INFORMATION TECHNOLOGY LAW

DISPENSE

(Ignazio Zangara)

… … …

SEZIONE VI

LA TUTELA DELLA RISERVATEZZA E IL TRATTAMENTO DEI DATI PERSONALI NEL GDPR

INTRODUZIONE

La tutela giuridica della sfera individuale è materia di rilevanza costituzionale e riguarda la persona e i dati ad essa collegati.

Il valore assoluto della persona, della sua individualità, reale e rappresentata, conosce soltanto il limite, per il vero assai circoscritto, dell'interesse pubblico qualificato. Di norma, tutti hanno il diritto di preservare la propria sfera individuale, sulla quale nessuno può e deve esercitare alcun potere se non con il consenso dell'interessato. Ciò vale sia per la dimensione fisica che per quella rappresentativa e sia nel mondo reale che in quello virtuale. Ciascuna persona è padrona del suo essere e dei dati che la riguardano e l'ordinamento giuridico mette in campo una serie di strumenti idonei affinché ciascuno possa per controllarne l'integrità e contrastare eventuali abusi, per non trasferire ad altri le libertà che lo Stato riconosce.

La materia è assai vasta e in questa sede ci occuperemo soltanto della tutela dei dati personali e del loro trattamento con strumenti cartacei ed elettronici.

La gran parte dei dati esistenti sono stati prodotti negli ultimi anni e ciò si deve ai nuovi sistemi di comunicazione, all'Internet delle cose e alla proliferazione della dimensione *social* della rete, oltre che al processo generale di informatizzazione di tutte le attività umane. I dati personali sono tuttavia solo una porzione dei dati prodotti e possono essere contenuti e veicolati sia su documenti cartacei sia su documenti elettronici.

I dati che ci riguardano sono oggetto di trattamento in maniera distribuita da una moltitudine di sistemi di gestione, di analisi e di archiviazione (anagrafe, scuola, istituti, università, sanità, fornitori di servizi, esercizi commerciali, enti ed associazioni, ecc.).

La riservatezza delle nostre azioni va in perfetta sintonia con gli spazi di libertà che dobbiamo difendere per vivere pienamente la dimensione individuale e collettiva e, quindi, per non essere vincolati (leggasi, eterodeterminati) nelle scelte quotidiane (più di quanto non lo siamo già!)[1]. Difendere i dati che ci riguardano significa essere liberi di fare scelte, fuori dai condizionamenti esterni, ed essere liberi di esprimere la nostra persona, contro chi vorrebbe, e spesso ci riesce, l'omologazione, lo schiacciamento, il controllo.

Per dirla con Stefano Rodotà (forse il padre per eccellenza della tutela della riservatezza in Italia), la tutela complessiva della persona e la protezione dei suoi dati è una garanzia nei confronti di ogni potere, pubblico o privato che sia.

Siamo tutti soggetti passivi del trattamento dei dati personali, cioè di dati che ci riguardano direttamente, e soggetti attivi di azioni di trattamento dei dati di altri.

Le norme a tutela della riservatezza hanno lo scopo di sviluppare la sensibilità all'auto-rispetto e al rispetto degli altri, prevedendo azioni e strumenti perché tale tutela possa essere effettiva. Il concetto di tutela della *privacy* si fa risalire convenzionalmente al 1890, anno in cui due studiosi americani (S. Warren e L. Brandeis) pubblicarono il saggio "The right to privacy". In un primo momento, il concetto di *privacy* fu riferito esclusivamente al diritto di essere lasciati da soli (*right to be let alone*). Di lì a poco, si distinsero due aspetti del medesimo fenomeno: uno passivo legato alla sfera di intimità, mirante ad erigere un confine invalicabile, non oltrepassabile, a protezione del

[1] Si pensi alla segretezza del voto, un principio espresso all'art. 48 della nostra Costituzione, quale espressione imprescindibile di una esistenza libera.

singolo e delle sue informazioni personali senza il suo consenso esplicito ed uno attivo volto a dare valore alla libertà di ciascuno di poter compiere scelte personali ed intime in piena autonomia, senza correre il pericolo di essere condizionato, influenzato ed etichettato dall'esterno.

Di recente, specialmente con il nuovo Regolamento europeo dedicato al tema in analisi – di cui si dirà qui appresso –, si è sviluppato il principio secondo cui la riservatezza dei dati personali è intesa come diritto di controllare l'uso e la circolazione dei propri dati personali, che costituiscono un bene primario nella società dell'informazione.

LE NORME DI RIFERIMENTO

La Costituzione, che si occupa di riservatezza in più disposizioni, all'art. 2 enuncia il principio generale secondo cui "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità …" e, al successivo art. 3, dispone che "Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana …".

Nella Convenzione internazionale firmata a Roma nel 1950 dai Governi membri del Consiglio d'Europa, all'art. 8, è disposto che "Ogni persona ha diritto al rispetto della sua vita privata (anche virtuale) e familiare, del suo domicilio (anche informatico) e della sua corrispondenza (anche elettronica). Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui".

A tutela dei diritti indicati nelle prescrizioni legislative appena riportate, di ordine generalissimo, ogni individuo ha il potere di ricorrere innanzi alla Corte europea dei diritti dell'uomo di Strasburgo in via sussidiaria, cioè dopo aver percorso le vie giurisdizionali del paese di origine.

È bene tenere presente che il diritto alla riservatezza, pur rientrando tra i diritti della personalità, è, al pari di quanto è previsto per la tutela del diritto dell'immagine di cui all'art. 96 della legge sul diritto di autore, un diritto disponibile e, quindi, liberamente negoziabile. Ciò significa che possiamo consentire ad altri il trattamento dei dati che ci riguardano esprimendo il consenso.

La prima legge italiana dedicata interamente alla protezione dei dati personali è la n. 675/1996, denominata *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*. Ma con il decreto legislativo n. 196 del 30/06/2003, denominato *Codice in materia di protezione dei dati personali*, l'Italia ha espresso il primo tentativo al mondo di composizione sistematica ed organica delle disposizioni relative alla tutela dei dati personali.

Il Regolamento dell'Unione europea n. 679/2016, denominato *General Data Protection Regulation* (GDPR) è stato approvato il 27 aprile 2016 dal Parlamento e dal Consiglio dell'Unione Europea. Si compone di 99 articoli e 173 'Considerando'[2] ed è stato pubblicato sulla Gazzetta Ufficiale Unione Europea (GUUE) il 4 maggio 2016 ed entrato in vigore il 25 maggio dello stesso anno. In Italia, come negli altri 28 Stati membri dell'Unione[3], il Regolamento è direttamente applicabile. Il Governo italiano, con il d.lgs. n. 101 del 10 agosto 2018, ha armonizzato la normativa

[2] Nel GDPR le disposizioni normative sono accompagnate dai cosiddetti 'Considerando', in modo da offrire una lettura più ampia e ragionata delle previsioni introdotte, una sorta di guida alla lettura delle disposizioni.

[3] Con la Brexit, il Regno Unito non è più soggetto alle norme dell'Ue e ai fini dell'applicazione del GDPR deve considerarsi paese terzo. Al momento pertanto sono 27 i paesi membri dell'Ue.

interna (essenzialmente il Codice del 2003) alla nuova disciplina europea, adattando le norme con essa incompatibili.

Il Regolamento europeo è una fonte normativa di portata generale, è valido e uguale per tutti gli Stati membri dell'Unione ed è obbligatorio in tutti i suoi elementi e direttamente applicabile. Le sue norme producono effetti vincolanti nei confronti di tutti coloro – autorità pubbliche e soggetti privati – che sono soggetti al rispetto del diritto dell'Unione europea.

Le norme contenute in un Regolamento europeo entrano in vigore e iniziano a produrre direttamente i loro effetti giuridici senza che vi sia la necessità di adottare misure di recepimento da parte degli Stati membri nel loro ordinamento giuridico interno (c.d. norme *self-executing*).

Diversamente dal Regolamento, la Direttiva europea è obbligatoria solo nel fine che intende perseguire e sono necessarie le norme interne, adottate dai paesi membri, di recepimento e di attuazione.

Con lo scopo di fornire pareri, opinioni e linee guida sulle norme europee in tema di *data protection*, l'articolo 29 della Direttiva europea 95/46 ha istituito il Gruppo Art. 29 Working Party (WP29), un gruppo di lavoro composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati (GEPD-EDPS) e da un rappresentante della Commissione europea. Il 25 maggio 2018, data in cui il GDPR è diventato pienamente operativo, il Gruppo Art. 29 è stato sostituito dal Comitato europeo per la protezione dei dati (European Data Protection Board), quale organo avente il compito di garantire l'applicazione del Regolamento.

Tramite una Direttiva Ue 2016/680, collegata al GDPR, è stata dettata la disciplina speciale, e in parte derogatoria, per i trattamenti dei dati da parte dell'Autorità giudiziaria e di tutte le Forze di polizia, quindi per la sicurezza nazionale e l'ordine pubblico.

L'AMBITO DI APPLICAZIONE MATERIALE E TERRITORIALE DEL GDPR

Il GDPR, al quale faremo riferimento in generale per la trattazione del tema della riservatezza dei dati personali, si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.

Il GDPR non si applica ai trattamenti di dati personali effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; ai trattamenti effettuati dagli Stati membri nell'esercizio di attività legate alla politica estera e alle sicurezza; ai trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse (vedi Direttiva 2016/680); ai trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico (esenzione per uso personale).

Il GDPR si applica al trattamento dei dati personali di Interessati che si trovano nell'Unione, effettuato da un Titolare del trattamento o da un Responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti Interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'Interessato; b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Il GDPR si rivolge a tutti coloro che trattano dati personali di residenti in Ue, indipendentemente da dove è ubicata la sede del trattamento (si pensi ai *server* per lo storaggio di dati di imprese operanti in Europa che possono essere collocati anche in Stati extraUe).

Il GDPR si applica al trattamento dei dati personali effettuato da un Titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (Considerando 25, rappresentanza diplomatica o consolare extraUe di uno Stato membro).

FIGURE CHIAVE NEL GDPR

I soggetti implicati nei processi di trattamento dei dati personali sono il Garante, il Titolare ed il Responsabile del trattamento, il Responsabile per la protezione dei dati e il soggetto Interessato[4].

Il Garante per il trattamento dei dati è un'Autorità amministrativa indipendente; il Regolamento prevede la costituzione di un'Autorità di controllo in ciascuno Stato membro e fissa identici compiti e poteri per le Autorità (artt. 57 e 58) in tutti i paesi Ue. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vicepresidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

Tra i principali compiti assegnati al Garante si possono indicare i seguenti:

a) sorveglia e assicura l'applicazione del Regolamento;
b) promuove la consapevolezza e favorisce la comprensione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti in relazione al trattamento, con particolare attenzione ai minori;
c) fornisce consulenza al Parlamento nazionale, al Governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento;
d) su richiesta, fornisce informazioni all'Interessato in merito all'esercizio dei propri diritti derivanti dal Regolamento e, se del caso, coopera a tal fine con le Autorità di controllo di altri Stati membri;
e) tratta i reclami proposti da un Interessato, o da un organismo, un'organizzazione o un'associazione e svolge le indagini opportune sull'oggetto del reclamo e informa il reclamante dello stato e dell'esito delle indagini.

In estrema sintesi, si può dire che il Garante ha poteri di indagine, correttivi, autorizzativi, consultivi e di infliggere sanzioni amministrative pecuniarie.

Il Titolare (art. 24) è la persona fisica o la persona giuridica, l'autorità pubblica, il servizio o qualsiasi altro 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, ivi compreso il profilo della sicurezza. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, 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 Regolamento.

Il Responsabile del trattamento (art. 28) è la persona fisica o la persona giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo, designato dal Titolare del trattamento, che tratta dati personali per conto di quest'ultimo. È una figura facoltativa – cioè non in tutte le realtà in cui sono trattati dati personali è necessario che sia individuato un Responsabile del trattamento – e può ricevere l'incarico dal Titolare con qualunque atto giuridico, incluso un contratto (il contenuto minimo dell'accordo fra il Titolare ed il Responsabile è riportato all'art. 28, co. 3. Nel contratto, redatto in forma scritta, potranno essere stabilite clausole in relazione alla durata del rapporto, alla natura del trattamento, alla finalità e alle responsabilità di tipo civile, penale ed amministrativo a carco del Responsabile).

[4] Nella trattazione dell'argomento di cui alla presente sezione, al solo fine didattico, i soggetti implicati nel trattamento dei dati sono riportati in maiuscolo perché possano essere individuati più chiaramente durante lo studio.

È Responsabile del trattamento, ad esempio, il commercialista di un professionista o di una impresa, il consulente del lavoro, il fornitore di servizi di una amministrazione pubblica che tratta dati personali per conto di quest'ultima.

L'art. 82 stabilisce che Titolare e Responsabile rispondono in solido nei confronti dell'Interessato i cui dati siano stati trattati in violazione del GDPR. Ciò significa che il soggetto violato potrà indistintamente chiedere il risarcimento del danno per intero all'uno o all'altro soggetto.

Tra le novità più rilevanti riportate nel GDPR vi è senz'altro il concetto di "accountability" enunciato all'art. 24. Si tratta di una previsione, per così dire, strategica e consiste in una investitura del Titolare e del Responsabile di una particolare forma di responsabilità che li obbliga a dare conto del proprio operato. Questi, infatti, per garantire il corretto trattamento dei dati personali non potranno più sostenere, come avveniva con la vecchia normativa, di aver adottato le misure minime di sicurezza per garantire il corretto trattamento dei dati personali, ma dovranno rendicontare il loro operato, dimostrando di aver adottato misure idonee per assicurare affidabilità e competenza nella gestione dei dati personali.

Il principio di *accuontability* è declinato in tre attività: 1) la "trasparenza" intesa come garanzia della completa accessibilità alle informazioni, in primo luogo per i cittadini, anche in quanto utenti del servizio; 2) la "responsività" intesa come la capacità di rendere conto di scelte, comportamenti e azioni e di rispondere alle questioni poste in merito al trattamento effettuato; 3) la "compliance" intesa come capacità di far rispettare le norme, sia nel senso di finalizzare l'azione all'obiettivo stabilito nelle leggi che nel senso di osservare e far osservare le regole di comportamento a chiunque interviene nella filiera del trattamento. Il Titolare ed il Responsabile del trattamento devono essere in grado di dimostrare che hanno adottato un complesso di misure giuridiche, organizzative e tecniche per la protezione dei dati personali, anche attraverso l'elaborazione di specifici e adeguati modelli organizzativi.

Alcuni esempi di azioni concrete potrebbero essere l'adozione di sistemi di *intrusion detection* nella rete interna di un'azienda e di *disaster recovery*, per garantire l'integrità dei dati, e la continuità operativa dei servizi.

L'*accountability*, così com'è intesa nel GDPR, determina una inversione dell'onere della prova in caso di danno di qualsiasi natura derivante dal trattamento dei dati relativi ad un soggetto: il Titolare e il Responsabile sono tenuti a dimostrare di aver utilizzato tutti gli accorgimenti necessari (nei limiti delle possibilità dell'ente/impresa e della sua dimensione) per scongiurare il verificarsi dell'evento dannoso (tecnicamente, *data breach*); il danneggiato dovrà soltanto dichiarare di aver subito un danno ed è in tal modo dispensato dal dimostrare, ad esempio, la falla del sistema informatico (cosa, peraltro, assai complicata per l'Interessato).

Proseguendo nella disamina delle figure chiave enunciate nel GDPR, all'art. 37, è previsto il Data Protection Officer (DPO) o Responsabile della protezione dei dati (RPD). Si tratta di una persona fisica, il cui ruolo si colloca funzionalmente tra la vigilanza dei processi interni alla struttura e la consulenza; ha quindi una doppia veste e funge da 'ponte di contatto' tra la realtà in cui opera e l'Autorità Garante nazionale. Il DPO deve essere nominato quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico: il WP29 ha dato un'interpretazione estensiva di organismo pubblico e ha raccomandato, come una buona pratica, la nomina del DPO anche da parte delle organizzazioni private che svolgono funzioni pubbliche o che esercitano pubblici poteri. La sua attività dovrebbe coprire tutte le operazioni di trattamento, comprese quelle che non sono legate alla esecuzione di un compito pubblico o esercizio del dovere ufficiale (ad esempio la gestione di un *database* dei dipendenti). Secondo le linee guida redatte dal WP29 la nomina del DPO è altresì obbligatoria quando le attività principali (cd. *core business*) del Titolare o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli Interessati, nonché nel caso di trattamento, su larga scala, di speciali categorie di dati personali o di dati relativi a reati

e condanne penali. Il concetto di "larga scala" dev'essere valutato sulla base di alcuni specifici criteri: quali, ad esempio, il numero di Interessati coinvolti nel trattamento, la durata del trattamento e la sua estensione geografica (tra i trattamenti effettuati su larga scala, in particolare, rientrano la geo-localizzazione, per finalità statistiche, dei clienti di una certa attività, ad esempio catene di ristoranti; il trattamento dei dati bancari dei propri clienti da parte di una compagnia assicurativa; il trattamento, da parte di un motore di ricerca, dei dati personali degli utenti per l'invio di pubblicità mirata). Tra i trattamenti non su larga scala, invece, sono ricompresi: il trattamento dei dati dei pazienti da parte del medico di un famiglia ed il trattamento dei dati personali di natura penale da parte di un avvocato.

Inoltre, anche ove il Regolamento non imponga in modo specifico la designazione di un DPO, può risultare utile procedere a tale designazione su base volontaria.

L'art. 39 prescrive che il DPO deve svolgere, in piena autonomia ed indipendenza, i compiti qui di seguito sinteticamente riportati: informare e fornire consulenza al Titolare e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR; sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati; cooperare con il Garante per la protezione dei dati personali.

L'Interessato o data subject, infine, è la persona fisica cui si riferiscono i dati personali (identificata o identificabile), cioè colui al quale spetta il controllo dei propri dati che lo riguardano (trattati da altri) anche attraverso i diritti che gli sono riconosciuti dal GDPR, di cui di dirà più avanti.

Il Regolamento non si applica nel trattamento di dati anonimi (anche per finalità statistiche e di ricerca).

Ai sensi dell'art. 4, par. 1, del GDPR, per dato personale si intende «Qualsiasi informazione riguardante una persona fisica identificata o identificabile (Interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

I dati che nel Codice italiano, ante riforma del 2016, erano classificati come "dati sensibili" sono stati ricompresi nel Regolamento europeo all'art. 9 con la denominazione "Categorie particolari di dati personali". L'articolo, infatti, dispone che «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici[5], dati biometrici[6] intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona».

Infine, all'art. 10, sono individuati i dati personali relativi a condanne penali e reati, per i quali è previsto che «Il trattamento … deve avvenire soltanto sotto il controllo dell'Autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli Interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica».

IL TRATTAMENTO DEI DATI PERSONALI

Per trattamento dei dati personali si intende "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati

[5] Si intendono i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione (DNA ed RNA).

[6] Si intendono i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici (linee cutanee dei polpastrelli delle dita o impronte digitali).

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[7] mediante trasmissione, diffusione[8] o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

Le disposizioni contenute nel GDPR non si applicano ai trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico nonché ai trattamenti effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.

Strettamente collegati al "principio di necessità" di cui all'art. 3 del GDPR, in base al quale, il Titolare deve trattare esclusivamente i dati indispensabili per l'attività o il servizio che svolge per conto del soggetto Interessato, sono i principi della *privacy by design* e *privacy by default*. In particolare, con il primo principio enunciato, il Regolamento intende richiamare l'attenzione dei Titolari sull'esigenza che la protezione dei dati personali venga garantita fin dalla progettazione dei sistemi o dei mezzi per il trattamento. A questo proposito, l'art. 25 stabilisce che il Titolare del trattamento dei dati personali deve adottare delle misure tecniche e organizzative idonee a dare concreta attuazione a quelle che sono le disposizioni e i principi in materia di protezione dei dati e garantire in questo modo i diritti degli Interessati. La predisposizione delle misure necessarie è prescritta sia nel momento in cui il Titolare del trattamento debba determinare i mezzi del trattamento stesso, sia quando ponga in essere le vere e proprie operazioni di trattamento. In ordine al secondo principio enunciato, la protezione dei dati personali deve essere garantita per «impostazione predefinita», cioè i sistemi devono essere predisposti affinché la *privacy* sia garantita già dalla prima applicazione. Potrà semmai il singolo utente allargare le maglie della tutela (allentando i settaggi vincolanti) e rinunciare ad alcuni aspetti di riservatezza.

LICEITÀ DEL TRATTAMENTO

Il trattamento di dati personali di altre persone fisiche può essere effettuato solo se è fondato su una base giuridica certa. In altri termini, il trattamento è lecito soltanto se è fondato su uno dei seguenti punti: a) l'Interessato ha espresso il proprio consenso per una o più specifiche finalità[9]; b) è necessario per l'esecuzione di un contratto di cui l'Interessato è parte[10]; c) è necessario per adempiere ad un obbligo legale al quale è soggetto il Titolare del trattamento[11]; d) è necessario per salvaguardare degli interessi vitali dell'Interessato o di altre persone fisiche[12]; e) è necessario per l'esecuzione di un compito di pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento[13]; f) è necessario per il perseguimento di un legittimo interesse del Titolare del trattamento[14], a condizione che non prevalgano i diritti e le libertà fondamentali

[7] Dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'Interessato, dal rappresentante del Titolare, dal Responsabile e dagli Incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

[8] Dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

[9] Si veda *infra* il consenso informato.

[10] Costituiscono esempi: il trattamento dei dati da parte del commercialista o del consulente del lavoro per l'esecuzione di un contratto di lavoro presso un'azienda – busta paga, ritenute previdenziali, inquadramento dei dipendenti.

[11] Si pensi alla trasmissione di dati sanitari dei pazienti da parte delle strutture ospedaliere al Ministero della Salute o alla trasmissione delle ricette mediche dei clienti da parte dei farmacisti per il rimborso sul servizio sanitario nazionale oppure la trasmissione al MUR dei dati degli studenti immatricolati o laureati presso una università italiana.

[12] Si pensi ad un ricovero d'urgenza ed il conseguente trattamento dei dati di un paziente in pericolo di vita.

[13] Si pensi al trattamento dei dati delle parti da parte del consulente tecnico d'ufficio (CTU) incaricato nell'ambito di un processo giurisdizionale.

[14] Si pensi al *marketing* diretto non automatizzato.

dell'Interessato che richiedono una protezione maggiore dei dati personali (ad es. dati personali di soggetti minori).

Se, dunque, il trattamento trova legittimazione in una delle precedenti lettere, i dati trattati devono essere esatti ed aggiornati, pertinenti, completi e non eccedenti. I dati personali sono conservati in una forma che consenta l'identificazione dell'Interessato per un periodo di tempo non superiore a quello necessario agli scopi per cui sono stati legittimamente raccolti e trattati.

L'INFORMATIVA

Ai sensi degli artt. 12-14, l'informativa è un documento che illustra le ragioni e le finalità della raccolta dei dati, la base giuridica del trattamento, i dati dei soggetti legittimati al trattamento, la natura obbligatoria o facoltativa del conferimento dei dati per ricevere un determinato servizio, il periodo di conservazione dei dati, i diritti degli Interessati, l'esistenza di un processo decisionale automatizzato (profilazione), l'eventuale trasferimento ad altri soggetti dei dati raccolti, l'eventuale trasferimento dei dati in paesi extra Ue, ecc. L'informativa deve essere, di norma, fornita direttamente agli Interessati al momento della raccolta dei dati. Deve prevedere gesti positivi dell'Interessato per la raccolta del consenso (libero, specifico e informato). Non è consentito prevedere modelli di raccolta del consenso precompilati. La forma dell'informativa è libera, ma quella scritta ha evidentemente una valenza probatoria maggiore.

DIRITTI DEGLI INTERESSATI

I soggetti cui si riferiscono i dati personali, nella loro qualità di Interessati, hanno il diritto in qualunque momento di chiedere al Titolare del trattamento informazioni in merito all'esercizio dei propri diritti.

In particolare, gli Interessati hanno diritto di:

- conoscere i contatti del Titolare e, ove previsto, del Responsabile del Trattamento nonché del Responsabile per la protezione dei dati;
- ottenere la conferma dell'esistenza o meno dei propri dati e di conoscerne il contenuto, l'origine e le finalità;
- chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi, la limitazione del trattamento che li riguardano, di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- revocare il consenso in qualsiasi momento, senza tuttavia pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca. In tale caso, non saranno raccolti ulteriori dati che li riguardano, ferma restando l'utilizzazione di quelli eventualmente già raccolti, senza alterarli, per assolvere agli obblighi di legge o per fini amministrativi o di quelli che, in origine o a seguito di trattamento, non siano riconducibili a una persona identificata o identificabile;
- proporre reclamo ad un'Autorità di controllo.

Il Titolare del trattamento deve fornire all'Interessato le informazioni relative all'azione intrapresa riguardo ad una richiesta di accesso, ai sensi degli articoli da 15 a 20, senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato per un massimo di altri due mesi, se necessario, tenuto conto della complessità della richiesta e del numero di richieste. Qualora si applichi la proroga, l'Interessato è informato dei motivi del ritardo entro un mese dal ricevimento della richiesta.

Con il riconoscimento del diritto alla cancellazione o all'oblio l'Interessato ha il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia conforme al Regolamento.

Tuttavia, è lecita l'ulteriore conservazione dei dati qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica e storica o finalità statistiche o per accertare, esercitare o difendere un diritto in sede giudiziaria.

Per rafforzare il diritto all'oblio nell'ambiente *online*, è previsto che il Titolare del trattamento che abbia pubblicato dati personali sul web cancelli qualsiasi *link* verso tali dati personali o copia o riproduzione di essi.

Ai sensi dell'art. 21, l'Interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, nei casi in cui il trattamento derivi dall'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri o dalla tutela di un interesse legittimo del Titolare. Il Titolare del trattamento si deve astenere dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati per finalità di *marketing* diretto, l'Interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità.

Il Regolamento pone una particolare attenzione al trattamento automatizzato dei dati personali che possa sfociare in decisioni che sono proprie della macchina e non dell'uomo. L'art. 22, al proposito, ribadisce, come principio generale, che l'Interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.

Infine, un cenno in più va riferito al diritto alla portabilità dei dati: a norma dell'art. 20 l'Interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti ad un Titolare del trattamento ed ha il diritto di trasmettere tali dati a un altro Titolare del trattamento senza impedimenti da parte del Titolare del trattamento cui li ha forniti e, inoltre, ha il diritto di ottenere la trasmissione diretta dei dati da un Titolare del trattamento all'altro, se tecnicamente fattibile.

Quest'ultimo diritto riconosciuto all'Interessato costituisce una delle più importanti novità del Regolamento. Il diritto di 'portare' i propri dati personali, ad esempio, da un *provider* ad un altro oppure del trasferimento del pacchetto delle informazioni personali da un *social network* ad un altro.

REGISTRI DEL TRATTAMENTO E DATA PROTECTION IMPACT ASSESSMENT (DPIA)

È previsto all'art. 30 che il Titolare e, ove previsto, il Responsabile del trattamento tengano i registri delle attività di trattamento svolte sotto la propria responsabilità.

I registri del Titolare e del Responsabile hanno contenuti lievemente differenti e, per sommi capi, devono contenere: il nome e i dati di contatto del Titolare e del Responsabile e, ove presente, del Responsabile della protezione dei dati e le finalità del trattamento; la descrizione delle categorie di trattamenti e delle categorie degli Interessati; se vi è trasferimento dei dati verso paesi extra Ue; la descrizione delle misure di sicurezza, tecniche ed organizzative adottate.

Vi sono casi di esonero dall'obbligo di tenuta del registro delle attività di trattamento quando si tratti di realtà con meno di 250 dipendenti, purché i trattamenti di dati personali non presentino elementi ritenuti comunque di rischio per gli Interessati.

In ossequio al principio di *accountability*, una rete documentale a comprova dell'attività effettuata ha valenza probatoria forte (e ciò vale per i registri, la raccolta del consenso, i dpia, i

contratti, i codici di comportamento, le certificazioni, i pareri del DPO e quelli richiesti direttamente al Garante, ecc.).

La valutazione d'impatto sulla protezione dei dati o Data Protection Impact Assessment (DPIA) è un'attività prescritta agli artt. 35-36. Allorquando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è previsto che il Titolare effettui, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. Tale attività di processo aiuta a gestire i rischi connessi al trattamento dei dati personali per i diritti e le libertà delle persone fisiche derivanti dal trattamento, con speciale riferimento ai principi di proporzionalità e necessità ad esso correlati e volta ad identificare i rischi connessi al fine di individuare in anticipo le misure e accorgimenti necessari per mitigare tali rischi.

È altresì previsto che il Titolare del trattamento, prima di procedere al trattamento, consulti l'Autorità di controllo nei casi in cui la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenti un rischio elevato.

DATA BREACH E VIOLAZIONI

Il Regolamento prevede espressamente l'obbligo del Titolare di notifica e comunicazione tempestiva all'Autorità di controllo in presenza di violazioni di dati personali che possano compromettere le libertà e i diritti dei soggetti Interessati.

Nel caso in cui la violazione sia accertata e sia di grado elevato, la procedura prescrive, altresì, la comunicazione agli Interessati[15]. Appurato il rischio conseguente dalla violazione, gli artt. 33 e 34 del GDPR indicano ai Titolari i termini, le modalità, i contenuti e le deroghe della notifica e della comunicazione di *data breach*.

L'art. 33 impone al Titolare di notificare la violazione all'Autorità di controllo entro 72 ore dal momento in cui ne viene a conoscenza. Il tempo di riferimento da cui iniziano a decorrere i termini della notifica viene individuato quindi nel momento in cui il Titolare acquisisce consapevolezza dell'avvenuta violazione.

Nelle linee guida, il WP29 ha disposto che debba considerarsi "a conoscenza" il Titolare che abbia un ragionevole grado di certezza in merito alla verificazione di un incidente di sicurezza. È evidente che, in base alle specifiche circostanze, mentre alcune violazioni saranno facilmente rilevabili, per altre sarà necessario instaurare un'indagine più approfondita. In questi casi, durante la fase di investigazione, il Titolare può essere considerato privo di un grado di conoscenza tale da far scattare immediatamente l'obbligo di notifica. Ciò precisato, il Gruppo ha sottolineato che il diligente comportamento del Titolare sarà in ogni caso valutato sulla base della sua tempestiva attivazione in caso venga informato di una possibile infrazione. La fase investigativa, quindi, non deve essere abusata per prorogare illegittimamente il termine di notifica.

Il Gruppo ha raccomandato ai Titolari di predisporre un piano di sicurezza che evidenzi le procedure organizzative interne da adottare nella gestione di eventuali violazioni e l'organigramma dei soggetti o dei livelli direttivi a cui è necessario fare riferimento per riportare l'accadimento. L'art. 33 dispone l'obbligo in capo al Responsabile del trattamento di informare tempestivamente il Titolare dell'avvenuta violazione. In linea di principio, il Titolare deve considerarsi a conoscenza della violazione nel momento in cui il proprio Responsabile ne sia venuto a conoscenza. Non deve quindi esistere alcuna dilazione temporale nelle comunicazioni tra i due. Le linee guida prospettano l'ipotesi che il Responsabile, sulla base di specifica autorizzazione del Titolare contrattualmente

[15] Si pensi al rinvenimento di uno *skimmer* nel bancomat, scoperto all'apertura dell'istituto bancario dal Titolare del trattamento. In tali casi, il Titolare deve dare immediata comunicazione al Garante e agli Interessati per limitare i danni di furto di identità, oltre che di ordine economico finanziario, e deve darne comunicazione all'Autorità giudiziaria, sporgendo denuncia contro ignoti presso la Questura o i Carabinieri.

prevista, possa eseguire personalmente la notifica al Garante per conto di quest'ultimo, fermo restando che le responsabilità nei confronti dell'Autorità e degli Interessati scaturenti dalla notifica, o dalla sua mancanza, permangano in capo al Titolare.

Nel caso in cui una violazione possa compromettere i diritti e le libertà di cittadini situati in diversi Pasi membri, il Gruppo ha chiarito che dovrà utilizzarsi il meccanismo delle "Autorità capofila", ossia la notifica dovrà essere effettuata all'Autorità garante situata nello Stato membro presso cui si trova lo stabilimento principale o l'unico stabilimento del Titolare o del Responsabile. Il meccanismo decisionale nei casi di trattamento transfrontaliero risponde alla logica dello "sportello unico".

REGIME SANZIONATORIO

Per la violazione delle norme poste a tutela della protezione dei dati il GDPR prevede l'applicazione di sanzioni amministrative pecuniarie.

La definizione delle altre sanzioni (tra cui anche quelle penali) resta di competenza dei legislatori nazionali.

Il GDPR individua due valori massimi determinati in una somma pari a 10 o 20 milioni di euro o, ove superiori, determinabili calcolando una percentuale (2% o 4% sul fatturato delle imprese) a seconda del tipo di violazione.

I Responsabili del trattamento rispondono in solido per il risarcimento del danno con Titolari, Contitolari e altri Responsabili.

L'art. 82 del GDPR, prevede la possibilità per l'Interessato che subisca un danno materiale o immateriale di ottenere il risarcimento del danno dal Titolare o dal Responsabile. Le azioni legali saranno esperite presso le giurisdizioni degli Stati membri competenti.

Si incorre nelle sanzioni nei casi qui di seguito esemplificati:

- violazione delle condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione;
- trattamento illecito di dati personali che non richiede l'identificazione dell'Interessato;
- mancata o errata notificazione e/o comunicazione di un *data breach* all'Autorità nazionale competente;
- violazione dell'obbligo di nomina del DPO;
- mancata applicazione di misure di sicurezza;
- inosservanza di un ordine, di una limitazione provvisoria o definitiva concernente un trattamento, imposti da un'Autorità nazionale competente;
- trasferimento illecito *cross-border* di dati personali ad un destinatario in un paese terzo.

I criteri per la determinazione delle sanzioni amministrative pecuniarie sono la natura, la gravità e la durata della violazione, il carattere doloso o colposo della violazione nonché il grado di cooperazione con l'Autorità di controllo al fine di porre rimedio alla violazione e attuarne i possibili effetti negativi.

L'Interessato può chiedere al giudice naturale in ambito civilistico il risarcimento del danno morale economico, senza limiti prefissati dalla legge.

La carenza di risorse economiche e materiali non può costituire ipotesi di esenzione di responsabilità.

Nel Considerando 148 è offerta all'Autorità nazionale l'opportunità di sostituire la sanzione pecuniaria con un ammonimento, "in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica".

CODICE ETICO, CODICE DI COMPORTAMENTO E CERTIFICAZIONE

I codici etico e di comportamento costituiscono il riferimento per ciascuna realtà sociale ed economica, pubblica o privata che sia, per la responsabilizzazione nei processi gestionali e

produttivi e per moralizzare la condotta dei dipendenti e di chi entra in relazione con esse (diritti e doveri morali, tutela degli individui, gestione delle risorse, qualità, competitività, crescita, coerenza, rapporti con i colleghi e con gli utenti o con i clienti, diligenza, politiche anticorruzione, politiche e responsabilità sociali, ecc.). Sono norme giuridiche di grado subordinato che si aggiungono alle norme primarie di settore. In particolare, il codice etico esprime i principi, i valori e gli ideali dell'ente/azienda/attività professionale in genere, giuda i processi decisionali e l'attività produttiva ed è rivolto all'esterno. Il codice di comportamento, che origina dal codice etico, ha rilevanza interna e guida l'agire dei singoli; è rivolto alle persone che lavorano presso un ente/azienda o che svolgono un'attività professionale o che con quella vengono in contatto nella qualità di utenti/clienti o prestano un servizio per conto della stessa. Codici etico e di comportamento sono già emanati per categorie nella quasi totalità dei settori sociali ed economici, ma le amministrazioni, gli enti, le istituzioni, i professionisti e gli imprenditori possono adottarne propri su base volontaria, specificando e dettagliando con ulteriori disposizioni i valori e le finalità che intendono tutelare e perseguire nello svolgimento delle rispettive attività.

Il codice etico risponde a quanto previsto nel d.lgs. n. 231/2001, che disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, ivi compresi i reati contro la Pubblica amministrazione, contro la fede pubblica, contro il patrimonio, ecc. commessi dai dipendenti, prevedendo anche, in caso di trasgressione, responsabilità di tipo civile, penale, amministrative e contabili, oltre ai provvedimenti disciplinari.

La violazione delle disposizioni contenute nel codice etico è a tutti gli effetti un inadempimento delle obbligazioni contrattuali con ogni conseguenza prevista dalla legge, compresi la risoluzione del contratto e il risarcimento dei danni.

Il codice di comportamento definisce i doveri minimi di diligenza, lealtà, imparzialità e buona condotta dei dipendenti e dei *partner*, fornitori, utenti.

All'art. 40 del GDPR si trova un riferimento specifico ai codici di condotta in materia di protezione dei dati personali. In particolare, è disposto che 1. Gli Stati membri, le Autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese. 2. Le associazioni e gli altri organismi rappresentanti le categorie di Titolari del trattamento o Responsabili del trattamento possono elaborare i codici di condotta, modificarli o prorogarli, allo scopo di precisare l'applicazione del presente regolamento, ad esempio relativamente a: a) il trattamento corretto e trasparente dei dati; b) i legittimi interessi perseguiti dal Responsabile del trattamento in contesti specifici; c) la raccolta dei dati personali; d) la pseudonimizzazione dei dati personali; e) l'informazione fornita al pubblico e agli Interessati; f) l'esercizio dei diritti degli Interessati; g) l'informazione fornita e la protezione del minore e le modalità con cui è ottenuto il consenso dei titolari della responsabilità genitoriale sul minore; h) le misure e le procedure di cui agli articoli 24 e 25 e le misure volte a garantire la sicurezza del trattamento di cui all'articolo 32; i) la notifica di una violazione dei dati personali alle autorità di controllo e la comunicazione di tali violazioni dei dati personali all'Interessato; j) il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali; k) le procedure stragiudiziali e di altro tipo per comporre le controversie tra Titolari del trattamento e Interessati in materia di trattamento, fatti salvi i diritti degli Interessati ai sensi degli articoli 77 e 79.

Ai sensi dell'art. 42, gli Stati membri, le Autorità di controllo, il Comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai Titolari del trattamento e dai Responsabili del trattamento. Sono tenute in considerazione le esigenze specifiche delle micro, piccole e medie imprese.

La Certificazione Etica Social Accountability 8000 (SA8000) per il codice etico si occupa del rispetto dei diritti umani; consente così di diminuire i rischi di abusi, quali il lavoro minorile o coatto, la discriminazione, la salute e la sicurezza sul lavoro, la violazione della *privacy*.

Gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'Autorità di controllo al fine di consentire alla stessa di esercitare i suoi poteri a norma dell'articolo 58, paragrafo 2, lettera h), ove necessario. Gli Stati membri garantiscono che tali organismi di certificazione siano accreditati da uno o entrambi dei seguenti organismi:

a) dall'Autorità di controllo competente;

b) dall'organismo nazionale di accreditamento designato.

In conclusione, si può affermare che tra le misure volte a prevenire fenomeni di violazione della riservatezza rientrano anche i codici di condotta. La funzione di guida e di dissuasione dal commettere atti in violazione delle norme a protezione della riservatezza, soprattutto se contenute in codici di condotta certificati, aggiungono un importante tassello di compliance al GDPR che il Titolare può vantare.

La tutela della riservatezza non coincide con l'osservanza delle leggi, ma dipende dal modo in cui noi gestiamo il rapporto con la nostra persona e con quelli con cui entriamo in relazione, ben al di là dei precetti.