UNIVERSITÀ DEGLI STUDI "MAGNA GRAECIA DI CATANZARO"
Corso di INFORMATICA GIURIDICA
DOCENTE: Avv. Prof. FABRIZIO SIGILLÒ - A.A. 2026/2027
TRATTAMENTO DEI DATI PERSONALI (REGOLAMENTO EUROPEO – GDPR)

1) INTRODUZIONE 3
2) ACCOUNTABILITY E COMPLIANCE 4
3) LA STRUTTURA DEL REGOLAMENTO 4
4) LE ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONALI 6
5) IL DESTINATARIO DELLA TUTELA DEL TRATTAMENTO DATI: LA PERSONA FISICA 8
6) DATI PERSONALI COMUNI 8
7) DATI PARTICOLARI 8
8) I SOGGETTI OBBLIGATORI DEL TRATTAMENTO DATI 9
TITOLARE DEL TRATTAMENTO 10
CONTINTOLARE 12
RESPONSABILE DEL TRATTAMENTO 13
INCARICATI DEL TRATTAMENTO 14
RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RDP OD ANCHE DPO) 14
I COMPITI DEL DPO 15
I CRITERI DI SCELTA DEL DPO 16
9) PECULIARITÀ DEL TRATTAMENTO DEI DATI 18
PRIVACY BY DEFAULT 19
PRIVACY BY DESIGN 19
10) CONSENSO ed INFORMATIVA. 19
IL CONSENSO 20
CARATTERISTICHE DEL CONSENSO 21
INTERESSE LEGITTIMO 22
11) INFORMATIVA 23
CONTENUTO MINIMO DELL'INFORMATIVA 23
12) IDENTITÀ E DATI CONTATTO DEL TITOLARE O RAPPRESENTANTE. 24
13) I DIRITTI DELL'INTERESSATO 25
ACCESSO PREVENTIVO 25
DIRITTO D'ACCESSO 26
DIRITTI DI RETTIFICAZIONE 26

DIRITTO DI LIMITAZIONE 27
CONTESTAZIONE DEL TRATTAMENTO DEI DATI 27
OPPOSIZIONE AL TRATTAMENTO DEI DATI PERSONALI 28
DIRITTO ALL’OBLIO 28
RICHIESTA DI RIMOZIONE DEI DATI E CORRISPONDENTE OBBLIGO DEL TITOLARE DI RIMOZIONE. 29
CONDIZIONI PER LA PROPOSIZIONE DELLA DOMANDA DI CANCELLAZIONE 29
14) DATA BREACH 30
ECCEZIONI ALL’OBBLIGO DI NOTIFICAZIONE 32
15) LE FORME DI TUTELA 32
TUTELA AMMINISTRATIVA 33
TUTELA GIUDIZIARIA 33
L’AZIONE RISARCITORIA 34
16) LE SANZIONI 35
LA DECISIONE 27189/2023 DELLA CORTE DI CASSAZIONE 37
L’AZIONE RISARCITORIA 39
17) IL DECRETO LEGISLATIVO 101/2018 40
18) INTELLIGENZA ARTIFICIALE E PROTEZIONE DEI DATI 41
19) La privacy che verrà: digital OMINIBUS 41

INTRODUZIONE

Il Regolamento Europeo per il trattamento dei dati personali (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) interviene nel tentativo di uniformare le regole comunitarie in materia, introducendo principi generali sganciati dal convincimento che l'osservanza degli adempimenti burocratici possano ritenersi corretta gestione del dato personale ed orientati ad una completa ed attenta valutazione delle modalità con cui quella gestione viene espletata.

Le disposizioni regolamentari abrogano quelle originariamente disposte con la Direttiva 95/46/CE (c.d. Regolamento generale sulla protezione dei dati) e divengono definitivamente operative sull'intero territorio comunitario nell'anno 2018 e, con precisione, nel ventesimo giorno successivo alla pubblicazione nella Gazzetta Ufficiale (25 maggio 2016) e quindi il **25 maggio 2018**.

La data non si riferisce all'entrata in vigore del Regolamento coincidente, in effetti, con la sua pubblicazione, in considerazione del fatto che i regolamenti UE sono immediatamente esecutivi e non richiedono cioè la successiva attività di recepimento da parte degli Stati membri.

Il termine biennale si riferisce piuttosto alla moratoria concessa agli Stati per predisporre l'adeguamento delle leggi nazionali al regolamento nei settori espressamente individuati dal Regolamento e senza con ciò escludere la possibilità che la Comunità europea potesse attivare eventuali procedure per inottemperanza nei confronti di quegli Stati che non avessero adempiuto ed applicare le conseguenti sanzioni.

L'esigenza di regolamentare le disposizioni sul trattamento dei dati personali nasce sostanzialmente dall'ampliamento, per alcuni versi incontrollato ed incontrollabile, di questo settore e che si spiega con forme sempre più pressanti, invasive e tali da imporre l'adozione di procedure unitarie e di utili forme di garanzia.

È per questo che il Regolamento introduce nuove tipologie di tutele in favore degli interessati (coloro cioè i cui dati vengono trattati) realizzando un insieme di obblighi a carico di Titolari e

Responsabili del trattamento di dati personali, chiamati – come si diceva - ad un approccio non più occasionale e, come detto, meramente burocratico ma attento alle effettive esigenze di tutela che il Regolamento persegue.

ACCOUNTABILITY E COMPLIANCE

In questo senso si colloca l'idea di spostare temporalmente i criteri di trattamento e protezione dei dati fin dalla **fase in cui quel trattamento viene ideato e progettato insieme al sistema con cui esso verrà attuato**, adottando contestualmente comportamenti che consentano di scongiurare il verificarsi di problemi di vario tipo.

Si tratta di forme di responsabilizzazione imposte in prima battuta al titolare, soggetto primario del trattamento e perciò chiamato ad un approccio conforme ai principi di **compliance** (adeguatezza alle disposizioni del Regolamento) e di ***accountability*** *(capacità di rendere conto dell'operato)* e quindi consistente non di burocratici e prestampati adempimenti ma di valutazione, eseguita in maniera dinamica, del rischio che un determinato trattamento può cagionare ai diritti ed alle le libertà degli interessati e riscontrare in tempo reale che i mezzi e gli strumenti adottati siano idonei ad evitare essi possano essere danneggiati, predisponendosi alla possibilità di dover rendere ragione di quel che è stato fatto a tal fine in punto di conformità al Regolamento.

Deve purtroppo dirsi che questo tipo di approccio non è stato immediato e neanche agevolato dalla struttura del Regolamento che differisce da quella tipica della normativa italiana.

I provvedimenti legislativi italiani contengono tradizionalmente una parte introduttiva che richiama i precedenti storici e i pareri acquisiti preliminarmente all'approvazione e pro- segue con l'elenco degli articoli da cui il provvedimento è composto.

LA STRUTTURA DEL REGOLAMENTO

Il Regolamento presenta invece una impostazione diversa e sicuramente originale in quella parte che suddivide le disposizioni **tra norma e *considerando***. Quest'ultima nasce con l'idea di

porsi quali semplici sezioni illustrative delle norme ma alla fine dei conti viene così spesso richiamata dalle norme stesse tanto da integrarsi con il Regolamento e rendere consistente l'effettiva portata delle relative disposizioni che si risolvono in 99 articoli e 173 considerando, per un totale di 272 norme, situazione che in alcuni casi danno vita a situazioni non univoche.

Esaminando i profili generali del Regolamento si ha modo di ravvisare un'attenzione maggiore a concetti quali l'informativa ed il consenso, al trattamento automatizzato dei dati personali ed alle relative limitazione, all'ampliamento dei diritti propri dell'interessato da azionare nei confronti di chi li tratta, all'individuazione di criteri rigorosi per il trasferimento dei dati al di fuori dell'Ue ed, ancora, alle forme di tutela per i casi in cui il dato venga ad essere in qualche modo indisponibile ad esempio a causa di una perdita o di una violazione (c.d. *data breach*).

Sono punti elaborati in un contesto ben diverso da quello a cui si era abituati sotto il vigore della precedente normativa nazionale (D.Lgs. 196/2003), caratterizzata dalla presenza di un sistema certamente forse più comprensibile ma non per questo percepito dal destinatario, attento a predisporre, ma in maniera standardizzata, atti e documenti utili all'acquisizione ed alla gestione dei dati personali senza quella valutazione specifica che consentisse di differenziare l'uno dall'altro dei soggetti del trattamento stesso e, più precisamente la diversità del dato che ogni singola persona porta con sè.

Nonostante la differenza tra il D. Lgs. 196/2003 (ispirato all'elencazione di norme) ed il Regolamento (ispirato invece alla formulazione di principi) non è dato rinvenire particolari novità sul piano delle definizioni che restano sostanzialmente invariate rispetto alla normativa nazionale previgente.

Anche il Regolamento (come il D.Lgs. 196/2003) individua **l'oggetto della tutela nella persona fisica** talvolta utilizzando il termine al plurale e quindi rivolgendosi a quelle ipotesi in cui più soggetti contemporaneamente possono essere oggetto della protezione dei dati (si pensi, a titolo di esempio, ad una richiesta di accesso ai documenti della P.A. che può coinvolgere la posizione del controinteressato ma anche dei controinteressati).

Permane altresì il disinteresse alla **persona giuridica** che anche il Regolamento sancisce, scrivendolo nero su bianco in quella parte dell'introduzione in cui evidenzia come "***La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale***

***è un diritto fondamentale**".*

Preliminare ad ogni approfondimento sul contenuto del Regolamento si rivela, in primo luogo, l'individuazione dell'oggetto che esso regola e cioè il trattamento dei dati personali, per esso intendendosi lo svolgimento di **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.**

LE ATTIVITÀ DI TRATTAMENTO DEI DATI PERSONALI

Variegate le azioni in cui può essere eseguito il trattamento e che comprendono quindi:

- la **raccolta** dei dati, operazione preliminare ed imprescindibile per il trattamento dei dati e che realizza l'inizio del trattamento stesso;
- la **registrazione** e cioè la memorizzazione dei dati su un qualsiasi supporto (e quindi anche la carta);
- l'**organizzazione**, ovvero la classificazione dei dati secondo un metodo prescelto;
- la **strutturazione** e cioè la distribuzione dei dati secondi schemi precisi;
- la **conservazione** preordinata a mantenere memorizzate le informazioni su un qualsiasi supporto;
- la **consultazione** intesa come lettura dei dati personali ma realizzabile anche mediante la semplice visualizzazione dei dati;
- l'**elaborazione** con cui si interviene sul dato personale modificandone la sostanza e si differisce in tal senso dall'**elaborazione** che può riguardare anche solo parte minima del dato personale;
- la **selezione** con cui si individuano i dati personali nell'ambito di gruppi di dati già memorizzati;
- l'**estrazione** con cui il dato viene estrapolato da gruppi già memorizzati;

- il **raffronto** ovvero il confronto tra dati, sia un conseguenza di elaborazione che di selezione o consultazione;
- l'**utilizzo** intesa quale definizione ed attività generica ma da svolgersi in maniera corretta;
- l'**interconnessione** e quindi un trattamento che si ottiene attraverso l'uso di diverse banche contenenti dati personali;
- il **blocco**, definizione da intendersi nel senso letterale e quindi una sospensione nell'esecuzione di trattamento (che può essere imposto da diverse ragioni);
- la **comunicazione** con cui il dato viene trasferito, ceduto, conferito ad altri che hanno quindi modo di conoscere quei dati;
- la **diffusione** che realizza la conoscenza all'esterno del dato a soggetti indeterminati, in qualunque forma e quindi anche mediante messa a disposizione o consultazione. (Pubblicazioni on line);
- la **cancellazione** che consiste nell'eliminazione di dati;
- la **distruzione** che è la definitiva eliminazione dei dati.

Ognuna di queste attività rimangono sganciate dalle modalità con cui vengono esercitate *("…con o senza l'ausilio di processi automatizzati…"*) e restano indifferenti anche al luogo in cui il trattamento viene eseguito, così come chiarito nelle disposizioni regolamentari di cui all'art. 3 ed al considerando 2 che sanciscono, per l'appunto, il **CARATTERE EXTRATERRITORIALE DEL REGOLAMENTO** estendendone la sua portata in misura indipendente dalla nazionalità e dalla residenza del titolare del dato personale e dal luogo in cui esso opera e quindi anche nel caso in cui il trattamento venga eseguito in paesi diversi dagli Stati membri.

La definizione che precede ci consente di ritenere che la tutela del dato personale assume nel Regolamento valore primario ed inderogabile se non in casi eccezionali che esso stesso individua, esentandone l'applicazione ai casi di trattamento effettuati:

- per attività sottratte al diritto dell'Unione Europea (es. sicurezza nazionale);
- dagli Stati membri in materia di politica estera e sicurezza comune;
- per attività esclusivamente personale o domestico da persona fisica;
- dall'Autorità Giudiziaria o di Polizia per il perseguimento di reati o tutela della

sicurezza pubblica.

IL DESTINATARIO DELLA TUTELA DEL TRATTAMENTO DATI: LA PERSONA FISICA

Lato attivo di questa tutela si è detto essere la persona fisica e, specificamente, il suo dato personale da intendersi come qualsiasi informazione (nome, codice fiscale, immagine, voce, impronta digitale, traffico telefonico) concernente una persona fisica identificata o identificabile, anche indirettamente, oppure informazioni riguardanti una persona la cui identità è nota o può comunque essere accertata mediante informazioni supplementari.

DATI PERSONALI COMUNI

La possibilità che la persona sia identificata od anche identificabile rende estremamente ampio l’elenco della casistica che consente di individuare un soggetto collocando tra gli elementi primari il nome, il cognome, la data di nascita od il luogo e l’indirizzo di casa ed integrandoli con quelli secondari ma non per questo irrilevanti quali l’indirizzo di posta elettronica, il numero di passaporto o quello di targa del veicolo di proprietà od anche il numero della carta di credito od ancora i suoi dati biometrici (volto, impronte digitali e, per alcuni versi, finanche la calligrafia), indirettamente suscettibili di consentire un collegamento con un soggetto rendendolo identificabile.

Lo stesso sarà identificabile anche attraverso dati apparentemente singolari quali l’indirizzo IP (una sorta di indirizzo telematico che individua a dire il vero il modem che è collegato alla rete internet e non specificamente il soggetto che sta usufruendo di quel collegamento).

La **Corte di Giustizia UE**, nelle sentenze (C-413/23; 655/23) del 4 settembre 2025, ha ad esempio chiarito l’effettiva qualificazione dell’informazione quale "dato personale", precisando che esso diventa dato personale solo se un soggetto dispone di mezzi ragionevolmente utilizzabili per identificare la persona.

DATI PARTICOLARI

L'esemplificativa e non esaustiva elencazione che precede si unisce poi ad una **tipologia particolare di dati che gli artt. 9 e 10 del Regolamento** sottopongono a trattamento speciale ritenendoli sensibili (così erano definiti nelle legislazione previgente al Regolamento). Si tratta di quei dati personali idonei a rivelare:

- l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici e biometrici (es. un gruppo di fotografie caricate online); la salute del soggetto, la sua vita sessuale o quello relativo al suo orientamento sessuale.

Particolari e sottoposti a trattamento speciale sono anche i **dati giudiziali**, ovverosia quelli che rivelano l'esistenza di provvedimenti penali suscettibili di iscrizione nel casellario giudiziale, o la qualità di indagato o imputato.

I SOGGETTI OBBLIGATORI DEL TRATTAMENTO DATI

Tutti i soggetti che a vario titolo vengono interessati o coinvolti nel trattamento dei dati personali, costituiscono il **lato attivo** del trattamento stesso e vengono definiti dettagliatamente nel Regolamento secondo una elencazione che si discosta poco e comunque solo parzialmente da quella utilizzata dal D.Lgs 196/2003.

D.LGS. 196/2003		REGOLAMENTO EUROPEO
Titolare del trattamento è, secondo la normativa vigente, la persona fisica, giuridica, p.a., qualsiasi ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati		Titolare del trattamento è individuato nella persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
Responsabile del trattamento = persona		**Responsabile del trattamento** è la persona

fisica, persona giuridica, pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.		fisica o giuridica, autorità pubblica, servizio o altro organismo **che tratta dati personali per conto del titolare del trattamento** (senza però determinare lo scopo o il mezzo).
Interessato = la persona fisica cui si riferiscono i dati personali		Interessato = 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.
Incaricati = persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile		**Incaricati**. Non sono espressamente menziona- ti nel Regolamento ma vengono individuati in relazione agli obblighi del Titolare di indicare, per l'appunto, coloro che possono trattare i dati

TITOLARE DEL TRATTAMENTO

Il **TITOLARE DEL TRATTAMENTO** è una figura costantemente presente nella regolamentazione del trattamento dei dati ed è individuata nella persona fisica o giuridica, autorità pubblica, servizio o qualunque altro organismo che, **singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali**.

In considerazione dei compiti attribuitigli si presume che il ruolo del titolare coincida con chi ha la possibilità di decidere in seno all'ente od all'azienda e viene di solito quindi individuato, per comodità, con il suo "vertice" o l'organo.

Egli non va individuato però nella persona fisica ma semmai nella sua veste di rappresentanza dell'Ente, dello Studio, dell'Amministrazione; sono questi i titolari del trattamento dei dati (e

quindi lo sarà il Ministero e non il Ministro).

In considerazione della peculiarità e delicatezza dell'incarico è elevato il livello di responsabilità ascritta al titolare del trattamento che si estende non solo all'attività svolta direttamente ma anche a quella eseguita per suo conto da altri soggetti.

Sebbene non sia richiesta una preparazione particolare del titolare (lo è perché tratta i dati ed è in grado di decidere finalità e modalità di trattamento) è scontato ritenere che personalmente o con l'ausilio di qualcuno questi debba essere consapevole di quel che sta facendo e dei modi in cui intende farlo, conformandosi certamente alle disposizioni del Regolamento ma anche predisponendosi a rendere prova del suo operato.

Egli – come detto all'inizio – non dovrà semplicemente fare ma piuttosto chiarire cosa ha fatto, perché l'ha fatto e perché ha ritenuto di farlo in conformità al Regolamento, predisponendo un libercolo, un quadernetto, un registro che possa fornire dimostrazione concreta dell'adozione e della messa in atto, da parte sua, delle misure ritenute adeguate ed efficaci in termini di garanzia nel trattamento (e cioè di ogni sua singola attività) ed in rapporto alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento, il tutto in considerazione del rischio per i diritti e le libertà delle persone fisiche.

È anche per questo che dovrà conoscere la portata dei dati che nel contesto in cui opera verranno trattati curando anche di disporre indicazioni ed istruzioni idonee a limitare (escludere sarebbe ancora meglio) danni a quel soggetto che abbiamo detto essere **l'*interessato*** (si pensi al danno che potrebbe derivare dal possesso di dati suscettibili di causare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, procedure di decifratura non autorizzata della pseudonimizzazione o qualsiasi altro danno economico o sociale significativo.

Non meno importante l'ipotesi in cui i dati attengano a quella categoria che abbiamo sopra individuato come *particolari* a cui si uniscono dati riferiti a **persone fisiche vulnerabili** (es. portatori di disabilità o minori).

Non meno dannoso potrebbe rivelarsi la disponibilità di un trattamento riguardante una

notevole quantità di dati personali e un **vasto numero di interessati** (es. ospedali).

Tutte queste eventualità costituiscono oggetto di una valutazione preventiva che il titolare dovrebbe adottare mediante politiche interne (policy) e misure che soddisfino i principi della protezione dei dati **di default e quindi fin dalla progettazione del trattamento.**
Tra esse potrebbero essere utili, ancorché dovute, la **riduzione al minimo del trattamento** dei dati personali (tratto cioè solo quel che effettivamente mi serve senza eccedere), l'elaborazione di **caratteristiche di sicurezza** o miglioramento di quelle preesistenti, il ricorso a forme di **pseudonimizzazione** dei dati personali.

Il tutto da individuarsi mediante una sorta di **ricognizione preliminare** del contesto in cui il titolare opererà concretamente e che potrà risolversi nell'adempimento alle disposizioni Regolamentari (che non casualmente prevede l'utilità di quella c.d. **DPIA**, valutazione dell'impatto collegato al trattamento dei dati, suscettibile di suggerire utili soluzioni anche nei casi in cui essa non fosse ritenuta obbligatoria per disposto di legge).

CONTINTOLARE

L'attività di titolare potrà essere svolta autonomamente ovvero, ai sensi dell'articolo 26 del Regolamento in regime di **CONTITOLARITÀ** ovverosia in compresenza di più soggetti/titolari che insieme contribuiscono a determinare le finalità e i mezzi del trattamento secondo una suddivisione di compiti e responsabilità da affidarsi ad un accordo interno che renda percepibile questa situazione soprattutto all'interessato mettendolo in grado di sapere a chi deve rivolgersi per esercitare i diritti.

Rivela in questo senso il già richiamato carattere extraterritoriale del Regolamento che si traduce nella necessità che il titolare sia presente anche nel caso in cui il trattamento venga svolto da un titolare (principale) non stabilito nell'Unione Europea che offra però beni e servizi a soggetti compresi nell'Unione e che, in questo caso, sarà tenuto a nominare un **RESPONSABILE** espressamente incaricato (anche dal responsabile eventualmente) con mandato scritto e senza con ciò spostare il livello di responsabilità generale del titolare del trattamento o del responsabile del trattamento quali mandanti del rappresentante.

RESPONSABILE DEL TRATTAMENTO

Se il titolare è destinato a trattare personalmente i dati ed allora la figura del responsabile coinciderà con quella del titolare.

Se invece decide di affidare questa attività ad un soggetto diverso da esso ed allora provvederà alla nomina del **RESPONSABILE DEL TRATTAMENTO** e cioè del **soggetto che gestisce il trattamento per conto del titolare**.
A differenza dell'incarico di titolare quella del responsabile suggerisce una maggiore attenzione nell'individuazione del soggetto prescelto poiché egli non deve essere un chicchessia ma un soggetto (persona fisica o giuridica) che presenti garanzie sufficienti in termini di **conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del GDPR**, soprattutto in tema di sicurezza del trattamento.

Auspicabile – come anche per il titolare – che le decisioni vengano adottate sulla base di codici di condotta generali applicabili ad esempio a singole categorie di operatori che svolgono l'attività di responsabile (es. codici di condotta degli avvocati o dei medici o delle aziende che sono da questi incaricati) che rendano più agevole la percezione dei compiti da svolgere e quindi fornire la prova di quel che è stato svolto.

Stante la funzione dei compiti demandati al Responsabile e la responsabilità che ne deriva (che è la stessa del titolare salvo il caso in cui riesca a dimostrare l'assoluta estraneità all'evento) il rapporto dovrebbe essere consacrato in un **atto scritto** (es. contratto, verbale del consiglio di amministrazione, delibera dell'ente) che comprenda l'argomento dell'incarico, la durata del trattamento, la natura e le finalità dello stesso, il tipo di dati personali, le categorie di interessati, i compiti e le responsabilità specifiche nel contesto del trattamento da eseguire e del relativo rischio.

Anche la funzione di Responsabile può essere in qualche modo delegata in favore di c.d. **CO RESPONSABILI** ed anche nei loro confronti però il rapporto rimarrà interno tra essi ed il delegante mentre l'interessato avrà come unico riferimento il Responsabile principale.

INCARICATI DEL TRATTAMENTO

La definizione degli incaricati a dire il vero non esiste nel Regolamento ma se ne desume la sua esistenza dall'obbligo che il titolare ha di annotare le persone che egli autorizza al trattamento dei dati (segretarie d'ufficio, praticanti di uno studio legale).

La loro presenza deve darsi per scontato in qualsiasi ambiente lavorativo ed è quindi inevitabile che contestualmente al trattamento dei dati personali vi siano incaricati di eseguire questo trattamento che agiranno sotto le disposizioni e la responsabilità del titolare.

Ecco perché la loro mancata indicazione ascrivibile al titolare e la mancata individuazione dei singoli compiti ad essi affidati, si traduce in una inosservanza alle disposizioni del Regolamento e la possibilità che da ciò derivino sanzioni.

RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RDP OD ANCHE DPO)

Tra i soggetti coinvolti nel trattamento dei dati personali vi è il **responsabile per la protezione dei dati (DPO secondo la dizione inglese Data Protection Officer)** figura invero erroneamente intesa quale nuova perché in effetti preesistente al Regolamento Europeo Privacy.
Essa era in effetti già presente nelle organizzazioni italiane più complesse ma non aveva ancora quel carattere di obbligatorietà che oggi viene prevista per alcune categorie di soggetti che gestiscono dati personali e che si uniscono a quelli indicati, per l'appunto, come **obbligatoriamente tenuti** alla sua nomina **nel caso in cui "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali**", profilo – quest'ultimo – in parte modificato dall'intervento integrativo apportato dall'art. 2 sexiesdecies del D.Lgs 101/2018 che, per quel che riguarda l'Italia, ha previsto l'obbligo anche per le autorità giudiziarie nell'esercizio delle loro attività.

Indicativamente, ma anche in maniera estremamente semplicistica, il DPO può essere qualificato come una sorta di revisore dei conti del trattamento dei dati personali destinato cioè a tenere sotto controllo, verificare e intervenire in quella materia in alcuni casi obbligatoriamente (la sua presenza è cioè necessaria pur senza che il suo contribuito sia

vincolante per il titolare o il responsabile), tutelare il titolare e il responsabile del trattamento di cui supervisiona le attività svolgendo un regolare e periodico controllo (c.d. *audit*) e una attività informativa e formativa all'interno del contesto in cui egli opera.

All'obbligatorietà in ambito pubblicistico, espressamente sancita dal Regolamento non fa riscontro un altrettanto trattamento nel **contesto privatistico** laddove il DPO è richiesto obbligatoriamente, ma in maniera forse un po' troppo generica, per lo svolgimento di particolari attività principali del titolare e del responsabile consistenti del **monitoraggio del trattamento di dati personali eseguiti su larga scala** (art. 37 co. 1 lett. b GDPR), concetto affatto chiaro, in parte assistito dal contributo interpretativo esperito dal Gruppo di lavoro dei Garanti Europei (**Working Party art. 29**), ma sostanzialmente riassunto in una elencazione esemplificativa della tipologia di attività comprese in questa tipologia di trattamento e, tra esse, **in ambito pubblicistico**, gli operatori di telecomunicazione, quelli che effettuano profilazione degli utenti per finalità di marketing comportamentale oppure per erogare premi assicurativi, quelli che tramite applicazioni informatica sono in grado di acquisire la localizzazione del soggetto o di monitorare lo stato di salute tramite dispositivi indossabili e interconnessi (c.d. wearable devices); vi rientrano ancora i c.d. *programmi di fedeltà* ed in ambito privatistico coloro che svolgono quale attività principale il trattamento di dati particolari o giudiziari su larga scala (allargandosi questo elenco a cliniche ma anche banche od assicurazioni).

Si tratta di una definizione talmente generica che è lo stesso WP29 a concludere salomonicamente suggerendo, nei casi di dubbio, la nomina di un RPD (o DPO) anche in ambito privatistico.

I COMPITI DEL DPO

Altrettanto genericamente indicati i **compiti del DPO** che non coincidono con gli ordini impartiti ai dipendenti, in considerazione della sua condizione di soggetto esterno, non subordinato ed anzi solitamente individuato al di fuori del contesto lavorativo interno al titolare od al responsabile del trattamento, da cui quindi rimane indipendente.

È il soggetto che nomina il DPO ad essere però destinatario delle attività a quest'ultimo affidate, ravvisate nel Regolamento ed integrate dal lavoro del WP29.

Esse si individuano più specificamente nella:

1) informazione e consulenza al titolare e al responsabile del trattamento nonché ai dipendenti degli obblighi derivanti dal regolamento;

2) sorveglianza sull'osservanza del regolamento e delle altre disposizioni europee o di diritto interno in materia di protezione dati;

3) sorveglianza sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e attività di controllo;

4) fornitura di pareri e sorveglianza nella redazione della Data protection impact assessment (c.d. **Dpia**)[1];

5) mantenimento di una posizione di contatto con l'Autorità Garante per la protezione dei dati personali con cui il DPO è richiesto anche a collaborare ove richiesto;

6) controllo sulla corretta documentazione di eventuali violazioni dei dati personali (c.d. Data Breach Notification Management) e tempestiva comunicazione all'Autorità di controllo (il Garante per l'appunto)[2].

I CRITERI DI SCELTA DEL DPO

Peculiarità del DPO rispetto agli altri soggetti coinvolti nel trattamento dei dati deve ritenersi l'**elevata professionalità della persona fisica o giuridica individuata per ricoprire l'incarico**.

Stante il suo diretto rapporto con il soggetto apicale che provvede alla nomina, pare ragionevole ritenere che il DPO debba avere una adeguata autorevolezza nella gerarchia dell'ente (sarebbe d'altra parte singolare pensare che un semplice dipendente possa assicurare l'indipendenza rispetto al datore di lavoro a cui è subordinato gerarchicamente così

[1] La DPIA (valutazione d'impatto sulla protezione dei dati) è una procedura preordinata a conoscere, di solito preventivamente, le caratteristiche del trattamento dei dati, valutandone la necessità e la proporzionalità, e strutturando la loro gestione con il minor rischio possibile.

[2] Di DATA BREACH e della funzione del GARANTE si parlerà in seguito nella trattazione di questo documento.

come ancora più difficile pensare che questo tipo di DPO possa imporre scelte tecnico-giuridiche al proprietario dell'azienda/titolare).

Non da ultimo deve considerarsi la possibilità che il dipendente possa essere colpito da provvedimenti disciplinari connessi alla sua veste di lavoratore e quindi impedito allo svolgimento di questa attività ma che lo stesso possa continuare a svolgere l'altra attività di DPO senza che nessuno possa opporre alcunché.

La scelta del DPO interna od esterna non modifica in ogni caso il **livello di responsabilità del DPO che resta sempre contenuto nei soli vincoli contrattuali** con l'effetto che egli non potrà essere destinatario di sanzioni disciplinari, né diretto referente delle richieste di risarcimento da parte degli interessati che pure dovessero discendere da comportamenti irregolari od illegittimi del DPO.

Anche nei casi in cui dal suo operato dovesse derivare un evento dannoso per l'interessato o per il trattamento dei dati dell'ente in cui egli opera, la responsabilità continuerà a gravare su titolare e responsabile, fatta salva l'azione di regresso[3] nei suoi confronti che i due soggetti potranno proporre nella sede più adeguata

Neanche da escludere (anzi molto frequente) lo svolgimento di attività di DPO presso diversi contesti lavorativi. In questo caso, oltre alla mancanza di conflitti tra l'uno e l'altro dei titolari che lo nominano, sarà egli a dover garantire la reperibilità con qualsiasi mezzo.

Come detto in precedenza, la delicatezza del ruolo e dei compiti di pertinenza del DPO rendono indispensabile una preventiva valutazione sull'**elevata professionalità del candidato**.

Egli deve conoscere la normativa europea ma anche quella statale del paese in cui opera, deve

[3] In maniera estremamente semplicistica, può dirsi che l'azione di regresso consiste personalmente nel sostenere gli effetti negativi di una azione proposta nei confronti del titolare o del responsabile e poi agire giudizialmente per il recupero delle somme impegnate (fermo restando l'obbligo di dimostrare che il fatto deve ascriversi al DPO

avere conoscenze progettuali ed organizzative per la gestione dei dati personali, deve avere conoscenze anche tecniche che consentano l'individuazione delle misure di sicurezza finalizzate alla tutela dei dati conformi ai requisiti di legge, assicurando, in particolare, che non abbiano a verificarsi i rischi di distruzione o perdita, anche accidentale dei dati od accessi non autorizzato o trattamenti non consentiti o non conformi alle disposizioni del Regolamento.

Deve quindi avere certamente ma anche informatiche che, ove mancanti, dovranno essere integrate dall'ausilio di entità di contorno che abbiano quelle conoscenze.

Va da ultimo precisato che il ruolo del DPO è tanto elevato da legittimare le aspirazioni espressamente precisate dal Regolamento che prevede l'agevolazione dell'attività che egli deve svolgere sia sul piano strettamente economico ma anche strutturale (uffici, collocazione logistica, supporto telematico o telefonico), con ogni inevitabile effetto sull'impegno di spesa che la nomina del DPO comporterà e che in ambito pubblicistico imporrà una annotazione specifica nei bilanci annuali mentre in quella privatistica cagionerà un investimento ulteriore da gestire adeguatamente.

PECULIARITÀ DEL TRATTAMENTO DEI DATI

Esaminati i concetti generali del dato personale ed i soggetti al cui trattamento è affidato, deve procedersi all'individuazione dei principi che guidano la possibilità di acquisire e dunque gestire un dato personale.

Vigono, in proposito, profili che hanno portata generale ma possono ritenersi fondamento del trattamento dei dati personali che potrà essere svolta per **FINALITÀ DETERMINATE, ESPLICITE e LEGITTIME** e previa acquisizione in maniera **ADEGUATA, PERTINENTE** e successiva permanenza **LIMITATA AL TEMPO NECESSARIO** (principio c.d. della **minimizzazione dei dati**).

Questi principi vengono tradotti in una terminologia anglosassone che richiede un adeguata traduzione nella lingua italiana.

Ci si riferisce alle definizioni di PRIVACY BY DEFAULT e PRIVACY BY DESIGN da ritenersi presupposto irrinunciabile per procedere al trattamento dei dati.

PRIVACY BY DEFAULT

Si intende per PRIVACY BY DEFAULT l'obbligo di assicurare il rispetto degli elementi sopra indicati sin dal momento in cui si decide di acquisire e trattare i dati personali.

PRIVACY BY DESIGN

In una con esso dovrà essere osservato il principio di PRIVACY BY DESIGN che sposta proprio alla fase iniziale la valutazione di adeguatezza delle modalità con cui i dati verranno trattati.

Per rendere più percepibile le definizioni, si pensi alla più tradizionale eventualità con cui il dato personale verrà trattato: l'uso di uno sistema elettronico.

- È in quella fase che si dovrà considerare l'adeguatezza dell'applicazione che si intenderà utilizzare alle disposizioni del Regolamento.
- È in quella fase che si dovranno progettare le misure di minimizzazione dei dati acquisiti.
- È in quella fase che si dovranno prevedere sistemi di sicurezza adeguati alla tipologia del dato trattato (e quindi virtualmente differenti l'uno dall'altro).

La privacy – insomma – deve essere incorporata nel progetto di trattamento dati personali in modo da rispettare i principi generali dettati dal Regolamento.

Il solo fatto di aver strutturato l'adeguata gestione di trattamento dei dati non comporta però la possibilità di attivare l'acquisizione di questa attività che può ritenersi assoggettato ad altro presupposto riassumibile in un concetto pratico molto semplicemente riassumibile nella possibilità che i dati possano essere trattati ma solo lecitamente e cioè perché è la legge che lo autorizza o l'interessato che acconsente".

È questa la finalità a cui sono destinate le due figure del Regolamento denominate

CONSENSO ED INFORMATIVA.

Il trattamento se non autorizzato dalla legge deve essere acconsentito dall'interessato ed il consenso presuppone che l'interessato sia a conoscenza di quel che sta facendo.

Sarà quindi lecito il trattamento quando:

- è necessario all'esecuzione di un contratto di cui l'interessato è parte (principio che si estende anche alla fase precontrattuale che sia prodromica alla prima e quindi, ad esempio, tanto l'attività giudiziale di difesa quanto quella preliminarmente chiesta al difensore in sede stragiudiziale);
- è necessario per l'adempimento di obblighi derivanti da legge, regolamento o normativa comunitaria (es. attività giornalistica). In questo caso non occorre neanche il consenso;
- è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- è necessario per il perseguimento dei legittimi interessi del titolare del trattamento o di terzi;
- è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui il titolare è investito.

IL CONSENSO

Lecito lo sarà se sarà stato acquisito **il consenso** nelle forme indicate dal regolamento che individua precise caratteristiche in proposito.

Il CONSENSO deve

- essere **specifico**, cioè legato ad una finalità precisa;
- essere **informato** ovverosia basato sulla conoscenza di informazioni (anche queste individuate dal Regolamento) da parte dell'interessato.
- essere associato all'eventualità che l'interessato ne abbia bisogno per trasferirlo ad altro trattamento e per altre finalità e quindi deve essere "**portabile**"

Si è già detto in precedenza come la possibilità di trattare un dato debba necessariamente ricondursi ad una base giuridica che la giustifichi e che potrebbe essere **predisposta dalla legge** oppure **derivante dalla manifesta volontà della parte** i cui dati debbono essere trattati (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, 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).

Particolare rilevanza assume la prestazione del **consenso** da parte dell'interessato che nella

prescrizione regolamentare deve, in linea di principio, esistere ed essere conforme alle norme.

NON deve essere necessariamente "documentato per iscritto", né è richiesta la "forma scritta", sebbene sia la forma scritta che può dare prova provata dell’esistenza e della consistenza del consenso e cioè che il consenso ci sia stato, che sia stato "esplicito" (quando richiesto in forma esplicita) e che sia stata manifestata dall’interessato (cosa che pare logico affidare allo scritto piuttosto che alla semplice dichiarazione verbale.
Esplicito il consenso deve essere, in particolare, quello dedicato al trattamento dei **dati particolari** (sensibili) individuati all’art. 9 del Regolamento od anche quello preordinato a **decisioni basate su trattamenti automatizzati** (compresa la profilazione – art. 22).

Particolare **il consenso dei minori**, valido a partire dai 16 anni (sebbene questo limite sia stato ridotto a 14 dalla normativa nazionale introdotta con il D.Lgs. 101/2018) ed altrimenti necessitante dell’intervento dei genitori o di chi ne fa le veci.

CARATTERISTICHE DEL CONSENSO

Prescindendo dalle particolarità esso dovrà comunque essere **libero, specifico, informato e inequivocabile e manifestato con "dichiarazione o azione positiva inequivocabile"** escludendo, per l’effetto, che sia regolare la manifestazione di un consenso mediante comportamento passivo (consenso **tacito o presunto** spesso presente su internet laddove la manifestazione del consenso viene predisposta con il blocco su una casella che l’utente non può in alcun modo annullare).

Il fatto che il consenso debba obbligatoriamente rispondere a queste peculiarità importerà (anche a distanza di tanti anni dall’operatività del Regolamento) una verifica preliminare necessaria che consenta di ritenere conformi i consensi acquisiti durante la vigenza del D.Lgs. 196/2003 . Si dovrà quindi verificare che esso abbia una **autonomia rispetto ad altre richieste o dichiarazioni** rivolte all'interessato e comprese in un unico modulo di adesione; che sia stato reso in maniera comprensibile, semplice, chiara (soprattutto quando riferito a minori).

Se l’acquisizione del consenso costituisce ordinaria regolamentazione della liceità del trattamento del dato personale, vengono predisposte per particolari fattispecie in cui vi è una ragione che prevale su quello del trattamento dei dati e renderebbe inutile oltre che

complessa la prestazione del consenso.

I soggetti pubblici ad esempio non devono, di regola, chiedere il consenso per il trattamento dei dati personali

Così come esso non è richiesto in altre ipotesi espressamente menzionate dal Regolamento (si è detto menzionate perché vi è la definizione ma non una immediata associazione alle fattispecie a cui la definizione si riferisce).

Si tratta, in particolare, delle ipotesi ci sui all'art. 6 e riferite ad:

- **adempimento agli obblighi contrattuali** (per un contratto di assicurazione non potrà che essere necessario fornire i dati personali);
- **realizzazione di interessi vitali della persona interessata o di terzi** (mi trovo in ospedale e un mio congiunto sta morendo, non posso perdere tempo a vedere se ho o meno il consenso ad operarlo);
- **adempimento agli obblighi di legge** a cui è soggetto il titolare (qui è la legge che ci dirà i casi in cui non serve il consenso);
- interesse pubblico o l'esercizio di pubblici poteri (pensiamo alle pubbliche amministrazioni);
- **interesse legittimo** prevalente del titolare o dei terzi cui i dati vengono comunicati.

INTERESSE LEGITTIMO

Complessivamente facili da individuare le ipotesi rientranti nell'elencazione che precede, specifico il concetto di **INTERESSE LEGITTIMO PREVALENTE DI UN TITOLARE O DI UN TERZO**.

Esso va ricondotto ad una situazione di fatto tale che renda plausibile ed inderogabile la disponibilità dei dati personali privi del preventivo consenso.

È una valutazione che dovrà essere fatta dal titolare del trattamento mediante un criterio di bilanciamento fra legittimo interesse del titolare o del terzo ed i diritti e libertà dell'interessato (quale potrebbe essere la condizione di un minore o di un portatore di disabilità) privilegiati – questi ultimi - rispetto all'interesse legittimo.

Il concetto non può ritenersi cristallizzato nella definizione del Regolamento ma integrato ed

aggiornato periodicamente. Tanto hanno ad esempio fatto le **Linee Guida EDPB 1/2024 fornendo criteri più chiari per valutare quando il legittimo interesse può costituire una base giuridica valida,** richiedendo un **bilanciamento documentato tra l'interesse del titolare e i diritti dell'interessato**.

Fondamento della prestazione del consenso si è detto essere l'esigenza che l'interessato sappia perché e per cosa sta manifestando la sua volontà e quali effetti, ma anche quali diritti conseguono a quella dichiarazione.

INFORMATIVA

Sono i dati che il titolare deve inserire nell'**INFORMATIVA**, a cui il regolamento dedica una dettagliata trattazione agli artt. 13 e 14.

Anch'essa, al pari della manifestazione del consenso risponde ad esigenze di semplificazione e chiarezza e quindi dovrà essere concisa, trasparente, intellegibile e facilmente accessibile; utilizzare un linguaggio semplice e chiaro (in particolar modo se relativa ai minori) e far perfino ricorso a rapide infografiche o icone standardizzate che riassumano graficamente il loro contenuto.

Anche in tal caso l'informativa può essere conferita in forma orale ma allo stesso modo di quel che si è detto per il consenso, essendo preordinata a precostituire una fonte di dimostrazione e quindi di prova dell'adempimento dell'osservanza delle norme del Regolamento che sono imposte al titolare, sarà opportuno dare atto per iscritto della sua presenza.

CONTENUTO MINIMO DELL'INFORMATIVA

Anche dell'informativa vi è un contenuto minimo rinvenibile nell'elencazione dei citati articoli 13 e 14 che si riferiscono a:

- ✓ finalità e modalità del trattamento;
- ✓ natura obbligatoria o facoltativa del conferimento dei dati;

✓ oggetti e categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;

✓ diritti dell'interessato;

✓ dati identificativi del titolare, se designato, del DPO;

✓ base giuridica del trattamento;

✓ eventuale utilizzo di processi decisionali automatizzati per il trattamento (es. la profilazione), la logica di questi e le conseguenze per l'interessato.

Differente la regolamentazione dei tempi in cui l'informativa deve essere fornita.
Nel caso in cui i dati siano acquisiti **direttamente presso l'interessato** gli elementi che dovrà contenere l'informativa saranno:

- NOME E CONTATTO DEL TITOLARE
- CONTATTO DEL RPD (ove necessario)
- FINALITÀ DEL TRATTAMENTO E BASE GIURIDICA (INDICAZIONE) PERSEGUIMENTO DI LEGITTIMO INTERESSE (INDICAZIONE)
- DESTINATARI EVENTUALI A CUI POTRANNO ESSE COMUNICATI O TRASMESSI I DATI INTENZIONE DI TRASMETTERE I DATI ALL'ESTERO PERIODO DI CONSERVAZIONE DEI DATI ESISTENZA DIRITTI DI CONTROLLO O LIMITAZIONE
- POSSIBILITÀ DI REVOCA POSSIBILITÀ RECLAMO
- OBBLIGATORIETÀ O FACOLTATIVITÀ DEL CONSENSO PROCESSO AUTOMATIZZATO

Nel caso in cui l'acquisizione avvenga altrove e quindi **non presso l'interessato**, i dati dovranno essere completati con l'indicazione delle **CATEGORIE DEI DATI** (es. comuni, sensibili, giudiziari)**; FONTE DEI DATI** (proprio perché non acquisiti presso l'interessato)**.**

IDENTITÀ E DATI CONTATTO DEL TITOLARE O RAPPRESENTANTE.

In relazione alle due diverse ipotesi sarà quindi necessario predisporre l'informativa contestualmente all'acquisizione dei dati personali ove sia l'interessato a fornire i dati e rimandare ad un ragionevole lasso di tempo questo adempimento nel solo nel caso in cui sia

acquisito presso terzi intendendosi come "*ragionevole*" il tempo massimo di 1 mese, oppure ALL'ATTO DELLA COMUNICAZIONE CON L'INTERESSATO od ancora ALL'ATTO DELLA COMUNICAZIONE DATI A TERZI (se il trattamento è destinato alla comunicazione).

Anche al fine di assicurare il rispetto di questa tempistica e delle altre risposte che il titolare od il responsabile dovrà rendere, sarà inevitabile adottare anche misure organizzative interne all'azienda, all'ente, allo studio, idonee a garantire il loro rispetto.

Ovviamente l'informativa deve intendersi come una **componente dinamica** e non statica degli adempimenti perché legata alle finalità del trattamento originariamente effettuato. È chiaro quindi che se le finalità del trattamento o comunque alcuni elementi importanti di esso dovessero cambiare, si renderà necessario anche l'aggiornamento dell'informativa (nel senso che si dovrà provvedere ad aggiornare l'interessato ancor prima di procedere ad un ulteriore trattamento).

I DIRITTI DELL'INTERESSATO

Tra gli immancabili elementi dell'informativa, assume ruolo fondamentale l'elencazione dei **diritti dell'interessato**.

Più volte si è detto che in sostanza l'oggetto della tutela del Regolamento sia proprio l'interessato ed I suoi dati ed è a questo scopo che sono individuate specifici diritti esperibili da questo in ogni fase del trattamento.

ACCESSO PREVENTIVO

Significativa deve intendersi, in questo senso, quella forma di **accesso preventivo** denominato che risponde ad una semplice condizione di cui l'interessato dichiara di essere a conoscenza (penso tu abbia i miei dati ti chiedo preventivamente di comunicarmi di cosa si tratta).

E' una richiesta che va proposta al titolare prima dell'eventuale ricorso al Garante (che costituisce invece una forma di tutela in sede amministrativa) e deve essere dal primo riscontrata entro il termine di un mese, salva proroga di due mesi ove necessario e previa comunicazione all'interessato.

In linea di principio la risposta è obbligatoria salvi casi che possano ritenersi come

assolutamente impedienti da parte del titolare che in questo caso dovrà però spiegare al richiedente il perché avvisandolo dell'eventualità che è comunque possibile inoltrare la medesima richiesta per vie ufficiali mediante ricorso all'Autorità Garante.

Come tutte le forme di tutela riconosciute all'interessato la procedura è esente da spese. Resta ferma la possibilità di richiedere un contributo spese per casi specifici (esempio l'interessato ogni due mesi formula la richiesta; la trasmissione richiede l'inserimento dei dati nel CD e quindi mi paghi il CD).

DIRITTO D'ACCESSO

Diverso dall'interpello (e in qualche modo preliminare ad esso) è invece il **DIRITTO D'ACCESSO** per alcuni versi similare all'analoga forma prevista per gli atti amministrativi dalla L. 241/90 ed a quella c.d. "generalizzata" di cui alla D.Lgs 97/2016. Esso consiste quindi del **diritto di avere notizia su un trattamento di dati personale e conseguirne l'accesso**.

Può ritenersi una forma di controllo sulla consistenza dei dati di cui il titolare dispone, sulla correttezza dell'acquisizione o anche sulla completezza dei dati stessi (anche al fine di chiedere correzioni o rettifiche o anche cancellazione).

Anche in questo caso la richiesta, da dirigere al titolare, è semplificata e deve essere consentita con modalità quanto più semplici possibili (ad esempio mettendo sul sito un'area riservata che ne consente la visione) che escludono accertamenti preventivi diversi dalla semplice identificazione dell'interessato (a cui potrà quindi essere richiesto di allegare all'istanza la propria carta d'identità). Non va motivata e si traduce nel conseguente obbligo del titolare di fornire copia dei dati senza onere alcuno per il richiedente e con la precisazione che se

i dati sono stai conferiti in formato elettronico anche la copia dovrà essere inviata con le stesse modalità e potrà essere opposta solo con specifico rifiuto.

Anche e soprattutto all'esito dell'accesso chiesto formalmente od informalmente l'interessato sarà in grado di conoscere quali dati ha il titolare ed esercitare, nel caso, le altre tipologie di diritto.

DIRITTI DI RETTIFICAZIONE

Tra esse quello di **RETTIFICAZIONE** che realizza di fatto uno dei tanti principi sottostanti al

trattamento dati e cioè quello che i dati siano esatti e costantemente aggiornati.

È per questo che in presenza di imprecisioni o mancanze può essere richiesto al titolare di procedere alla sua rettifica.

DIRITTO DI LIMITAZIONE

Altro diritto è quello di ottenere la **LIMITAZIONE DEL TRATTAMENTO** che prescinde, in punto di principio, dal fatto che il dato sia stato acquisito legittimamente o illegittimamente ma si riferisce all'eventualità che l'interessato intenda contrassegnare i dati per stabilire quali possono essere utilizzati e quali no.

Potrebbe essere richiesto, ad esempio, nel caso in cui si dovesse rendere necessario trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento (solo alcuni quindi e non tutti) od anche se si intende rendere i dati personali selezionati inaccessibili agli utenti od anche rimuovere temporaneamente i dati pubblicati da un sito web o migrare quei dati su un sistema separato.

Potrei aver riscontrato che alcuni dei dati non sono più necessari (perché ad esempio non sono più indispensabili all'esecuzione di un contratto) ma altri si e quindi chiedere si limitarne la disponibilità al titolare solo a parte di essi.

Potrei aver visto che i miei dati sono inesatti in parte (il numero civico ad esempio) e quindi nel tempo necessario alla modificazione di quella componente del dato non mi pare utile renderlo disponibile.

In questo caso chiedo al titolare di limitare il dato (continua ad utilizzare tutti tranne il numero civico).

CONTESTAZIONE DEL TRATTAMENTO DEI DATI

Questo diritto può coincidere anche con la **CONTESTAZIONE DEL TRATTAMENTO** in corso tra interessato e titolare in ordine alla legittimità dell'acquisizione o del trattamento del dato personale. In questo caso questa tipologia di diritto mira a garantire una limitazione nell'utilizzo di quei dati oggetto del contendere e per il periodo necessario alla decisione sulla vertenza.

In questo caso quindi l'effetto non è la cancellazione del dato ma una sua limitazione nell'utilizzo.

OPPOSIZIONE AL TRATTAMENTO DEI DATI PERSONALI

Ulteriore diritto esercitabile dall'interessato è poi quello di **OPPOSIZIONE al trattamento**. Presupposto è, in questo caso, che il dato sia stato lecitamente acquisito e che io voglia **conseguire la cessazione del suo trattamento in via permanente laddove non compatibile con le finalità del consenso** od anche **oppormi al trattamento eseguito mediante marketing diretto e/o profilazione.**

Mentre in quest'ultimo caso la richiesta non potrà essere rifiutata, nell'altro potrebbe ad essa opporsi il rilievo che i dati hanno sul piano storico o statistico.

La richiesta, ancorché semplificata secondo i criteri sopra menzionati (agevole, senza costi a carico dell'istante) **richiede però che venga motivata l'opposizione**.

DIRITTO ALL'OBLIO

Novità del Regolamento può ritenersi invece il altrimenti indicato come **DIRITTO ALL'OBLÌO**.

Il diritto non è in effetti nuovo e comunque risente dello sviluppo giurisprudenziale europeo sulla materia.

Esso si sviluppa infatti sulla base della decisione assunta dalla Corte di Giustizia Europea nota come "*caso Google Spain"* (sentenza 317 del 13/5/2014).

Il caso muoveva da un ricorso inoltrato al Garante privacy spagnolo contro un editore spagnolo di un quotidiano e contro Google (sia Spagna che sede principale) e riguardava un imprenditore che attraverso una ricerca sul motore di ricerca Google aveva reperto un precedente pignoramento eseguito ai suoi danni nel corso dell'anno 1998.

Avendo chiuso quella vicenda, pagando quanto dovuto a chi aveva eseguito il pignoramento, aveva chiesto la rimozione dei suoi dati.

Dopo l'esito negativo proposto al Garante in sede amministrativa, la richiesta, inoltrata all'Autorità giudiziaria spagnola, fu da questa rimessa proprio alla Corte di Giustizia che ha riconosciuto il diritto esercitato dall'istante di conseguire la cancellazione definitiva di dati che

non servono più ed il conseguente obbligo per i motori di ricerca di rimuovere quelle informazioni perché non pertinenti in rapporto alle finalità per cui erano all’epoca state acquisite.

Anche il concetto di diritto all'oblio non deve ritenersi come consolidato ed immodificabile, tant’è che la nostra **Corte di Cassazione con sentenza n. 14488 del 30 maggio 2025**, ha evidenziato come **il diritto alla cancellazione dei dati non sia assoluto, ma debba essere bilanciato con il diritto di cronaca e l'interesse pubblico** senza per questo abbandonare il concetto che in precedenza abbiamo visto e che, nel caso in cui i fatti di cronaca non hanno più alcuna rilevanza pubblica attuale, lascia prevalere il diritto all'oblio dell'interessato.

Oggetto del diritto può quindi dirsi la

RICHIESTA DI RIMOZIONE DEI DATI E CORRISPONDENTE OBBLIGO DEL TITOLARE DI RIMOZIONE.

La sua effettiva realizzazione si rivela però non priva di incertezze in quanto essa finisce per imporre al titolare una valutazione continua sulla sua attività, obbligandolo a controllare con periodicità che i dati in suo possesso siano ancora necessari e possano cioè essere utilizzati.

È una verifica che in caso di esito negativo impone al titolare l’obbligo di cancellare quei dati a prescindere dal fatto che ne sia stata fatta richiesta dall’interessato ed il suo comportamento in questo senso potrà essere considerato positivamente nell’ottica della corretta osservanza del principio di responsabilizzazione che si è detto permea l’intero Regolamento.

CONDIZIONI PER LA PROPOSIZIONE DELLA DOMANDA DI CANCELLAZIONE

possono ritenersi:

- il fatto che i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- il fatto che l'interessato revoca il consenso su cui si basa il trattamento e non vi è altro legittimo motivo per il trattamento;
- l’ipotesi in cui l'interessato si oppone al trattamento e non vi è altro legittimo motivo per il trattamento;
- l’eventualità che i dati personali siano stati trattati illecitamente;

- l'esito positivo della procedura di opposizione al trattamento;
- l'obbligo alla cancellazione derivante da un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
- il fatto che i dati personali siano stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Le modalità sono evidentemente le solite e la cancellazione così come eseguita deve ritenersi **definitiva** nel senso che se pure intratterrò nuovi rapporti con lo stesso soggetto dovrà nuovamente acquisire il suo consenso in quanto quelli precedenti devono intendersi definitivamente spariti.

Per alcuni versi correlata alla possibilità di esercitare i diritti è l'effetto pregiudizievole riconducibile alla mancata conformità alle disposizioni del Regolamento, con esso intendendosi non solo l'irregolare acquisizione o trattamento del dato personale ma anche il verificarsi di quelle vicende che potremmo definire "patologiche" che possono verificarsi durante ogni fase del trattamento.

In questo senso il regolamento prevede, tra gli adempimenti del titolare una previsione che assume carattere di novità rispetto alla precedente legislazione.

DATA BREACH

Ci si riferisce all'ipotesi di VIOLAZIONE DEI DATI (c.d. data breach), ovverosia al caso in cui il dato, per una serie di variegati motivi, risulti non più utilizzabile, disperso o reso disponibile a soggetti non autorizzati.

L'accaduto non deve ritenersi legato alla sola e ben nota ipotesi di violazione degli strumenti elettronici (attacchi esterni od anche virus o malware che infetta il computer) ma anche a circostanze ordinarie non necessariamente connesse all'attività di gestione dei dati personali.

Si pensi all'ipotesi di un allagamento nell'uffici che rende inaccessibili ed illeggibili i dati contenuti nei fascicoli di carta od anche al furto di una borsa contenente dati personali od ancora al suo semplice smarrimento.

La fattispecie non è preordinata a spiegare l'intervento necessario nei casi di violazione dati ma piuttosto a sollecitare alla massima attenzione il titolare o il responsabile evitando di sottovalutare la delicatezza del compito svolto e la possibilità che semplici eventi (es. la perdita di una pen disc contenente dati personali) possano essere disastrosi.

L'ipotesi in cui ciò si verifichi importa un obbligo di una forma di autodenuncia che consiste nell'informazione da dirigere all'**Autorità di controllo (il Garante)**.

Può definirsi forma di autodenuncia in quanto la notificazione e l'accertamento delle cause potrebbe risolversi nell'accertamento successivo sull'effettiva osservanza delle disposizioni di Regolamento da parte del titolare e sulla responsabilizzazione dello stesso nell'attuazione delle misure adeguate ad evitare che il fatto potesse realizzarsi.

E' un profilo che rimanda quindi alle modalità con cui si è proceduto alla valutazione del rischio che il titolare avrebbe dovuto eseguire prima di procedere al trattamento e che dovrà essere valutata anche in relazione ad alcuni profili aspetti del tipo di trattamento ma anche e soprattutto degli effetti provocati dal data breach che potranno essere di maggiore o minore rilevanza in considerazione alla tipologia dell'attività eseguita dal titolare, dal numero e grado di sensibilità dei dati personali violati (più o meno particolari e necessitanti di maggiore tutela); dalla maggiore o minore facilità di associare i dati violati con una persona fisica (es. se io scelgo di contrassegnare i fascicoli dello studio con un numero piuttosto che con nome e cognome l'individuazione potrebbe risultare più difficile o anche impossibile); dalla gravità delle conseguenze per gli interessati: dal numero degli interessati esposti al rischio (ho reso accessibili i dati a tutti i miei dipendenti a solo a quelli che curano quel particolare settore della materia ?) ed anche dalle caratteristiche del titolare del trattamento (uno è se si tratta di un piccolo studiolo che pure è tenuto all'osservanza del Regolamento, altro se si tratta di una grande azienda che avrebbe potuto adeguarsi in maniera più completa per evitare il verificarsi e l'eventuale danno).

Tutte queste valutazioni saranno riscontrabili nell'apposito registro su cui l'evento dannoso dovrà essere annotato ed a cui farà seguito la pressoché contestuale notificazione **all'Autorità**, contenente informazioni utili a descrivere la natura della violazione dei dati personali ed a fornire elementi per valutarne la consistenza (ad esempio i dati di contatto del responsabile

della protezione dei dati o di altro punto di contatto presso cui ottenere maggiori notizie; le probabili conseguenze della violazione; la descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio in futuro od anche per attenuarne quelli legati alla violazione verificatasi).

Nel solco del periodico aggiornamento delle disposizioni del GDPR si inserisce il Digital Omnibus che propone di allargare il termine per la notifica da 72 a 96 ore, limitandola alle sole violazioni che comportano un rischio elevato per gli interessati

ECCEZIONI ALL'OBBLIGO DI NOTIFICAZIONE

costituiscono specifiche eventualità individuate dal Regolamento e, in particolare:

- ✓ l'attuazione di adeguate misure tecniche e organizzative di protezione e la loro concreta applicazione ai dati personali oggetto della violazione (ad esempio ho perso i dati ma siccome sono cifrati non sono leggibili;
- ✓ l'aver adottato comunque misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- ✓ la ricorrenza di sforzi sproporzionati per la comunicazione;
- ✓ la possibilità di comunicare pubblicamente o individuare una misura alternativa a far sì che interessati possano comunque essere informati dell'evento.

L'intero sistema predisposto dal Regolamento prevede inevitabilmente una serie di procedimenti diretti a tutelare, a verificare, a controllare ed a sanzionare evidentemente il soggetto (titolare o responsabile) che dovesse rendersi responsabile dell'inosservanza alle disposizioni che in precedenza abbiamo esaminato.

LE FORME DI TUTELA

Le forme di tutela predisposte dal Regolamento possono differenziarsi nei due grandi gruppi amministrativa e giudiziaria. Le prime sono esperibili presso Autorità amministrative come quella istituzionalmente demandata al controllo sul trattamento dei dati (l'Autorità Garante della protezione dei dati costituita in Roma); le altre invece vengono introdotte davanti all'Autorità giudiziaria competente.

TUTELA AMMINISTRATIVA

Può essere proposta dall'interessato o da enti a cui la legge nazionale riconosce la rappresentanza (es. associazioni di consumatori) nei confronti del titolare o del responsabile del trattamento dati.
Viene indirizzata all'Autorità dello Stato in cui ha residenza l'interessato od anche a quello del luogo in cui la violazione è stata commessa.

Può essere proposta con modalità semplici ed esenti da spese e si concluderà con una decisione di cui l'Autorità dovrà dare comunicazione al richiedente ed al titolare o responsabile, entrambi abilitati a reclamare quel provvedimento anche ricorrendo all'autorità giurisdizionale (si pensi al caso in cui oltre all'accoglimento del reclamo vengano imposte anche sanzioni accessorie per il titolare o il responsabile).

L'attività amministrativa posta in essere cioè dal Garante privacy è stata in alcuni mesi molto intensa e ha condotto a elevatissime sanzioni soprattutto in campo di telemarketing illegale (800.000 euro di multa e confisca delle relative banche dati) o di uso illegittimo dell'IA, come è successo per la società Luka che gestiva la chatbot Replika (5 milioni di euro) e Open Ai che, per una illegittima gestione dei dati personali degli utenti di ChatGpt è stata punita con il pagamento di 15 milioni di euro).

TUTELA GIUDIZIARIA

Segue le regole tradizionali del ricorso all'attività giurisdizionale del paese interessato alla proposizione dell'azione e che viene individuato o nella **sede dello stabilimento del titolare** o della **residenza abituale dell'interessato**.
Valgono le stesse regole soggettive del ricorso amministrativo e quindi l'azione potrà essere **proposta dall'interessato o da enti** a cui la legge nazionale riconosce la rappresentanza (es. associazioni di consumatori) e diretta verso il **titolare od il responsabile del trattamento dati**.

Autonoma rispetto alle azioni ma in qualche modo inevitabilmente connessa ai suoi esiti è quella esperibile in sede civile e diretta a conseguire il riconoscimento di un danno e la condanna del responsabile al pagamento di una somma di denaro secondo le ordinarie regole

del processo.

Il principio fa capo alle disposizioni di cui all'art. 24 del Regolamento nella parte in cui delinea la responsabilità del titolare del trattamento, rapportandola alla natura, all'ambito di applicazione, al contesto ed alle finalità del trattamento, nonché ai rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

In relazione a questi parametri 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.

Questo onere non deve intendersi come prescrizione statica (nel senso che deve ritenersi sufficiente intervenire una tantum per l'esecuzione di queste misure) ma dinamica, imponendo quindi il riesame e l'aggiornamento qualora necessario.

L'AZIONE RISARCITORIA

Se l'inosservanza di questa norma è produttiva di danno interviene il disposto di cui all'art. 82 che così recita "Chiunque subisca un danno materiale o immateriale causato da una violazione del presente Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento".

E una disposizione che ripropone, in qualche modo, una precedente previsione normativa del D.Lgs. 196/2003 che riteneva giuridicamente pericoloso l'esercizio del trattamento dati, imponendo l'adozione di misure idonee ad evitare il prodursi di un danno di cui avrebbe dovuto dare prova – se chiamato in causa – il titolare del trattamento del dato secondo le regole previste dall'**art. 2050 cod. civ.**

Questo principio viene complessivamente riprodotto nell'**art. 82** del Regolamento che riferisce al titolare o responsabile la legittimazione passiva nel giudizio di risarcimento danni ed il diritto ad ottenere il risarcimento, esonerando quelle parti dalla responsabilità per il solo caso in cui essi siano **in grado di dimostrare che l'evento dannoso non è in alcun modo loro imputabile**.

Sul piano oggettivo le misure richieste dal D.Lgs. 196/2003 erano riferite all'obiettivo di evitare il verificarsi del danno mentre oggi esse si riferiscono all'esigenza di dar prova del

rispetto alle norme del Regolamento ed all'adeguamento alle sue disposizioni.

Sul piano **soggettivo** l'individuazione dei due soggetti interessati all'azione di risarcimento (titolare e responsabile) fa capo alla responsabilità solidale di entrambi.

Sarà il titolare ad essere obbligato a mettere in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento.

Sarà il **responsabile** a rispondere del trattamento dei dati demandatogli dal titolare.

Deve invece escludersi che possano essere direttamente coinvolti gli altri soggetti che a vario titolo sono compresi nelle procedure di trattamento dei dati personali. Tanto dicasi, ad esempio, per l'incaricato che risponderà semmai nei confronti del titolare in virtù del rapporto di lavoro di dipendenza. Altrettanto deve ritenersi per il DPO/RPD in quanto la sua responsabilità non potrà che contenersi nei limiti del rapporto contrattuale con il titolare od il responsabile che lo abbia nominato, fatta salva quindi l'eventualità che il danno sia riconducibile alla responsabilità del primo e quindi gli altri agiscano in rivalsa nei suoi confronti ma sempre al di fuori delle procedura di tutela a cui si è fatto sopra riferimento e che si svolgeranno sempre tra interessato e titolare o responsabile.

LE SANZIONI

Effetto della violazione del Regolamento sarà quindi, in prima battuta, l'applicazione delle **sanzioni** dallo stesso predisposte, che si collocano in due sezioni e prevedono la **condanna pecuniaria** fino all'importo di euro 10.000.000, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente ovvero di 20.000.000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente.

La formulazione delle norme in materia conferma quella tendenza, già richiamata in altre parti di questo documento, che vuole il Regolamento un insieme di principi più che di norme, sicuramente differente dallo schema giuridico proprio del sistema normativo italiano e suscettibile di ingenerare non secondarie incertezze sul piano pratico.

Con riferimento alle sanzioni questa preoccupante divergenza si rivela immediatamente all'occhio del lettore.

L'indicazione delle sanzioni come contenute nella norma menzionata sembrerebbe infatti priva di alcun criterio di proporzionalità (e quindi, ma solo virtualmente, potrebbe ritenersi che ogni violazione possa comportare quel tipo di sanzione), esse mancano di un valore minimo di riferimento (*fino a*… ma non anche …*a partire da*…) e non è specificato il comportamento che potrebbe ingenerare l'applicazione della sanzione (con l'effetto di ritenere che ogni e qualsivoglia violazione delle norme del Regolamento possano essere destinatarie della gravissima sanzione).

La genericità della formulazione normativa contenuta nel Regolamento finisce per violare quella finalità perseguita dal Regolamento stesso: l'uniformità di gestione della materia in ambito comunitario. È chiaro, infatti, che la mancanza di una linea guida unica potrebbe determinare che un fatto sia valutato in un certo modo in un paese europeo e diversamente in un altro.

Deve piuttosto ritenersi che l'accertamento alla condanna non porterà automaticamente all'applicazione delle sanzioni nei termini sopra indicati e men che meno che il massimo della sanzione possa discendere dalla prima violazione delle disposizioni regolamentari.

In sede interpretativa si è evidenziata pertanto l'esigenza di ritenere operativa un criterio di gradazione delle sanzioni, rapportandola alla rilevanza del fatto e che quindi, in alcuni casi, potrebbe risolversi anche solo semplicemente in un richiamo piuttosto che in una sanzione pecuniaria e che nella pratica applicazione del sistema sanzionatorio debbano adottarsi criteri quanto più equivalenti in tutti gli Stati membri.

Può comunque dirsi che la predisposizione di un sistema estremamente severo come quello sanzionatorio sopra esaminato possa contribuire a svolgere, in primo luogo, una opportuna finalità dissuasiva sebbene poi la sua concreta applicazione non potrà che essere adottata **in relazione alla natura, alla gravità e alla durata della violazione / al numero di interessati lesi / al carattere doloso o colposo della violazione / all'esistenza ed alla tipologia ed idoneità delle misure adottate per attenuare il danno / al grado di responsabilità e soprattutto alle disposizioni delle norme statali che regolano le singole fattispecie**.

Sono questi i principi che hanno guidato una recente decisione della Corte di Cassazione con cui sono stati indicati utili per la determinazione dei parametri essenziali delle sanzioni per

violazione nel trattamento dei dati personali.

LA DECISIONE 27189/2023 DELLA CORTE DI CASSAZIONE

Con una recente decisione (**ordinanza 27189 del 22/9/2023**) la Corte di cassazione ha indicato i parametri per la quantificazione delle sanzioni derivanti dall'inosservanza del Regolamento.

Oggetto dell'impugnazione era un provvedimento con cui il Garante privacy aveva indicato in 2.600.000,00 euro la sanzione ad una società che gestisce il servizio di rider e che si riteneva aver violato le disposizioni sul trattamento dati personali dei suoi dipendenti.

Il Tribunale a cui la società aveva fatto ricorso aveva annullato il provvedimento ritenendo che la sanzione era eccessiva ma senza indicarne l'ammontare perché ritenuto impossibile.

La sentenza del Tribunale è stata quindi impugnata dal Garante privacy davanti alla Corte di Cassazione che ha accolto il ricorso sancendo alcuni principi di diritto nuovi e comunque rilevanti anche in considerazione dell'affidamento che viene riservata alle decisioni della Suprema Corte soprattutto quando contengono l'interpretazione delle norme di legge.

In questo senso la Corte ha così risposto ai motivi su cui il ricorso era fondato

MOTIVO DI RICORSO	DECISIONE DELLA CASSAZIONE
La sanzione era corretta perché basata sui parametri e sugli elementi determinati dall'art. 83 del Regolamento privacy, irrogata nella misura consentita dal parametro edittale	Nel quantificare la sanzione parametro di riferimento deve essere la **rilevanza del caso concreto**. Non c'è quindi un criterio generale per stabilire l'entità della sanzione ma essa deve essere **riferita ad ogni singolo caso**. In rapporto al singolo caso quindi la sanzione, secondo le regole dell'art. 83 del GDPR, deve risultare **proporzionata** e **dissuasiva**;
	La sanzione da irrogare nel caso di

	violazione, con dolo o colpa, di una o più disposizioni del Regolamento non deve superare l'importo specificato per la violazione più grave (*e cioè fino a 10.000.000 euro o fino a 20.000.000 euro del fatturato annuo).* Il Regolamento prevede però alternativamente e per il caso di imprese un aumento della sanzione aumenta fino al 2% ovvero fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente. Questo secondo tipo di parametro rappresenta una forma di sanzione **più grave** rispetto alla sanzione pecuniaria esplicitata e **non è riduttiva** della condanna.
Il Tribunale, annullando il provvedimento perché non in grado di determinare la sanzione, aveva mancato di esaminare un fatto decisivo relativo al metodo di calcolo per quantificare la sanzione stessa	Secondo la Cassazione il giudice non poteva dire che non era in grado di quantificare la sanzione, in quanto **il giudice** di primo grado **avrebbe potuto annullare la sanzione**, **avrebbe anche potuto ridurla** se ritenuta eccessiva, ma **NON avrebbe potuto** (come ha fatto) **annullare** semplicemente il provvedimento sol perché riteneva sproporzionata la sanzione irrogata.

Nel sistema penalistico rileveranno, ad esempio, ipotesi propri di quello italiano quali la

recidiva del responsabile (ad es. quante volte è accaduto e quale il comportamento successivo ad un primo richiamo) ed il suo **pentimento operativo** (aver cercato di intervenire in qualche modo per circoscrivere danni) od anche la cooperazione con l'autorità di controllo nella fase di accertamento del fatto dannoso.

L'AZIONE RISARCITORIA

Se queste sono le sanzioni amministrative conseguenti alla violazione delle disposizioni regolamentari, non può escludersi che dalla violazione possa derivare un danno per l'interessato od anche per altri soggetti.

Nell'uno e nell'altro caso deve ritenersi che il danno prodotto possa essere quello patrimoniale (talvolta immediatamente quantificabile) ma anche non patrimoniale (che dovrà quindi essere quantificato dal giudice che conoscerà del giudizio per risarcimento danni secondo una valutazione discrezionale di cui il decidente scriverà le motivazioni nella sentenza conclusiva del processo).

Utile linea guida a tal proposito si rivela l'intervento della **Suprema Corte di Cassazione** che ha mirato ad attenuare le conseguenze a carico di chi tratta i dati personali, prevedendo che il risarcimento del danno non patrimoniale è dovuto solo nel caso in cui sia superato il livello di tollerabilità ed il pregiudizio non sia futile (così Cass. civ., sez. I, 23/05/2016, n. 10638; sez. III, 13/10/2016, n. 20615; sez. VI 11 gennaio 2016 n. 222; sez. III, sentenza 15/07/2014 n° 16133).

Il danno non patrimoniale non va cioè ritenuto *in re ipsa* per il fatto di aver prodotto danno all'interessato ma andrà va debitamente allegato e provato da chi lo invoca in tal modo riducendo in tal modo che possano prevalere le c.d. liti "bagatellari" (cause di infimo valore preordinate a conseguire condanne di altrettanto infimo valore ma che rallentano il funzionamento del sistema giustizia).

L'accertamento del danno non patrimoniale, sostiene la Cassazione, sarà di fatto rimesso al giudice del merito che dovrà quantificare il danno non solo sulla base delle prove prodotte, ma anche sulla base del contesto temporale e sociale in cui si è verificato il danno stesso.

Ultimo, ma non in ordine di importanza, l'ultima categoria di sanzioni prevista dal Regolamento riferita invero alle **violazioni non soggette a sanzioni amministrative pecuniarie (rif. art. 84 Reg.** secondo cui **"***Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione.*
Tali sanzioni devono essere effettive, proporzionate e dissuasive).

Ogni Stato è stato quindi messo in condizione di intervenire su particolari settori del regolamento in modo da personalizzarle senza ovviamente violare i principi basilari.

IL DECRETO LEGISLATIVO 101/2018

Anche l'Italia ha provveduto in tal senso comunicando alla Commissione europea, entro il termine predeterminato le modifiche apportate nella forma del **Decreto Legislativo 101/2018**.

Significativo delle problematiche che aveva ingenerato la lettura del sistema di sanzioni sopra riportato è il regime meno rigoroso predisposto per gli otto mesi successivi all'entrata in vigore del decreto.

Si è ritenuto equo invitare il Garante ad una valutazione più cauta quantomeno nella fase di prima applicazione delle disposizioni sanzionatorie, lasciandolo pur libero di svolgere ispezioni ma invitandolo anche ad essere meno rigoroso nell'irrogazione delle sanzioni amministrative, introducendo anzi un regime di sanatoria per I fatti accertati prima del decreto 101/2018.

Particolarmente importante l'introduzione nel Sistema fin qui delineato di comportamenti suscettibili di assumere rilevanza penale.

Vengono in rilievo in questo senso le disposizioni di cui agli art. 167 e seguenti del decreto in esame e che puniscono il **Trattamento illecito dei dati**; la **Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala**; l'**Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala**; la **Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante** e **l'Inosservanza dei provvedimenti dell'Autorità**.

INTELLIGENZA ARTIFICIALE E PROTEZIONE DEI DATI

L'avvento dell'intelligenza artificiale generativa ha reso necessario un coordinamento tra il GDPR e il nuovo Regolamento Europeo sull'Intelligenza Artificiale (AI Act). L'AI Act (di cui si parlerà nella successiva dispensa) che è il Regolamento sull’uso dell’IA non sostituisce il GDPR, ma è complementare ad esso e quindi i sistemi di IA che trattano dati personali devono rispettare entrambe le normative.
In questo senso si colloca ad esempio un orientamento che autorizza il trattamento dei dati basato su legittimo interesse per l’addestramento dei modelli di IA, a patto che esso sia preceduto da una valutazione d'impatto e garanzie adeguate.
Lo stesso Garante italiano, con le Linee Guida del giugno 2024, ha fornito indicazioni per prevenire il "web scraping" illecito da parte dei sistemi di IA (ovvero la pesca a strascico sulla rete per acquisire dati anche personali con cui addestrare il modello) suggerendo misure come aree riservate e clausole nei termini di servizio.
Infine il citato Digital Omnibus propone di modificare l'AI Act per consentire, a determinate condizioni, il trattamento di dati sensibili per lo sviluppo di sistemi di IA, con l'obiettivo di ridurre gli oneri amministrativi per le imprese.

LA PRIVACY CHE VERRÀ: DIGITAL OMINIBUS

A novembre 2025, la Commissione Europea ha presentato il "**Digital Omnibus**", oggetto di orientamento del Consiglio UE il 21 ottobre 2026 e contenente un pacchetto di proposte per **semplificare e armonizzare il GDPR** senza intaccarne i principi fondamentali.

Le modifiche proposte al GDPR riguardano, tra gli altri:

- la chiarificazione della nozione di dato personale in senso "relativo" (un'informazione è dato personale per un soggetto solo se questi dispone di mezzi ragionevolmente utilizzabili per identificare la persona);
- l'introduzione di una disciplina della pseudonimizzazione;

- l'introduzione di un elenco unico europeo dei trattamenti che richiedono una DPIA, in sostituzione degli elenchi nazionali;

Trova posto anche la indicazione di una **estensione del termine per la notifica dei data breach** (concetto che sarà sviluppato da qui a poco) passandolo da 72 a 96 ore.

C’è inevitabile spazio per l’intelligenza artificiale, con la facoltà di basare su "legittimo interesse" il trattamento di dati personali per l'addestramento di modelli di AI e nuove deroghe per il trattamento di dati sensibili nello sviluppo e funzionamento di sistemi di intelligenza artificiale.
Si tratta di proposte in fase di negoziazione interistituzionale e quindi non ancora vigenti ma che rivelano il carattere dinamico del GDPR e la direzione verso cui si muove il legislatore europeo in materia.