Il Regolamento europeo in materia di protezione dei dati personali

Principali novità e ambito di applicazione

La riservatezza e la protezione dei dati personali

La sfera della riservatezza è la più ***vulnerabile*** *a causa dei moderni mezzi di comunicazione. Pertanto, la definizione di privacy si arricchisce di* ***nuovi significati****. Dal «diritto ad essere lasciati soli» tipico del diciannovesimo secolo, si arriva infatti alle più recenti istanze di tutela dei dati personali.*

La riservatezza e la protezione dei dati personali

Parallelamente, si assiste a un progressivo ampliamento della nozione di sfera privata, che comprende ormai situazioni e interessi prima esclusi dall'area della ***protezione giuridica****, e si proietta ben al di là della pura identificazione di un soggetto e dei suoi comportamenti riservati. Si può così definire la* ***sfera privata come l'insieme di azioni, comportamenti, opinioni, preferenze, informazioni personali su cui l'individuo intende mantenere un controllo esclusivo****.*

La riservatezza e la protezione dei dati personali

La prima norma di riferimento è l'art. ***8 della Convenzione Europea dei Diritti dell'Uomo,*** *firmata a Roma. I commi 1 e 2 di questo articolo stabiliscono che: «****Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*** *Non può esserci ingerenza di un'autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui».*

La riservatezza e la protezione dei dati personali

La nostra Costituzione – art. 13, 14 e 15

Art. 13

La libertà personale è inviolabile

Non è ammessa forma alcuna di detenzione, di ispezione o perquisizione personale, né qualsiasi altra ***restrizione della libertà personale****, se non per atto motivato dell'autorità giudiziaria e nei soli casi e modi previsti dalla legge*

Art. 14

Il domicilio è inviolabile

Non vi si possono eseguire ispezioni o perquisizioni o sequestri, se non nei casi e modi stabiliti dalla legge secondo le garanzie prescritte per la tutela della libertà personale

Art. 15

La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili.

La loro limitazione può avvenire soltanto per atto motivato dell'autorità giudiziaria con le garanzie stabilite dalla legge.

La riservatezza e la protezione dei dati personali

La produzione europea in materia di dati è stata innanzitutto rappresentata dalla ***Direttiva 46/95/CE****, oggi abrogata e sostituita dal Regolamento (UE)* ***2016/679*** *del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla «protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati».*

La riservatezza e la protezione dei dati personali

La direttiva bilanciava dunque la ***salvaguardia dei diritti individuali*** *e l'interesse alla circolazione dei dati statuendo, con formula positiva, l'obbligo degli Stati membri di garantire la* ***«tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata con riguardo al trattamento dei dati personali».***

La riservatezza e la protezione dei dati personali

Con formula negativa è espresso il divieto di ***«restringere o vietare la libera circolazione dei dati personali tra gli stessi Paesi, per motivi connessi a tale tutela».***

Questa finalità è stata conservata e rafforzata dal ***Regolamento (UE) 2016/679,*** *il quale espressamente prevede che* ***«la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale».***

Il nuovo Regolamento europeo

- ***Elementi essenziali***
- ***Le principali novità del nuovo Regolamento europeo***
- ***Il programma di adeguamento; che cosa dobbiamo fare?***
- ***Misure di sicurezza***

Il nuovo Regolamento europeo – elementi essenziali

Regolamento europeo concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati

Regolamento europeo 2016/679

- ***approvato dal Parlamento europeo il 14 aprile 2016***
- ***in vigore dal 24 maggio 2016***
- ***direttamente applicabile dal 25 maggio 2018***

Il nuovo Regolamento europeo – elementi essenziali

- ***La protezione dei dati personali è un diritto fondamentale (art. 8 par. 1 Carta dei diritti fondamentali dell'Unione Europea)***
- ***Il diritto alla protezione dei dati non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e contemperato con altri diritti fondamentali (Considerando 4)***

Il nuovo Regolamento europeo – elementi essenziali

Al fine di assicurare un livello coerente e elevato di protezione delle persone e rimuovere gli ostacoli alla circolazione dei dati personali, il livello di protezione dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali deve essere equivalente in tutti gli Stati membri (Considerando 10)

Il nuovo Regolamento europeo – elementi essenziali

- ***Abroga la direttiva europea 95/46/CE – Direttiva Madre***
- ***Non abroga il D.Lgs. n. 196 del 2003***
- ***Non abroga i provvedimenti del Garante della Privacy***
- ***Emanato il D. lgs n. 101/2018 – adeguamento al Regolamento Europeo***

Il nuovo Regolamento europeo

coordinamento normativo

Ove il regolamento preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri, gli Stati membri possono nella misura necessaria per la coerenza e per rendere le disposizioni nazionali comprensibili alle persone integrare elementi del regolamento nel proprio diritto nazionale

(Considerando 8)

Il nuovo Regolamento europeo

coordinamento normativo

Per quanto riguarda il trattamento dei dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del regolamento

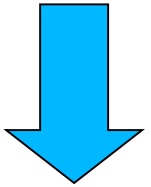
(Considerando 10)

Il nuovo Regolamento europeo

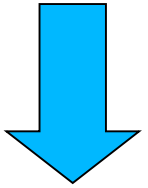
coordinamento normativo

Il Regolamento detta

la DISCIPLINA GENERALE



Normative nazionali per disciplina speciale e di settore



Valutazione di conformità

Il nuovo Regolamento europeo

coordinamento normativo

- ***Non abroga il D.lgs. n. 196 del 2003***
- ***Disapplicazione di norme nazionali in contrasto con il regolamento***
- ***Applicazione di norme nazionali derogatorie (ove ammesso), integrative, speciali***

Il nuovo Regolamento europeo – Capi

- ***Disposizioni generali***
- ***Principi***
- ***Diritti dell'interessato***
- ***Titolare del trattamento e responsabile del trattamento***

Il nuovo Regolamento europeo – Capi

- ***Trasferimento di dati personali verso paesi terzi o organizzazioni internazionali***
- ***Autorità di controllo indipendenti***
- ***Cooperazione e coerenza***
- ***Mezzi di ricorso, responsabilità e sanzioni***

Il nuovo Regolamento europeo – Capi

- ***Disposizioni relative a specifiche situazioni di trattamento***
- ***Atti delegati e atti di esecuzione***
- ***Disposizioni finali***

Il nuovo Regolamento europeo

AMBITO DI APPLICAZIONE MATERIALE

- ***Si applica solo al trattamento di dati personali di persone fisiche***
- ***Riguarda trattamenti interamente o parzialmente automatizzati o non automatizzati se i dati personali sono contenuti in un archivio o sono destinati a confluirvi***

Il nuovo Regolamento europeo

ambito di applicazione materiale

NON SI APPLICA ai trattamenti:

- ***effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico***
- ***di informazioni anonime o dati personali anonimizzati***

Il nuovo Regolamento europeo

ambito di applicazione materiale

NON SI APPLICA ai trattamenti:

- ***per attività che non rientrano nel diritto dell'Unione (es. sicurezza nazionale)***
- ***per attività di speciale rilevanza pubblica (es. politica estera e di difesa comune)***
- ***effettuati da autorità ai fini di prevenzione, accertamento e repressione reati e ai fini di sicurezza pubblica***

Il nuovo Regolamento europeo
AMBITO DI APPLICAZIONE MATERIALE

Caratteristica saliente del nuovo Regolamento:

La disciplina si applica **«indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»** e stabilisce l'applicazione delle sue regole a Titolari e Responsabili non stabiliti nell'Unione Europea che trattino dati personali di persone fisiche che si trovino nell'UE.

La direttiva 95/46 preveda l'applicazione della normativa quando il trattamento di dati è effettuato nel contesto delle attività di uno stabilimento del titolare situato nell'Unione.

Il nuovo Regolamento europeo
AMBITO DI APPLICAZIONE MATERIALE

Il Codice della Privacy si è adeguato a questo principio e prevedeva che le norme del codice si applicassero al «trattamento di dati personali, anche detenuti all'estero, **effettuato da chiunque è stabilito nel territorio dello Stato** o in luogo soggetto alla sovranità dello Stato»

Con il nuovo Regolamento la tutela è estesa a coloro che si trovino nell'Unione indipendentemente dal luogo in cui il trattamento sia effettuato

EXTRATERRITORIALITA' DEL REGOLAMENTO

Le principali novità

del nuovo Regolamento europeo

Novità del regolamento europeo

DEFINIZIONI art. 4

- ***DATO PERSONALE: qualsiasi informazione riguardante una persona fisica identificata o identificabile***

CONCETTO DI IDENTIFICABILITÀ

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 uno più elementi caratteristici della sua identità fisica, genetica, psichica, economica, culturale o sociale*

Novità del regolamento europeo

DEFINIZIONI art. 4

Non vi è la definizione di DATI SENSIBILI E GIUDIZIARI

CATEGORIE PARTICOLARI DI DATI

- ***Dati genetici***
- ***Dati relativi alla salute = dati sanitari (Considerando 35)***
- ***Dati biometrici***

Novità del regolamento europeo

DEFINIZIONI art. 4

CATEGORIE PARTICOLARI DI DATI

- ***DATI GENETICI: «dati relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscano informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione»***

Novità del regolamento europeo

DEFINIZIONI art. 4

CATEGORIE PARTICOLARI DI DATI

- ***DATI BIOMETRICI:** «dati personali ottenuti da un trattamento specifico relativi alla caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici»*

Novità del regolamento europeo

DEFINIZIONI art. 4

CATEGORIE PARTICOLARI DI DATI

- ***DATI RELATIVI ALLA SALUTE: «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute»***

Novità del regolamento europeo

DEFINIZIONI art. 4

TRATTAMENTO

«Qualsiasi operazione o insieme di operazioni, compiute ***con o senza l'ausilio di processi automatizzati*** *e* ***applicate a dati personali o insieme 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»***

Novità del regolamento europeo

DEFINIZIONI art 4

- ***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, per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economia, la salute, le preferenze personali, gli interessi, il comportamento, l'ubicazione e gli spostamenti di detta persona fisica*

Novità del regolamento europeo

DEFINIZIONI art. 4

- ***PSEUDONIMIZZAZIONE:*** *il trattamento di dati personali in modo che tali dati non possano più essere attribuiti ad un interessato senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni 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***

Novità del regolamento europeo

DEFINIZIONI art. 4

*Con **PSEUDONIMIZZAZIONE** si intende una metodologia finalizzata ad «allontanare» il dato dalla persona a cui si riferisce.*

Contestualmente, il legame tra il dato e la persona deve essere mantenuto. La pseudonimizzazione è ottenuta mediante la cifratura dei dati o la crittografia.

Novità del regolamento europeo

DEFINIZIONI art. 4

- ***PSEUDONIMIZZAZIONE:*** *è una tecnica che consiste nel conservare i dati e le informazioni dell'utente in una forma che impedisca l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive*

DEFINIZIONI art. 4

RESPONSABILE DEL TRATTAMENTO*: la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento*

DEFINIZIONI art. 4

TITOLARE DEL TRATTAMENTO: *la persona fisica o giuridica, l'autorità pubblica o altro organismo che determina le finalità e i mezzi del trattamento di dati personali*

Novità del regolamento europeo

DEFINIZIONI

- ***CONSENSO:*** *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile (non vale il silenzio assenso) che i dati personali che lo riguardano siano oggetto di trattamento*

Principi

- ***Liceità***
- ***Correttezza***
- ***Trasparenza – sensibilizzazione dei cittadini***
- ***Finalità determinate, esplicite e legittime***

Novità del regolamento europeo

Principi

LICEITA' DEL TRATTAMENTO

Il trattamento è lecito se ricorrono una delle seguenti condizioni:

- ***l'interessato ha espresso il consenso;***
- ***il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte;***
- ***Il trattamento è necessario per adempiere un obbligo legale;***
- ***Il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato;***

Novità del regolamento europeo

Principi

LICEITA' DEL TRATTAMENTO

Il trattamento è lecito se ricorrono una delle seguenti condizioni:

- ***Il trattamento è necessario per l'esecuzione di un compito di un interesse pubblico;***
- ***il trattamento è necessario per il perseguimento di un legittimo interesse del titolare del trattamento o di terzi a condizione che non prevalgano gli interessi, i diritti e le libertà fondamentali dell'interessato in particolare se minore.***

Principi

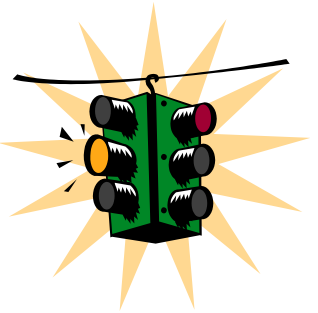
- ***Minimizzazione – pertinenza e non eccedenza***

(Privacy by design – privacy by default)

- ***Esattezza***
- ***Limitazione delle conservazione***
- ***Integrità e sicurezza***

Novità del regolamento europeo

Principi



- ***Responsabilizzazione***
- ***Neutralità degli strumenti***

Liceità del trattamento

Ogni trattamento deve trovare fondamento in <u>un'idonea base giuridica</u>

(art. 6 Regolamento)

consenso

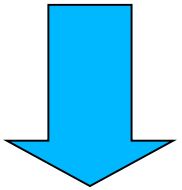
adempimento obblighi contrattuali

interessi vitali della persona interessata o di terzi

Liceità del trattamento

Ogni trattamento deve trovare fondamento in un'idonea base giuridica

(art. 6 Regolamento)



obblighi di legge cui è soggetto il titolare

interesse pubblico o esercizio di pubblici poteri

interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati

Liceità del trattamento

CONSENSO

- ***Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato abbia prestato il proprio consenso al trattamento dei dati personali***

  Il consenso dei minori è valido a partire dai 16 anni; prima di tale età occorre raccogliere il consenso del titolare della responsabilità genitoriale.

  Gli Stati membri possono per legge stabilire un'età diversa purché non inferiore a 13 anni --- Il D.lgs. 101/2018 ha portato a 14 anni l'età minima per esprimere il consenso

Liceità del trattamento

CONSENSO

- ***deve essere libero, specifico, informato e <u>inequivocabile</u> e non è ammesso il consenso tacito o presunto***

- ***deve essere manifestato attraverso "dichiarazione o azione <u>positiva inequivocabile"</u>***

(considerando 39 e 42)

Liceità del trattamento

Trattamento di categorie particolari di dati personali

Principio

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

(art. 9 regolamento)

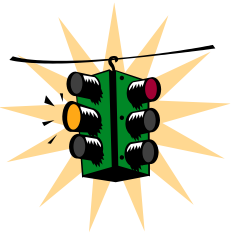
Liceità del trattamento

Il divieto non si applica nei seguenti casi

- ***Consenso esplicito***
- ***Obblighi e diritti in materia di lavoro***
- ***Per tutelare un interesse vitale dell'interessato e quest'ultimo sia nell'incapacità di manifestare il proprio consenso***
- ***Il trattamento è effettuato nell'ambito delle sue legittime attività da una fondazione, associazione o organismo senza scopo di lucro***
- ***Il trattamento è necessario per esercitare o difendere un diritto in sede giudiziaria***
- ***Il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica (gravi minacce alla salute)***

(art. 9 regolamento)

Liceità del trattamento



Trattamento di categorie particolari di dati personali

***Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stato membri**, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato*

(art. 9 e 10 regolamento)

Informativa (art. 13 e 14 Regolamento)

Tipologie di informativa

- ***<u>Informativa diretta</u>: in occasione della raccolta diretta dei dati presso l'interessato***

- ***<u>Informativa ulteriore</u>: in occasione di un mutamento della finalità rispetto ai dati già raccolti (trattamento per finalità diverse o ulteriori)***

Informativa (art. 13 e 14 Regolamento)

Tipologie di informativa

- ***<u>Informativa successiva</u>: in occasione della raccolta da altro titolare***

  NB: non è dovuta se:

- ***l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro***
- ***comunicare le informazioni risulta impossibile o implica uno sforzo sproporzionato***

Informativa (art. 13 e 14 Regolamento)

I CONTENUTI DELL'INFORMATIVA SONO PIÙ AMPI

Deve specificare:

- ***L'identità e i dati di contatto del titolare del trattamento***
- ***I dati di contatto del RPD-DPO***
- ***Le finalità***
- ***la base giuridica del trattamento***
- ***se trasferisce i dati personali in Paesi terzi e nel caso attraverso quali strumenti***
- ***il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione***
- ***Il diritto di accesso dell'interessato, di revoca del consenso nonché il diritto a proporre reclamo ad autorità di controllo***

Informativa (art. 14 Regolamento)

Nell'ipotesi in cui i dati personali non siano raccolti direttamente dall'interessato

Deve specificare:

- ***L'identità e i dati di contatto del titolare del trattamento o del suo rappresentante***
- ***I dati di contatto del RPD-DPO***
- ***Le finalità del trattamento e la base giuridica***
- ***La categoria di dati personali in questione***
- ***Eventuali destinatari o categorie di destinatari dei dati personali***

Informativa (art. 13 e 14 Regolamento)

Quando?

Nel caso di dati personali non raccolti direttamente presso l'interessato, l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione (non della registrazione) dei dati (a terzi o all'interessato)

Informativa (art. 13 e 14 Regolamento)

Come deve essere

- ***forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile***
- ***linguaggio chiaro e semplice e per i minori occorre prevedere <u>informative idonee</u>***
- ***data, in linea di principio, per iscritto e preferibilmente in formato elettronico***
- ***può essere fornita anche oralmente***

Diritti degli interessati

Diritto all'autodeterminazione

- ***Modalità per l'esercizio dei diritti***
- ***Diritti di accesso***
- ***Diritto di cancellazione (diritto all'oblio)***
- ***Diritto di limitazione del trattamento***
- ***Diritto alla portabilità dei dati***

Diritto di accesso – art. 15

Diritto dell'interessato di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e di ottenere informazioni circa:

- ***Le finalità del trattamento***
- ***Le categorie dei dati in questione***
- ***I destinatari***
- ***Il periodo di conservazione***

Diritto di accesso – art. 15

- ***Il termine per la risposta all'interessato è 1 mese, estendibili fino a 3 mesi***
- ***Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive ovvero se richieste più copie***
- ***il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità***

Diritto di accesso - art. 15

- ***Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento.***
- ***Fra le informazioni che il titolare deve fornire occorre indicare il periodo di conservazione previsto o, se non è possibile, i criteri utilizzati per definire tale periodo, nonché le garanzie applicate in caso di trasferimento dei dati verso Paesi terzi***

Diritto alla rettifica e Diritto all'oblio
art. 16 e 17

Il diritto cosiddetto "all'oblio" si configura come un ***diritto alla cancellazione*** *dei propri dati personali* ***senza ingiustificato ritardo*** *e il titolare ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali se:*

- ***I dati personali non sono più necessari rispetto alle finalità per cui sono stati raccolti;***
- ***L'interessato revoca il consenso;***
- ***L'interessato si oppone al trattamento;***
- ***I dati personali sono stati trattati illecitamente;***
- ***I dati personali devono essere cancellati per adempiere un obbligo legale;***

Diritto di cancellazione
diritto all'oblio

Non si applica se il trattamento è necessario

per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

Diritto di cancellazione
diritto all'oblio

La decisione Google Spain

Con la decisione Google Spain del 2014 la Corte di Giustizia ha formalmente esplicato la **sussistenza del diritto all'oblio** quale espressione del diritto alla privacy in riferimento a **vicende personali diffuse online e che non siano più di pubblico interesse**. *A opinione della Corte, inoltre, «i diritti fondamentali prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico ad accedere all'informazione in occasione di una ricerca concernente il nome di una determinata persona».*

Diritto di cancellazione
diritto all'oblio

Sentenze recenti

Con la sentenza n. ***13161/2016****, il Giudice della Suprema Corte hanno ulteriormente definito il diritto all'oblio in correlazione con il* ***trascorrere del tempo****.*

In definitiva i Giudici della Suprema Corte riconoscono il diritto all'oblio già dopo il trascorrere di ***due anni*** *dalla vicenda, a ribadire che la definizione dell'oblio è in effetti una questione complessa e il requisito del trascorrere del tempo non trova applicazione in ragione di un lasso di tempo predeterminabile. Di conseguenza si rende comunque necessaria la valutazione della* ***attualità della notizia e soprattutto, dell'aggiornamento della stessa****.*

Diritto alla rettifica
art. 16

***Diritto di rettifica:** L'interessato ha diritto di ottenere dal titolare del trattamento la rettifica dei dati personali che lo riguardano senza ingiustificato ritardo.*

***L'interessato** ha altresì il diritto ad ottenere l'integrazione dei dati personali incompleti anche fornendo una dichiarazione integrativa*

Diritti degli interessati

Diritto di limitazione del trattamento - art 18

- *quando il titolare ne contesti l'esattezza;*
- *il trattamento è illecito e l'interessato si oppone alla cancellazione;*
- *il titolare del trattamento non ne abbia più bisogno*

Nuovo diritto alla portabilità dei dati – art 20

l'interessato ha diritto di ricevere in formato strutturato i dati personali che lo riguardano e ha diritto di trasmettere tali dati a un altro titolare senza impedimento da parte del titolare del trattamento

Diritto di opposizione – art. 21

L'interessato ha diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano, compresa la profilazione.

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 e che prevalgono sugli interessi o diritti dell'interessato.

Se i dati trattati hanno finalità di marketing l'interessato può opporsi in ogni momento e i dati non saranno più oggetto del trattamento per tali finalità

I soggetti privacy

Titolare del trattamento – art. 24

Persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali

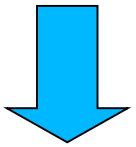
Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al presente regolamento

Responsabile del trattamento – art 28

Persona fisica o giuridica che tratta i dati personali per conto del titolare del trattamento

I soggetti privacy

Responsabile del trattamento (esterno)



Obblighi specifici distinti da quelli del titolare

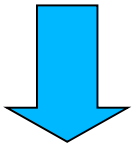
Tenuta del registro dei trattamenti

Adozione di idonee misure tecniche e organizzative per la sicurezza

Designazione RPD-DPO

I soggetti privacy

Incaricato del trattamento



Personale autorizzato al trattamento sotto l'autorità diretta del titolare o del responsabile

Obbligo di istruzione e formazione

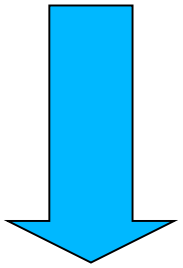
I soggetti privacy

Responsabile interno

Amministratore di sistema

Un nuovo approccio
alla gestione della privacy

Accountability



Responsabilizzazione

Un nuovo approccio alla gestione della privacy

Privacy by design

Privacy by default

Registri delle attività di trattamento

Sicurezza del trattamento

Data breach

Valutazione d'impatto privacy

Responsabile della protezione dei dati

Un nuovo approccio
alla gestione della privacy

Responsabile della protezione dei dati

Data protection officer
Art. 37 – 38 - 39

Responsabile della protezione dei dati

La figura del Data Protection Officer è presente negli Stati Uniti a partire dagli anni Novanta. Gli Stati Uniti e i Paesi anglosassoni vantano il maggior numero di responsabili per la protezione della privacy.

Responsabile della protezione dei dati

Agli inizi del Duemila il numero di ***Privacy Officer*** *assunti da aziende statunitensi aumenta rapidamente, e in egual misura ciò accade anche in Europa, soprattutto in ragione delle leggi e delle direttive sulla protezione dei dati personali che hanno previsto l'obbligo per tutte le imprese e organizzazioni di designare nel loro interno una persona incaricata della gestione della privacy*

Responsabile della protezione dei dati

Data Protection Officer in Italia

In Italia, al contrario, la figura del Privacy Officer stenta a trovare un'opportuna diffusione. Nel 2006 il presidente del Garante per la Privacy affermava che era «poco diffusa la figura del Privacy Officer, ben conosciuta invece in altri Paesi. È il segno di una certa fatica ad adeguarsi ad una visione della ***protezione dati attiva e dinamica.*** In linea generale, le imprese italiane hanno infatti inteso adeguarsi alla normativa in materia di privacy soprattutto al fine di evitare le sanzioni del Garante. Hanno quindi eseguito un **adeguamento formale**, senza il ricorso a professionisti in materia di *data protection*

Responsabile della protezione dei dati

Data Protection Officer in Italia

Si è dunque gradualmente diffusa la percezione che il Privacy Officer possa avere un ruolo importante nel contesto italiano. La designazione della figura è tuttavia rimasta facoltativa ***fino alla promulgazione del Regolamento Europeo del 2016****.*

Responsabile della protezione dei dati

Nomina obbligatoria del Data Protection Officer

Il Regolamento (UE) 2016/679 stabilisce la necessità di nominare il Responsabile del Trattamento dei Dati (RTD). In particolare, il Considerando 97 sancisce che: ***«Il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati».***

Responsabile della protezione dei dati

Art. 37 par. 1 Nomina obbligatoria nei seguenti casi:

a. *se il trattamento è svolto da **un'autorità pubblica** o da un organismo pubblico;*

b. *se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il **monitoraggio regolare e sistematico** di interessati **su larga scala**;*

c. *se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati personali o di dati relativi a **condanne penali o reati**.*

Responsabile della protezione dei dati

«monitoraggio regolare e sistematico»

Il «monitoraggio regolare e sistematico» viene definito come il monitoraggio *effettuato periodicamente o in via continuativa*: per esempio la **profilazione online**

Responsabile della protezione dei dati

«larga scala»

attività che «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 […] per le libertà e i diritti degli interessati».

Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato.

Responsabile della protezione dei dati

- *E' designato in funzione delle **qualità professionali**, in particolare della **conoscenza specialistica** della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti*

- *Può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi*

Responsabile della protezione dei dati

- *E' tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali*

- *Dispone delle risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica*

Responsabile della protezione dei dati

- *E' **"dotato di indipendenza"***
- *E' tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti*
- *Può svolgere altri compiti e funzioni purché non diano adito a un conflitto di interessi*

Responsabile della protezione dei dati - compiti

- ***informare e fornire consulenza*** *al titolare del trattamento o al responsabile del trattamento e ai dipendenti che eseguono il trattamento in merito agli obblighi privacy*
- ***sorvegliare*** *l'osservanza della normativa privacy e le 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***

Responsabile della protezione dei dati – conflitto di interessi

L'art. 38, par. 6, del Regolamento (EU) 2016/679 prevede che al RPD è consentito di «svolgere altri compiti e funzioni», ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che ***«tali compiti e funzioni non diano adito a un conflitto di interessi».***

Responsabile della protezione dei dati

Il Responsabile della protezione dei dati
NON è RESPONSABILE
in caso di inosservanza della normativa privacy

Responsabile della protezione dei dati

Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo

Approccio basato sul rischio e misure di accountability

Privacy by design

«prevenire, non correggere»

La garanzia e il rispetto del diritto alla riservatezza e alla protezione dei dati deve essere considerato valutato e attestato

sin dalla progettazione

di ogni processo e progetto e dei relativi supporti informatici tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche

Approccio basato sul rischio e misure di accountability

Privacy by default

«privacy come impostazione di default». Ciò comporta che i soggetti non debbano preoccuparsi di proteggere i propri dati poiché questi sono già protetti dal sistema.

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento

Approccio basato sul rischio e misure di accountability

Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento, allorché preveda 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

Approccio basato sul rischio e misure di accountability

Valutazione d'impatto sulla protezione dei dati

E' obbligatoria nei casi seguenti:

- *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*
- *il trattamento, su larga scala, di categorie particolari di dati personali o di dati relativi a condanne penali e a reati*
- *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico*

Approccio basato sul rischio e misure di accountability

Valutazione d'impatto sulla protezione dei dati

- *L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati*
- *L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati*

Approccio basato sul rischio e misure di accountability

Valutazione d'impatto sulla protezione dei dati

non si effettua

… qualora il trattamento trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica...”

Videosorveglianza per gli enti pubblici

Approccio basato sul rischio e misure di accountability

Consultazione preventiva dell'Autorità di controllo

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio

Registro delle attività di trattamento

Approccio basato sul rischio e misure di accountability

Ogni titolare e responsabile (esterno) del trattamento tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Il registro deve contenere le seguenti informazioni:

- ***Nome e dati di contatto del titolare, del responsabile e del DPO;***
- ***Le finalità del trattamento;***
- ***Descrizione della categoria dell'interessato;***
- ***ove applicabile, i trasferimenti di dati personali verso un paese terzo;***
- ***Termini per la cancellazione***

Approccio basato sul rischio e misure di accountability

Sicurezza del trattamento

Misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio 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

Violazione dei dati personali – Data breach

- ***Obbligo di notifica all'Autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche***
- ***Obbligo di documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio***
- ***Obbligo di comunicare la violazione all'interessato senza ingiustificato ritardo quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche***

Violazione dei dati personali – Data breach

- ***La comunicazione all'interessato deve avvenire con linguaggio semplice e chiaro e deve rilevare la natura della violazione dei dati personali.***
- ***Non è richiesta la comunicazione all'interessato se:***

- ***Il titolare ha messo in atto misure tecniche e organizzative adeguate di protezione;***
- ***Il titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato;***
- ***Detta comunicazione richiederebbe sforzi sproporzionati***

Codici di condotta

Certificazioni

Codici di condotta e Certificazioni art 40

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire la corretta applicazione del Regolamento.

Le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o responsabili possono elaborare codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento

Certificazione

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'istituzione di meccanismi di certificazione della protezione dei dati personali allo scopo di dimostrare la conformità al regolamento

Diritto al reclamo

Diritto al ricorso giurisdizionale

Art. 77 Diritto di proporre reclamo all'autorità di controllo

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguardi, violi il presente regolamento, ha diritto di proporre reclamo a un'autorità di controllo, nello Stato membro in cui risiede abitualmente, lavora oppure del luogo della presunta violazione

Art. 78 Diritto a un ricorso giurisdizionale

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale, la persona fisica o giuridica ha il diritto di proporre un ricorso giurisdizionale effettivo avverso una decisione giuridicamente vincolante dell'autorità di controllo che la riguarda

Diritto al risarcimento del danno

Chiunque subisca un danno materiale o immateriale causato da una violazione della privacy ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento

Diritto al risarcimento del danno

- ***Il titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il regolamento***
- ***Il responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento***
- ***Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile***

Diritto al risarcimento del danno

Danno patrimoniale: danno emergente e lucro cessante

Il danno emergente *corrisponde al* ***pregiudizio attuale****, ovverosia alla diminuzione patrimoniale o alla perdita economica che il danneggiato subisce.*

Il lucro cessante *si identifica nel* ***mancato guadagno*** *del danneggiato, relativamente, per esempio all'inadempimento del contratto.*

Diritto al risarcimento del danno

Danno non patrimoniale: art. 2059 c.c. - danno alla persona e lesione dei diritti della personalità

Le categorie di danno non patrimoniale sono: biologico, morale, esistenziale

La definizione di danno biologico si compone, dunque, di un elemento di natura psico-fisico e di un elemento che influisce sulle attività di relazione del soggetto

Danno biologico

Il danno biologico si compone, di un elemento di **natura psico-fisico** e di un **elemento che influisce sulle attività di relazione del soggetto**

Danno morale

Il **danno morale** è la sofferenza soggettiva cagionata da fatto illecito e in sé considerato, di regola un reato, come una forma di sofferenza che può essere sia di natura transitoria sia di natura permanente.

Danno esistenziale

Il danno esistenziale è individuato in qualsiasi ***compromissione delle attività realizzatrici della persona umana,*** *quale ad esempio la* ***lesione della serenità familiare, o del godimento di un ambiente salubre****. Il danno esistenziale si distingue dal danno biologico perché* ***non presuppone l'esistenza di una lesione fisica****, e si distingue da quello morale perché* ***non costituisce una sofferenza di tipo soggettivo***

Sanzioni e Rimedi

Comitato europeo per la protezione dei dati – art 68 è un organismo dotato di personalità giuridica. Tra i compiti vi è quello di consigliare la Commissione in merito la questione della protezione dei dati personali nell'UE. Ha inoltre il compito di pubblicare:

- ***Linee guida,***
- ***Raccomandazioni,***
- ***Best practices al fine di promuovere l'applicazione coerente del Regolamento***

Sanzioni e Rimedi

Sportello Unico relativamente ai Titolari del trattamento che si trovino ad operare in differenti Paesi dell'Unione.

I titolari dovranno confrontarsi esclusivamente con l'autorità del Paese dove hanno la sede principale, piuttosto che le autorità di tutti gli Stati membri

Sanzioni art 83 e 84

Le sanzioni penali restano di esclusiva competenza degli Stati membri

Sanzioni amministrative:

- natura, gravità e durata della violazione;

- carattere doloso o colposo della stessa;

- misure adottate dal Titolare o dal Responsabile per attenuare il danno subito dagli interessati;

- livello di cooperazione con l'autorità di vigilanza;

- benefici finanziari ottenuti

Sanzioni art 83 e 84

Entità delle sanzioni

Nella prima fascia vi sono le sanzioni amministrative fino a 10 milioni di euro o in caso di un impresa, fino al 2% del fatturato totale annuo dell'esercizio precedente

Nella seconda fascia le sanzioni fino a 20 milioni di euro e 4% del fatturato. Riguardano:

- ***Violazioni dei principi base del trattamento;***
- ***Violazioni diritti interessato;***
- ***Trasferimento dati a paese terzo;***
- ***Violazione di un ordine da parte dell'Autorità di controllo***

Il programma di adeguamento

che cosa dobbiamo fare?

Programma di adeguamento

Revisione e adeguamento Documento programmatico privacy

Registro dei trattamenti

Verifica e aggiornamento degli atti di nomina del personale interno

Programma di adeguamento

Redazione dei contratti e atti di individuazione dei Responsabili esterni

Designazione di un responsabile della protezione dei dati

Formazione del personale

Programma di adeguamento

Verifica servizi in contitolarità

Revisione informative sul trattamento dei dati

Definizione delle clausole contrattuali da apporre nei rapporti

Programma di adeguamento

- *Verifica dell'implementazione adeguatezza delle misure di sicurezza*
- *Valutazione in merito agli aspetti della privacy by design e della privacy by default*
- *Analisi fattispecie di valutazione di impatto privacy*
- *Misure organizzative per data breach*