REGOLAMENTO EUROPEO

Con il regolamento europeo 2016/679 che sarà applicabile in Italia dal 25 maggio prossimo, si ha

uno spartiacque

nelle norme che regolano la protezione dei dati.

Fino ad ora al centro delle normative sulla protezione dei dati è stata posta la persona fisica, titolare di diritti, di interessi legittimi e di aspettative che l'ordinamento riconosce e tutela.

Conseguentemente a tale impostazione l'interessato, cioè il soggetto cui si riferiscono i dati personali, è sempre stato considerato il vero protagonista della normativa, il centro di imputazione dei diritti che le norme prevedono.

Ne deriva che la protezione dei dati personali è stata intesa fino ad ora come il diritto a mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata nella relazione dell'individuo con la collettività.

Questo implica una importante conseguenza:

LA TUTELA VIENE MENO SE LA VIOLAZIONE NELL'USO DEI DATI NON DETERMINA UNA LESIONE O ANCHE SOLO UNA MESSA IN PERICOLO DELL'INDIVIDUO CUI FANNO RIFERIMENTO I DATI.

Ma con l'evoluzione tecnologica tutto cambia.

I dati acquistano valore in se e vengono tutelati per ciò che sono, a prescindere, si potrebbe dire dalle persone cui si riferiscono.

Nel corso del ventennio che separa l'approvazione della direttiva 95/46 dal regolamento 2016/679 si assiste ad una rapida trasformazione che porta al centro dell'attenzione i dati, intesi, non più come proiezione dell'individuo ma come vero e proprio bene giuridico da tutelare e valorizzare. Il dato personale diventa la materia prima della nuova economia basata sulla conoscenza e sull'elaborazione delle informazioni. I dati vengono, infatti, ormai considerati un potenziale motore per lo sviluppo ed una fonte di nuovi business ad altissimo valore.

Si è, in definitiva, compreso che i dati sono destinati a diventare sempre più la materia prima che sarà alla base dei servizi e dei prodotti innovativi.

A questo proposito è illuminante un episodio verificatosi qualche anno fa.

Un' adolescente del Minnesota riceveva a casa alcuni buoni-sconto per prodotti legati alla gravidanza da una catena di negozi statunitense. Il padre della ragazza, infastidito dalla campagna promozionale, si recava nel punto vendita più vicino per protestare con il direttore, sottolineando che in quel modo si finiva per sollecitare la ragazza a restare incinta. Il responsabile del negozio si scusava con il padre della ragazza e, qualche tempo dopo, si premurava persino di richiamarlo a casa. Durante la conversazione, tuttavia,

era il padre della ragazza a scusarsi, poiché, affermava, erano successe cose di cui non si era accorto e di lì a poco sua figlia avrebbe partorito un bimbo.
Alla base di questa storia c'è una intensa e ancora rudimentale (rispetto a quanto può accadere ora) attività di profilazione predittiva, attraverso la quale una catena di negozi riesce, sulla base degli acquisti effettuati confrontati con un paniere selezionato di prodotti, a prevedere lo stato e lo stadio di gravidanza di una donna.
Più di recente, alcuni ricercatori della Università di Stanford hanno ideato un' app per raccogliere i dati esteriori delle comunicazioni telefoniche di persone che si sono prestate all'esperimento. A partire da questi metadati, gli studiosi hanno inteso verificare se, attraverso i registri telefonici disponibili in rete e le informazioni reperibili sui social network, le persone partecipanti fossero identificabili e se fosse possibile trarre informazioni personali e sensibili su di loro. La risposta è stata sorprendentemente positiva, in modo particolare per la facilità con cui è stato possibile correlare i dati ed ottenere finanche specifiche informazioni sulla condizione di salute di una quota di queste persone.
In sostanza, dunque, si è compreso che l'utilizzo ottimale e, quindi, più efficiente, delle informazioni prodotte in formato elettronico può aumentare la produttività delle aziende.
Si è inteso che è necessario assicurare che i dati personali di ogni individuo siano adeguatamente protetti per aumentare la fiducia dei consumatori nei servizi online e nelle piattaforme di e-commerce in modo particolare.
Questa premessa era doverosa e permette di comprendere meglio il significato e la portata del GDPR (acronimo di General data protection regulation)– regolamento sulla protezione dei dati di cui passeremo ad indicare i principi essenziali.

DIVERSI sono i punti essenziali della nuova disciplina:

1) **Cambiano i criteri per stabilire a chi si applicano le norme**.

Viene introdotto il principio dell'applicazione del diritto dell'Unione Europea anche ai trattamenti di dati personali non svolti nella Unione, se relativi all'offerta di beni e servizi a cittadini dell'Unione Europea o tali da comportare il monitoraggio dei loro comportamenti. In precedenza invece, si applicava la normativa del luogo in cui aveva sede il titolare del trattamento. Questo implica che social network, piattaforme web e motori di ricerca saranno assoggettati alla disciplina europea, pur avendo sede fuori dall'Unione Europea se offrono beni o servizi a cittadini dell'Unione o se monitorano i loro comportamenti.

2)**Cambiano gli obblighi a carico di chi tratta i dati: viene introdotto il nuovo principio dell'accountability ovvero della responsabilizzazione**.

Fino ad oggi gli adempimenti in materia di dati personali erano basati su criteri formali e sulla logica dell'effettivo abuso dei dati raccolti. Si era

sanzionati se gli adempimenti non erano stati applicati e se le autorità di controllo lo rilevavano e lo contestavano.
Oggi, invece, è imposto al titolare del trattamento la corretta organizzazione, documentazione e tracciabilità obbligatoria delle attività di trattamento.
Chi non organizza bene la gestione dei dati che raccoglie è punibile per questo semplice fatto, a prescindere dall'abusivo utilizzo dei dati che ne possa essere derivato o meno.
3)**Viene previsto l'obbligo di redigere il Documento di valutazione di impatto (P.I.A acronimo di Privacy Impact Assessment) ad opera del titolare quando il trattamento dei dati** presenta un rischio elevato per i diritti e le libertà delle persone fisiche.
Come indicato dal Gruppo di lavoro 29, (organo consultivo indipendente dell'Unione Europea per la protezione dei dati personali istituito in virtù della direttiva 95/46) in caso di *trattamenti valutativi* come la profilazione, di *decisioni automatizzate* che producono effetti giuridici (assunzioni, concessione di prestiti, stipula di assicurazioni, monitoraggio sistematico (videosorveglianza), *trattamento di dati sensibili, giudiziari o di natura estremamente personale* (informazioni sulle opinioni politiche); *trattamenti di dati su larga scala, dati relativi a soggetti vulnerabili (*minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani), *utilizzo di nuove soluzioni tecnologiche* (riconoscimento facciale),
è necessario effettuare una analisi dei rischi in concreto generati dal trattamento dei dati. In sostanza il titolare del trattamento dovrà effettuare, fin dal momento della progettazione del processo aziendale, una valutazione di impatto per determinare le probabilità e la gravità del rischio del trattamento sui diritti e le libertà degli interessati. Questo consentirà allo stesso di adottare le misure tecniche ed organizzative per prevenire pericoli futuri. Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo perché esprime chiaramente la responsabilizzazione del titolare. Questi infatti è tenuto non solo a garantire l'osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantisce tale osservanza e la valutazione di impatto ne è un esempio.
Detta valutazione prevede tre distinte fasi da svolgersi periodicamente con cadenza almeno annuale:
analisi dei rischi;
definizione della lista delle criticità
definizione del programma di intervento.
A questo proposito occorre sottolineare che, è opinione di molti, tale è anche quella autorevole del gruppo di lavoro articolo 29, ritenere che qualora non sia imposto dalla legge risulti quanto meno opportuno effettuare una tale valutazione ai fini di meglio comprendere ed organizzare il trattamento dei dati scongiurando i pericoli connessi.

4) Nuovi meccanismi semplificati per l'esercizio dei diritti degli interessati.

Oggi esercitare i diritti di accesso, modifica, integrazione e cancellazione dei dati personali richiede che l'interessato si attivi e superi a volte difficoltà rilevanti per formulare l'istanza verso chi ha raccolto i suoi dati.

I nuovi criteri introdotti dal regolamento europeo, invece, richiedono di prevedere modalità volte ad agevolare l'esercizio da parte dell'interessato dei suoi diritti, compresi i meccanismi per richiedere gratuitamente, in particolare, l'accesso ai dati, la loro rettifica e cancellazione e per esercitare il diritto di opposizione. Diventa onere di chi raccoglie i dati predisporre anche i mezzi per inoltrare le richieste per via elettronica, in particolare qualora i dati personali siano trattati con mezzi elettronici.

5)**Viene introdotto l'obbligo di autodenuncia da parte del titolare del trattamento per le violazioni dei dati.** (art. 33)

Per violazione dei dati personali si intende la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso in modo accidentale o illecito, ai dati personali trasmessi, memorizzati o comunque elaborati.

A fronte di tale violazione il titolare deve comunicarla al Garante entro 72 ore dal fatto ed in alcune ipotesi anche all'interessato.

Il mancato rispetto di questo obbligo comporta l'applicazione di sanzioni amministrative pecuniarie.

Alla luce di tale nuovo obbligo appare evidente che risulteranno necessari interventi significativi per scongiurare tale rischio quali possono essere software di monitoraggio (c.d. software sentinella) che segnalino immediatamente le violazioni.

6) **Altra novità rilevantissima concerne le sanzioni.**

Le sanzioni sono diventate molto più pesanti:

-fino a 20 milioni di euro per i privati e le imprese non facenti parte di gruppi

- fino al 4% del fatturato complessivo su base mondiale per i gruppi societari multinazionali.

7) **Oltre al citato principio di responsabilizzazione, altri due principi caratterizzano la nuova disciplina e sono il principio della "privacy by design"e quello della "privacy by default"**

Con l'espressione privacy by design ci si riferisce alla tutela del dato fin dalla progettazione (ne sono espressione l'obbligo di redigere la valutazione di impatto) con l'espressione **"privacy by default"** ci si riferisce all'adozione di strategie interne capaci di acquisire e gestire i dati in modo da garantire che venga continuamente rispettata la loro tutela in ossequio alle norme vigenti al fine di consentire l'eliminazione o comunque abbattere la percentuale di rischio di trattamento illecito.

8) **Altra novità riguarda l'approccio meno formalistico e più sostanziale del consenso al trattamento dei dati dell'interessato.**

E' opportuno soffermarsi con maggiore puntualità sul consenso in considerazione della sua importanza.
Ai sensi dell'art. 4 del Regolamento il consenso è "qualsiasi manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."
Ci sono dunque 4 elementi da considerare per valutare la validità del consenso.

Liberamente prestato

Come precisato dal gruppo di lavoro 29, il consenso deve rappresentare una vera scelta e deve essere sotto il controllo dell'interessato. Ne segue che qualora il consenso venga inserito come parte non negoziabile di termini e condizioni si presume che non sia stato prestato liberamente.
L'espressione ***presume*** fa intendere, comunque, che il titolare possa provare che il consenso sia stato liberamente fornito.
Gli individui devono essere in grado di rifiutare o revocare il consenso senza subire un danno. Di conseguenza, il consenso non può essere una condizione per la fornitura di un servizio se tale attività di trattamento dei dati non è necessaria per offrire il servizio. Ad esempio la raccolta di dati di geolocalizzazione per scopi pubblicitari comportamentali non può rappresentare la condizione per fornire un servizio di video editing (elaborazione di un video). Analogamente il trattamento dei dati personali per i quali viene richiesto il consenso non può diventare direttamente o indirettamente la controprestazione di un contratto che è uno scenario abbastanza frequente in relazione, ad esempio alle app gratuite.
Il concetto di libertà nella manifestazione del consenso è rilevante anche al fine di introdurre il concetto di squilibrio di potere tra il titolare e l'interessato. Non sarebbe libero il consenso prestato dal dipendente che desse il proprio consenso per evitare conseguenze negative nel caso rifiutasse.

Consenso specifico

Per garantire questo requisito è necessario che
-il titolare indichi esattamente lo scopo, come salvaguardia contro l'abuso del trattamento;
-il consenso deve essere raccolto per ogni specifica finalità del trattamento dei dati e
-informazioni specifiche devono essere fornite con ciascuna richiesta di consenso. Deve esserci, cioè, una chiara separazione delle informazioni relative all'ottenimento del consenso per il trattamento, dalle informazioni su altri argomenti.

Consenso informato

Senza informazioni accessibili gli interessati non possono prendere decisioni informate e, pertanto, il gruppo di lavoro ha identificato sei informazioni minime necessarie:
-l'identità del titolare;
-la finalità di ciascun trattamento per il quale è richiesto il consenso
-quale tipologia di dati saranno raccolti ed utilizzati
-l'esistenza del diritto di revocare il consenso
-informazioni sull'uso dei dati per decisioni automatizzate, inclusa la profilazione
-se il consenso riguarda trasferimenti al di fuori dell'Unione Europea, i dettagli circa i possibili rischi di trasferimenti di dati verso Paesi Terzi in assenza di garanzie appropriate.
Non è stato chiarito dal gruppo di lavoro se tali informazioni possano essere contenute nella informativa. Credo che ciò sia possibile. E', in ogni caso, da ricordare che la informativa debba essere facilmente comprensibile, usando un linguaggio semplice.

Indicazione univoca di volontà

Il consenso al trattamento dei dati personali deve essere fornito mediante un chiaro atto affermativo. Si considera, pertanto, non valido il silenzio o la non attività come pure il consenso manifestato attraverso caselle di attivazione selezionate preventivamente e, con i limiti innanzi precisati, i consensi forniti come parte di un contratto o di accettazione di termini e condizioni generali di un servizio.
Oltre al consenso cosiddetto ordinario il regolamento europeo richiede un **CONSENSO ESPLICITO per il trattamento di categorie speciali di dati, come quelli relativi alla salute o i dati biometrici, (sono quei dati che si ricavano dalle caratteristiche somatiche o comportamentali della persona: rientrano in tale categoria le impronte digitali, la geometria della mano e del volto, la conformazione della retina o dell'iride, il timbro e la tonalità di voce), per i trasferimenti di dati verso paesi terzi o organizzazioni internazionali in assenza di adeguate salvaguardie e per processi decisionali automatizzati, inclusa la profilazione.**
Secondo il gruppo di lavoro 29 il requisito del consenso esplicito può essere soddisfatto non solo mediante una dichiarazione scritta, ma anche compilando un modulo elettronico, inviando una email, caricando un documento scanzionato con la firma dell'individuo o utilizzando una firma elettronica. Non è escluso che una dichiarazione orale possa soddisfare i requisiti del consenso esplicito, ma secondo il gruppo di lavoro potrebbe essere difficile dimostrare che tutti i requisiti sono soddisfatti.

Come si dimostra il consenso?

E' necessario collegare il consenso ottenuto alle informazioni fornite al momento del consenso. Inoltre, il consenso ottenuto deve essere conservato

per un periodo non eccessivo ai fini del trattamento dei dati e per difendere i diritti del titolare del trattamento.
Occorre osservare che, secondo il gruppo di lavoro, non esiste un limite temporale di validità del consenso. Tuttavia se le operazioni di trattamento cambiano o si evolvono considerevolmente, allora il consenso inizialmente prestato non è più valido e deve essere ottenuto un nuovo consenso.
Ci si può chiedere in proposito: se ci si registra ad una newsletter, è possibile continuare ad inviare tale newsletter per un periodo di tempo indefinito?

Come viene ritirato il consenso?

Gli individui devono essere in grado di revocare il consenso in qualsiasi momento con la stessa facilità con cui è stato inizialmente prestato. Laddove il consenso sia ottenuto attraverso un sito web, un'app, una e-mail, le persone devono essere in grado di revocare il consenso tramite la stessa modalità gratuita e senza alcun impatto sul livello di servizio offerto.
Il ritiro del consenso non influisce sulle precedenti attività di trattamento dei dati che rimangono legittime. Tuttavia, se non esiste altra base giuridica che giustifichi la conservazione dei dati personali dopo il ritiro del consenso, i dati dovrebbero essere cancellati o resi anonimi.

INFORMATIVA (art. 13 e 14)

Anche il Regolamento Europeo 2016/679 contempla la informativa, al pari del decreto legislativo 196/2003, tuttavia non sarà più uno strumento burocratico e formale.
Il regolamento specifica molto più in dettaglio le caratteristiche dell'informativa, che deve avere ***forma concisa, trasparente, intellegibile per l'interessato e facilmente accessibile;*** occorre utilizzare un linguaggio chiaro e semplice e per i minori occorre prevedere informative idonee (si veda anche considerando 58)
L'informativa è data, in via di principio, per iscritto e preferibilmente in formato elettronico (soprattutto nel contesto di servizi online) ***anche se sono ammessi "altri mezzi"***, quindi può essere fornita anche oralmente, nei casi previsti vale a dire, su richiesta dell'interessato e purchè sia comprovata con altri mezzi l'identità dell'interessato.
Quanto ***ai contenuti*** della informativa occorre evidenziare innanzitutto la necessità che venga indicato il titolare del trattamento nonché l'eventuale rappresentante nel territorio italiano, il responsabile della protezione dei dati qualora designato, le finalità del trattamento, i diritti degli interessati (compreso il diritto alla portabilità dei dati), se esiste un responsabile del trattamento e la sua identità e quali sono i destinatari dei dati.

La informativa deve, poi, indicare ***se trasferisce i dati personali in Paesi Terzi*** e, in caso affermativo, attraverso quali strumenti.

Al fine, poi, di garantire un trattamento corretto e trasparente il Regolamento Europeo impone che l'informativa contenga ***l'indicazione del periodo di conservazione dei dati*** o i criteri seguiti per stabilire tale

periodo di conservazione ed il diritto a presentare un **RECLAMO** all'autorità di controllo. (Il reclamo *è un atto circostanziato tramite il quale si rappresenta una violazione della disciplina in materia di protezione dei dati personali. L'attività ispettiva del Garante può essere attivata d'ufficio o su segnalazione o reclamo. L'esame del reclamo è improntato a criteri di semplicità delle forme osservate, speditezza ed economicità, anche in riferimento al contraddittorio. Il reclamo viene esaminato dall'Autorità che al termine dell'istruttoria che deve concludersi entro 6 mesi o entro i 9 nei casi più complessi e può concludersi con la promozione di un provvedimento del collegio ovvero senza nelle ipotesi meno gravi come ad esempio allorquando non si ravvisa una condotta non conforme, o trattasi di condotta risalente nel tempo o che ha esaurito i suoi effetti o sono state fornite adeguate assicurazioni da parte del titolare del trattamento. Nel caso di delibere del Collegio le stesse possono imporre il divieto di trattamento dei dati relativi a singoli soggetti, fermo restando la possibilità per il Collegio di invitare, anche in contraddittorio con l'interessato ad effettuare il blocco spontaneamente*)

Nell'ipotesi in cui il trattamento comporta ***processi decisionali automatizzati*** (ivi compresa la profilazione) l'informativa deve specificarlo e deve, anche, indicare la logica di tali processi decisionali e le conseguenze previste per l'interessato.

E', importante sottolineare la necessità **che sia indicata la base giuridica del trattamento.** In proposito occorre precisare che, ai sensi dell'art. 6 del Regolamento, ci sono sei ipotesi di basi giuridiche idonee a legittimare un trattamento lecito:
il consenso dell'interessato, esecuzione di un contratto, obbligo di legge, salvaguardia degli interessi vitali dell'interessato , esecuzione di un pubblico interesse e legittimo interesse del titolare.

Se il trattamento è basato sui legittimi interessi non occorre il consenso dell'interessato purchè, però, non prevalgano gli interessi e le libertà fondamentali dell'interessato tenuto conto delle ragionevoli aspettative dello stesso (in special modo se questi è un minore) in base alla relazione con il titolare.
Occorre, però, informare l'interessato del fatto che i suoi dati sono trattati in base a legittimi interessi. Per l'utilizzo dei legittimi interessi quale base giuridica del trattamento occorrono, dunque, alcuni requisiti:

1) Il titolare del trattamento ha necessità di elaborare il dato per fini propri o di terzi (ad esempio, se una società finanziaria cerca un suo cliente che è in ritardo con i pagamenti, la società ha il legittimo interesse ad

ottenere il nuovo indirizzo del cliente anche in assenza del consenso specifico;

2) Occorre bilanciare gli interessi del titolare con quelli dell'interessato e quindi, il trattamento appare ingiustificato se ha degli effetti pregiudizievoli sui diritti e le libertà del singolo (è evidente, riportandoci all'esempio di prima che l'interesse del cliente a non pagare quanto dovuto non può essere ritenuto legittimo)
3) Il trattamento delle informazioni deve essere equo e rispettare i principi di protezione dei dati (quindi la società finanziaria deve garantire che i dati siano precisi, aggiornati, non eccessivi – la società ottiene solo i dati necessari allo scopo vale a dire rintracciare il cliente.)

Anche se il Regolamento con contiene un elenco tassativo dei casi di "legittimo interesse" il Considerando 47 indica alcune circostanze nelle quali possono sussistere motivi legittimi per il trattamento cioè quando esista una relazione pertinente ed appropriata tra l'interessato ed il titolare del trattamento, ad esempio quando l'interessato è un cliente o alle dipendenze del titolare del trattamento. Ovviamente non si tratta di un'autorizzazione generalizzata al trattamento dei dati, ma è sempre richiesta un'attenta valutazione al fine di verificare se i diritti dell'interessato possano prevalere sui legittimi interessi del titolare.

Tempi dell'informativa:

Normalmente i dati sono raccolti direttamente presso l'interessato. In tal caso, l'informativa deve essere fornita prima della raccolta dei dati. In caso contrario, quando cioè i dati non sono raccolti direttamente (come nell'ipotesi in cui venga inviata una proposta all'indirizzo pec estratto dal pubblico registro), l'informativa deve essere fornita entro un termine ragionevole che non può superare un mese dalla raccolta, oppure deve essere fornita al momento della comunicazione (e non dalla registrazione) dei dati a terzi o all'interessato. In tal caso l'informativa deve contenere anche la indicazione della *categoria dei dati personali* in questione.

PROCESSO DECISIONALE AUTOMATIZZATO RELATIVO ALLE PERSONE FISICHE E LA PROFILAZIONE

Particolare attenzione è stata mostrata dal Regolamento Europeo al processo decisionale automatizzato (relativo alle persone fisiche) ed alla profilazione.

Ormai un numero sempre maggiore di settori, sia pubblici che privati, utilizza lo strumento della decisione automatizzata e la profilazione.

In realtà la procedura di delineazione del profilo di un individuo e il processo decisionale automatizzato possono rivelarsi di grande utilità, attribuendo vantaggi quali l'aumento dell'efficienza nelle varie operazioni relative ai dati personali ed il risparmio di risorse.

Ma le suddette modalità di trattamento dei dati possono causare rischi significativi per l'interessato.
Per PROFILAZIONE si intende una forma automatizzata di elaborazione riguardante dati personali che ha come obiettivo quello di analizzare, valutare e soprattutto elaborare previsioni sugli aspetti personali di una persona fisica.
Per realizzare tale scopo la profilazione procede innanzitutto alla raccolta dei dati, poi, alla loro analisi automatizzata allo scopo di identificare correlazioni, infine applica ad un individuo i modelli comportamentali elaborati per identificarne le caratteristiche attuali o future.
Così facendo, ogni individuo, i cui dati sono stati trattati secondo tale metodologia, sarà inserito in una determinata categoria, la quale, al bisogno, risulterà utile per formulare previsioni su di lui, ad esempio, sulla sua capacità di eseguire una determinata attività, sui suoi comportamenti probabili, sui suoi interessi.
Nella pratica, la profilazione può essere applicata sia ad un processo in cui la decisione finale sarà sempre assunta da una persona sia ad un processo decisionale esclusivamente automatizzato.
Quanto alla **nozione di processo automatizzato** deve essere inteso come lo strumento che consente all'operatore di assumere decisioni con mezzi tecnologici senza l'intervento o il coinvolgimento umano.
Le decisioni automatizzate possono basarsi sui dati forniti direttamente dalle persone interessate (attraverso, ad esempio, un questionario), oppure sui dati ricavati da un profilo dell'individuo.
Ne deriva che le decisioni automatizzate possono essere prese anche senza ricorrere ad una tecnica di profilazione.
Definiti i suddetti concetti si rileva come il Regolamento abbia introdotto specifiche disposizioni per garantire che tali tecniche di trattamento dei dati non siano usate in modo da avere un impatto negativo e ingiustificato sui diritti degli individui.
Come si legge nel considerando 71 l'interessato dovrebbe avere il diritto di non essere sottoposto ad una decisione che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridichi che lo riguardano o incida significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito.
L'art. 22 vieta di prendere **decisioni completamente automatizzate (vale a dire, ripetesi quelle che non prevedono l'intervento dell'uomo)** che possano produrre effetti giuridici sugli interessati o, comunque, che possano incidere significativamente su di loro.
Il suddetto divieto generale subisce, tuttavia, ***alcune deroghe*** sancite sempre dall'art. 22

1)- ***E' fatta salva l'ipotesi in cui la siffatta decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato ed il titolare del trattamento*** - Sul punto il Gruppo di lavoro chiarisce che la necessità di utilizzare decisioni automatizzate per l'esecuzione o la conclusione di un contratto deve essere interpretata in modo restrittivo. Il titolare deve essere in grado di dimostrare che la decisione automatizzata è necessaria e non sono disponibili mezzi alternativi meno invasivi;
2)-***sia autorizzata dal diritto dell' Unione o dello Stato membro cui è soggetto il Titolare del trattamento***;- il Preambolo n. 71 del Regolamento 2016/679 chiarisce che la legislazione degli Stati membri può autorizzare il ricorso ad un processo decisionale automatizzato, a titolo esemplificativo, per il monitoraggio e la prevenzione di frodi e dell'evasione fiscale o per garantire la sicurezza e l'affidabilità di un servizio fornito dal titolare del trattamento.
3)***-si basi sul consenso esplicito dell'interessato.***
In tutti i casi in cui trovi applicazione una delle sopracitate eccezioni, l'art. 22 del Regolamento sancisce che debbano trovare applicazione misure adeguate tra cui il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
Attesa l'importanza dei processi in esame e le gravi conseguenze che potrebbero derivare da errori nella fase della raccolta dei dati o nel processo decisionale con eventuali classificazioni o valutazioni errate occorre adottare misure che prevedono controlli ciclici sui processi automatizzati e sui dati raccolti.
Nell'ambito delle decisioni basate unicamente su un trattamento automatizzato il Regolamento introduce la necessità che vengano fornite all'interessato maggiori informazioni sulle modalità di creazione ed utilizzo di tali processi. Gli articoli 13 e 14 sanciscono il diritto dell'interessato a conoscere l'esistenza del processo decisionale automatizzato ed in particolare di ottenere informazioni significative sulla logica utilizzata per tale processo.
In particolare, il titolare del trattamento dovrà comunicare preliminarmente all'interessato l'esistenza di un processo decisionale. Così ad esempio una banca dovrebbe essere in grado di spiegare al proprio cliente i criteri posti alla base della decisione automatizzata assunta ed il cosiddetto punteggio di credito utilizzato per valutare se accogliere o meno una richiesta di prestito.
Allo scopo, potrà essere utile rendere note all'utente le fonti da cui il titolare ha attinto i dati, quali le informazioni fornite direttamente all'interessato sul modulo di domanda, quelle ricavate dall'osservazione della sua condotta, inclusi eventuali casi di pagamenti arretrati, quelle fornite da terzi o tratte da pubblici registri.

Tutto ciò troverà compimento con la comunicazione delle informazioni del titolare all'interessato per porlo in condizione di esercitare i suoi diritti.
La ratio sottesa a tali prescrizioni del legislatore europeo è quella di portare nella sfera di conoscibilità dell'interessato i criteri assunti per raggiungere la decisione sulle conseguenze previste di tale trattamento.

Un nuovo protagonista della tutela dei dati personali: il Responsabile della protezione dei dati (Data Privacy Protection).

IL RESPONSABILE DELLA PROTEZIONE DEI DATI denominato anche DPO acronimo di Data Protection Officer.

Trattasi di una figura di particolare importanza che ha **funzioni** di supporto e controllo, consultive, formative ed informative relativamente all'applicazione del Regolamento, coopererà con l'Autorità cui, infatti, deve essere comunicato il proprio nominativo e costituisce il punto di contatto rispetto agli interessati. Si ricordi, infatti, che nella informativa deve essere indicata la presenza eventuale del Responsabile Protezione dei Dati.

Si tratta, dunque, di una figura complessa, con molte funzioni.

Quanto **ai requisiti**, come chiarito dal Garante, non è necessario che sia iscritto in appositi albi o che abbia particolari attestazioni formali, ma deve conoscere normativa e prassi e le regole dell'ambiente nel quale lavora. Deve, poi, agire in piena autonomia ed indipendenza, senza ricevere istruzioni e riferendo direttamente ai vertici ed essere dotato di un ufficio e di risorse per l'espletamento reale dei suoi compiti..

Il ruolo di Responsabile della Protezione dei Dati può essere ricoperto da un **dipendente del titolare o del responsabile non in conflitto di interessi** che conosca la realtà operativa in cui avvengono i trattamenti

Detto incarico può essere affidato anche a soggetti esterni a condizione che garantiscano l'effettivo assolvimento dei compiti che il Regolamento assegna a tale figura.

La scelta tra un Responsabile interno o esterno è rimessa alla discrezionalità del titolare

Quanto alle **modalità di nomina** *quello interno* verrà nominato attraverso uno specifico atto di designazione, *quello esterno* in base ad un contratto di servizi.

Tali atti da redigere in forma scritta dovranno indicare espressamente i compiti attribuiti, le risorse assegnate per il loro svolgimento, nonché ogni altra utile informazione in rapporto al contesto di riferimento.

In ogni caso al DPO dovrà essere garantito un adeguato supporto in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. Resta comunque chiaro che il titolare o il responsabile del trattamento che abbia designato un responsabile della protezione dei dati resta pienamente responsabile dell'osservanza della normativa in materia di trattamento dei dati e deve essere in grado di dimostrarlo.

La nomina di un DPO non solleva il titolare da alcuna responsabilità verso l'esterno.
Si discute **se il ruolo** del Responsabile Protezione dei Dati **sia compatibile** con altri incarichi. La risposta data è positiva a condizione che non sia in conflitto di interessi.
In tale prospettiva appare preferibile, nota il Garante, evitare di assegnare il ruolo di responsabile di protezione dei dati a soggetti con incarichi di alta direzione (amministratore delegato, membro del consiglio di amministrazione, direttore generale) ovvero nell'ambito di strutture aventi potere decisionale in ordine alle finalità ed alle modalità del trattamento (direzione risorse umane, direzione marketing, direzione finanziaria). Da porre particolare attenzione anche all'eventuale assegnazione di tale incarico ai responsabili delle funzioni di staff (ad esempio il responsabile della funzione legale)
Si discute, inoltre, se il Responsabile della Protezione dei Dati sia una persona fisica o possa essere anche una persona giuridica.
Il regolamento prevede, espressamente, che il DPO possa essere un dipendente del titolare o del responsabile del trattamento, quindi **una persona fisica.**
Qualora il DPO sia individuato in un soggetto esterno, quest'ultimo potrà essere **anche una persona giuridica**, ma il Garante raccomanda, in ogni caso, di procedere ad una chiara ripartizione di competenze, individuando, ad esempio, una sola persona fisica atta a fungere da punto di contatto con gli interessati e l'Autorità di Controllo.
L'aspetto, forse più spinoso, di tale figura concerne i casi in cui è obbligatorio procedere alla designazione.
Sono obbligati , ai sensi dell'art. 37, le autorità pubbliche e gli organismi pubblici. (Vi rientrano le autorità nazionali, regionali e locali). In tale categoria rientrano anche gli ordini professionali (come enti pubblici non economici)
Sono poi obbligati gli altri soggetti qualora abbiano *come attività principale* trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala o trattamenti su larga scala di particolari categorie di dati personali o dati relativi a condanne penali e reati.
Per *attività principale* si intendono le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all'attività del titolare o del responsabile. Per esempio il trattamento dei dati relativi alla salute come le cartelle sanitarie dei pazienti è da ritenersi una delle attività principali di qualsiasi ospedale.
La definizione di larga scala non è contenuta nel regolamento ma il considerando 91 fornisce delle indicazioni in proposito:

al fine di stabilire se un trattamento sia effettuato su larga scala
è opportuno tenere conto del
-numero di soggetti interessati dal trattamento in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
-il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
-la durata ovvero la persistenza dell'attività di trattamento e
-la portata geografica dell'attività di trattamento
Il garante ha fornito il 26 marzo 2018 delle indicazioni sui soggetti obbligati:
Sono obbligati gli istituti di credito, società finanziarie, sistemi di informazione creditizia, società di informazioni commerciali, società di revisione contabile, istituti di vigilanza, imprese di somministrazione di lavoro e ricerca di personale, società operanti nel settore della cura della salute, della prevenzione/diagnostica sanitaria quali ospedali privati, laboratori di analisi mediche e centri di elaborazione, società di call center, società che forniscono servizi informatici, società che erogano servizi televisivi a pagamento, partiti e movimenti politici, sindacati, caf e patronati.
I soggetti non obbligati: tra i soggetti non obbligati rientrano, come chiarito dal Garante, i liberi professionisti operanti in forma individuale, agenti, rappresentanti e mediatori operanti non su larga scala, imprese individuali o familiari, piccole e medie imprese con riferimento ai trattamenti dei dati personali connessi alla gestione corrente dei rapporti con fornitori e dipendenti.
Occorre, infine, sottolineare come sia possibile o addirittura opportuno procedere alla nomina di tale figura anche nelle ipotesi in cui non sussista un obbligo in tal senso.
In tale circostanza troveranno applicazione tutti i requisiti previsti per quanto concerne la nomina, lo status ed i compiti esattamente come nel caso di una nomina obbligatoria.