali come nuova moneta virtuale (DATA ECONOMY)

Tutto ciò che viene pubblicato, scritto o postato, come anche i video o le foto, è destinato a rimanere a disposizione di chiunque.

Attualmente la tecnologia non è in grado di garantire il rispetto delle norme poste a tutela della privacy dei singoli.

Le informazioni fornite vengono vendute o scambiate con aziende operanti nell'e-commerce o con spammer.

Il rischio è quello di perdere il controllo dell'utilizzo dei propri dati una volta pubblicati in rete, in particolare nei social, con l'aggravante che, la permanenza in rete delle informazioni ponga significativi problemi anche in merito al diritto all'oblio.

Il fenomeno dello “sharenting”

Recenti statistiche testimoniano come, nonostante le tecnologie *touchscreen* siano proprietà dell’adulto, in realtà anche i bambini entrino in contatto con esse, già prima del compimento di tre anni di età.

Oltre al ruolo di “utente” dei social network, il bambino assume spesso anche quello di “contenuto” di immagini, video o post pubblicati da parte dei loro genitori che desiderano raccontare e mettere in luce le proprie esperienze vissute con i figli e condividerle con amici e conoscenti.

Questo fenomeno viene definito “sharenting”, neologismo che deriva dalla fusione delle parole ***share (condividere)*** e ***parenting (genitorialità)*** e mette in luce la tendenza dell’essere umano alla “vetrinizzazione”.

Lo sharenting

Quando un bambino appare in rete, circa nel 45% dei casi viene riportato anche il suo nome di battesimo.

Queste tracce digitali su cui i bambini non hanno controllo vanno a sedimentarsi in rete diventando parte della loro **identità digitale**.

I Social Network vengono spesso visti come dei "palcoscenici virtuali" che gratificano il genitore dandogli la possibilità di condividere preoccupazioni, dubbi, domande sulla gestione dei figli, soprattutto nella fascia di età 0-3 anni, fornendo loro sensazioni rassicuranti.

Rischi della pubblicazione di immagini dei bambini

Il pericolo maggiormente percepito dall'opinione pubblica è legato al fatto che le foto dei minori inserite in rete, in particolare nei Social Network, possano diffondersi tra sconosciuti, essere scaricate, modificate e condivise su siti utilizzati da pedofili.

Rischi della pubblicazione di immagini dei bambini

- La possibilità che delinquenti utilizzino i volti ricavati dalle fotografie per realizzare **fotomontaggi** e esporre le foto ritoccate su **siti di pedofili**.
- Il **rapimento** può essere un altro grande pericolo, se l'adulto non presta troppa attenzione alle impostazioni della privacy nei social, e fa sapere anche a sconosciuti dove si trova il bambino.
- Altra insidia legata alla pubblicazione online può essere il "**rapimento digitale**", ossia il **furto dell'identità online**, che consiste nella manipolazione di foto di bambini trovate on-line facendo credere che siano figli propri.

Ancora il "**child-grooming**" in cui il cyberpredatore raccoglie informazioni sul bambino e sulla sua famiglia instaurando una connessione virtuale volta a scopi illeciti.

Rischi della pubblicazione di immagini dei bambini

- Accanto a comportamenti con rilevanza penale potrebbero portare i bambini a diventare future vittime di **cyberbullismo**.

“Tutto ciò che noi postiamo rimane online, perciò oltre che nuocere alla vita dei bambini lo sharing senza criteri potrebbe contribuire a creare una sorta di dossier digitale sui piccoli”

*(**Giuseppe Riva**)*

Ma cosa dice la legge?

La **Convenzione ONU sui diritti dell'infanzia e dell'adolescenza**, approvata dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989, contiene principi fondamentali fra cui il ***diritto del minore ad essere ascoltato***. Con questa Convenzione il bambino passa da una condizione di inferiorità rispetto ai genitori a persona con libertà e diritti, posta sotto la responsabilità dell'adulto che deve impegnarsi a rispondere ai suoi diritti e bisogni.

Carta dei diritti fondamentali dell'Unione Europea

Stilata a Nizza nel 2000, acquisì efficacia diretta solol'1/12/**2009**, con l'adozione del **Trattato di Lisbona**. Quest'ultima, cita **all'art. 24** quali sono i **diritti del bambino**:

"I bambini hanno diritto alla protezione e alle cure necessarie per il loro benessere. Essi possono esprimere liberamente la propria opinione; questa viene presa in considerazione sulle questioni che li riguardano in funzione della loro età e della loro maturità. In tutti gli atti relativi ai bambini, siano essi compiuti da autorità pubbliche o da istituzioni private, l'interesse superiore del bambino deve essere considerato preminente…".

La pubblicazione

Per “pubblicazione” si intende la divulgazione di un’immagine attraverso un qualsiasi mezzo che la renda pubblica: mostre, siti internet, riviste, cartelloni pubblicitari, ecc.

Vi è una netta differenza tra il caso di pubblicazione della foto del minore **per scopi privati** (inserendo tutti i sistemi di sicurezza possibili) e **per scopi pubblicitari**: infatti in questo secondo caso, è necessario far firmare una liberatoria ai genitori e sottoporre agli stessi l’informativa sulla privacy.

La pubblicazione di immagini di minori

Ai genitori è consentito pubblicare foto o video riguardanti i propri figli (non esiste alcun divieto che sostenga il contrario), l'importante è che lo facciano con consapevolezza e senza metterlo in ridicolo, e che entrambi i coniugi siano d'accordo con questa scelta (art. 10 Codice Civile).

Nel 2017 il tribunale di Mantova ha pubblicato una sentenza sulla condivisione di immagini che riguardano i minori, stabilendo che per quanto riguarda le foto dei figli occorre il consenso di entrambi i genitori.

Cosa dice il Garante della Privacy ?

Nel dicembre 2016 ha formalizzato il **criterio della prudenza nella pubblicazione di foto o video nel Web**

Dichiarando necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

Questo consenso, per quanto riguarda l'infanzia, è in mano a chi esercita la patria potestà sul minore.

Reg. UE 2016/679 (GDPR)

“I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali”.

Come prevenire i rischi

La polizia postale sconsiglia ai genitori la diffusione di foto dei propri figli a causa della diffusione online di nuove modalità di adescamento dei minori nel cosiddetto darknet.

La documentazione come forma di trasmissione di esperienze La fotografia come vera e propria azione educativa

Nei servizi per l'infanzia è ritenuta utile la **documentazione di un progetto educativo**, come i video e le fotografie.

Tale documentazione si costruisce attraverso. l'**osservazione** di una situazione, l'analisi e la selezione dei materiali osservativi e successivamente attraverso la **rielaborazione**, la traduzione e l'interpretazione di questi ultimi

La fotografia può essere utile sia nello scambio di idee, messaggi o informazioni tra educatori e famiglie, sia per far riflettere i piccoli sul lavoro svolto annualmente e permette di rivedere ciò che è stato osservato, acquisendo più informazioni e dettagli, che a occhio nudo potrebbero essere sfuggiti.

La privacy nei servizi per l'infanzia

- Nei servizi per l'infanzia c'è una privacy da salvaguardare. Spesso gli asili "postano" sui Social Network gli scatti fatti ai piccoli durante le attività didattiche quotidiane, o durante le gite scolastiche.

- Tale trattamento dei dati deve essere previamente autorizzato dai genitori. Il servizio deve acquisire un **preventivo consenso alla pubblicazione su siti istituzionali o sui social della scuola**, delle foto scattate in occasione di eventi (come ad esempio le recite) raffiguranti i minori, in particolare quelle dove sono riconoscibili i volti.

- Il rischio infatti è quello di commettere un **reato**, con conseguente obbligo di risarcimento del danno.

La privacy nei servizi per l'infanzia

In qualità di pubblica amministrazione, la scuola tratta i dati degli studenti in forza di legge o di regolamento e pertanto **non è tenuta a chiedere il consenso** per la pubblicazione delle fotografie che ritraggono studenti, se rispetta le finalità istituzionali e didattiche proprie della scuola.

L'istituzione deve però dimostrare che la pubblicazione di fotografie o video è indispensabile per la valenza di uno o più progetti didattici. Per fare questo è necessario descrivere nel PTOF quali sono i **motivi didattici** che rendono necessaria la pubblicazione delle fotografie, esplicitando il **fine esclusivo** di "documentare le attività formative", gli **ambienti dove si intende pubblicare** le foto (in un sito, nei social ecc.) e il **grado di privacy applicato** o personalizzato.

Poiché la gestione dell'immagine del minore è tutelata anche dalla legge, è **comunque consigliato farsi rilasciare una liberatoria**, quanto più completa possibile, firmata da entrambi i genitori.

Grazie per l’attenzione

dott.ssa Elisa Palermo