DATI, PRIVACY E DATA PROTECTION

Diritto alla privacy e diritto alla protezione dei dati

"I dati ridefiniranno il nostro modo di produrre, consumare e vivere" (Commissione Europea, 2020). I dati rappresentano un asset essenziale e la loro circolazione è considerata come il motore della *data-driven innovation*, tanto da essere considerata dall'Unione una "libertà fondamentale tra i pilastri portanti del mercato unico europeo".

L'esigenza di regolare il diritto alla privacy e ad un corretto trattamento dei propri dati personali nasce con l'avvento e la diffusione delle tecnologie informatiche e telematiche e il loro impiego nel trattamento dei dati, posto che nel contesto digitalizzato il controllo sulla circolazione delle informazioni non poteva essere più svolto unicamente dall'interessato al quale i dati pertengono. La risposta del legislatore è stata quella di introdurre dei meccanismi che consentissero ai titolari dei dati di acconsentire o meno, a monte, all'immissione ed alla circolazione delle informazioni a loro riferite. Il consenso è, dunque, l'elemento fondamentale che governa il trattamento dei dati personali.

→ Nasce così il diritto alla protezione dei dati (**data protection**), in base al quale il titolare delle informazioni può limitare la circolazione dei propri dati, spostando la responsabilità sul soggetto al quale l'interessato ha ceduto l'informazione stessa, ossia il titolare del trattamento dei dati. Sulla base di tale diritto è stata, poi, sia a livello nazionale che a livello UE, coniata una articolata normativa che disciplina a quali condizioni, per quali finalità e secondo quali procedure i dati personali possono essere trattati.

Occorre, dunque, distinguere tra diritto alla privacy e diritto alla protezione dei dati, ossia due concetti che, nonostante vengano spesso sovrapposti, sono in realtà distinti:

- il diritto alla privacy è, in generale, il diritto alla riservatezza, ossia ad impedire interferenze nella propria vita privata, il diritto a mantenere la sfera della propria vita privata ed intima al riparo dagli altri (diritto ricavabile dalla interpretazione di articoli della Costituzione, quali quello alla inviolabilità della persona, e che deve essere controbilanciato rispetto ad altri interessi, quali l'interesse della società a conoscere determinate notizie o altre esigenze pubbliche);
- il diritto alla protezione dei dati è, invece, il diritto dell'interessato a controllare (ossia conoscere ed anche limitare) la circolazione di informazioni (dati) riguardanti la propria persona.

La normativa in materia di data protection disciplina, dunque, più specificamente, il rapporto tra due soggetti quanto al trattamento dei dati:

- l'**interessato** (il **data subject**), ossia la persona alla quale si riferiscono i dati;
- il **titolare del trattamento** (il **data controller**), ossia la persona (ivi incluse le autorità pubbliche) al quale l'interessato cede i dati e che stabilisce le finalità ed i mezzi del trattamento. È dunque colui che decide, in ultima istanza, come e perché trattare i dati dell'interessato.

Cos'è un "dato personale"? È qualsiasi elemento informativo (rappresentativo di una informazione) che sia in grado di essere riferita ad una determinata persona fisica e consenta, anche in combinazione ad altri elementi, di individuare il soggetto al quale tale informazione è riferibile. Non è, dunque, necessario che il dato sia affiancato dal

nome e cognome della persona al quale si riferisce, ma è sufficiente che l'interessato possa essere individuato all'interno di una categoria, anche da poche persone. Esempi di dati personali possono essere i seguenti:

- nome e cognome;
- dati relativi all'ubicazione;
- identificativo online;
- elementi relativi all'identità fisica;
- elementi relativi alla identità psichica, economica, culturale o sociale, ecc.

Spesso i termini "dato" ed "informazione" vengono usati come sinonimi, ma dal punto di vista informatico (ed anche giuridico) non è corretto. Infatti:

- un "dato" è una rappresentazione oggettiva, "grezza" e non interpretata della realtà, ossia ciò che è immediatamente percepito dall'esterno in relazione ad una persona senza alcuna particolare elaborazione;
- una "informazione" è una visione della realtà derivante dalla elaborazione e della interpretazione dei dati grezzi, ossia il significato che viene associato ai dati. L'informazione è, dunque, il risultato di una elaborazione di dati.

Il dato è, quindi, un elemento rappresentativo di una informazione. Potremmo, in termini molto semplici e riduttivi, dire che esiste un "primo livello", ossia il dato, ed un "secondo livello", un livello ulteriore che deriva dal dato, e che è, per l'appunto, l'informazione. Si parte da dati conosciuti per arrivare ad un risultato che precedentemente non era conosciuto (per "imparare qualcosa di qualcuno", potremmo dire), ossia l'informazione. Questo è fondamentale per comprendere i meccanismi di marketing (anche neuro-marketing) ed il funzionamento delle piattaforme, ad esempio (così come la normativa applicabile).

Le questioni di data protection si intrecciano, poi, con esigenze di sicurezza informatica dei dati (**data security**), da garantire attraverso lo sviluppo di sistemi gestionali il più sicuri possibile, specialmente con riferimento alla conservazione di dati nel cloud.

Dati personali vs. Big data. Il valore economico del dato come "oggetto di scambio"

La attuale normativa in materia di data protection (o comunque quella che sarà oggetto di studio) è relativa alla protezione dei soli dati personali.

Dati personali vs. Big data: i "big data" sono grandi volumi di dati, acquisiti principalmente in rete ed elaborati dall'Intelligenza Artificiale per trarne correlazioni e, dunque, nuove informazioni anche molto preziose. L'applicazione classica è quella della profilazione, che acquista dimensioni sempre più estese, tanto che si inizia a parlare addirittura di "privacy di gruppo" (group privacy).

Si tratta di dati di natura diversa, anche non necessariamente personali, anche in quanto potenzialmente anonimi. Ora, abbiamo detto che un dato per essere "dato personale" deve essere riconducibile, direttamente o indirettamente, ad una determinata persona, pertanto teoricamente un dato anonimo non è un dato personale, e dunque teoricamente la normativa in materia di data protection non potrebbe trovare applicazione. Ma, anche grazie all'analisi dei big data ed all'Intelligenza Artificiale,

potrebbe essere semplice "assegnare nome e cognome" ad un determinato dato inizialmente anonimo, e che dunque cesserebbe di essere tale. Cosa succede in tale caso quanto alla normativa applicabile?

Altra rilevante questione attiene al **valore economico del dato**.

È ormai principio assodato per il diritto quello secondo il quale i dati hanno un valore economicamente apprezzabile e, dunque, possono rilevare come "corrispettivo", come "prezzo" di un determinato servizio. Non è, dunque, corretto affermare, ad esempio, che i servizi di social network sono gratuiti, perché per il diritto "gratuito" è un prodotto o un servizio che viene fornito senza che chi lo fornisce riceva alcun tipo di corrispettivo (non necessariamente una somma di denaro, ma qualsiasi tipo di bene suscettibile di avere un valore economico, e dunque anche il dato)[1].

Il GDPR: elementi fondamentali della disciplina

Principale riferimento normativo in materia è oggi costituito dal Regolamento (UE) 2016/679 "*relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali, nonché alla libera circolazione di tali dati*", ossia il **Regolamento Generale sulla Protezione dei Dati (GDPR)**.

Alla luce del GDPR l'Italia ha poi modificato, nel 2018, il proprio precedente Codice della privacy (D.Lgs. n. 196/2003) per adeguarsi alle innovazioni portate dalla nuova norma, mediante il D.Lgs. n. 101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679). Il principale punto di riferimento resta, comunque, il GDPR, che è direttamente applicabile, mentre la normativa di fonte italiana assume rilievo di norme di contorno e completamento.

Gran parte delle norme previste dal GDPR si incentrano essenzialmente su un criterio di **gestione del rischio (risk management)**, che, come vedremo, impernia non soltanto la normativa in materia di data protection, ma anche gran parte delle vigenti e future regole in materia di "nuove tecnologie" (Intelligenza Artificiale, piattaforme, ecc.). Il principio consiste, in termini estremamente semplici, nell'obbligo di parametrare doveri e misure di sicurezza al rischio concreto connesso ad una determinata attività.

Qual è l'ambito applicativo del GDPR? In altri termini, a quali circostanze si applica il GDPR? In sintesi:

- il Regolamento tutela esclusivamente le persone fisiche, e non anche quelle giuridiche. Più in dettaglio, il GDPR:
    - tutela il diritto alla protezione del dato solo delle persone fisiche (in altri termini, l'interessato ai fini del GDPR può essere unicamente una persona fisica, e mai una persona giuridica); ma
    - impone obblighi e doveri (e sanzioni) sia alle persone fisiche che alle persone giuridiche, laddove esse trattino dati personali riferiti alle persone fisiche;

[1] Ad esempio, è stata accertato che il servizio di social network fornito da Facebook non può dirsi "gratuito" per il diritto, ed è stato dunque ordinato a Facebook di non utilizzare il claim che precedentemente poteva essere letto da tutti gli utenti nella pagina del sito utilizzata per il login, ossia "Iscriviti. È gratis e lo sarà sempre". Questo perché Facebook riceve dagli utenti un gran numero di dati che vengono utilizzati, ad esempio, a fini di marketing e profilazione, quindi Facebook riceve un corrispettivo. Il "prezzo" del servizio reso da Facebook sono i dati degli utenti.

- si applica a tutti i trattamenti elettronici, cartacei e manuali di dati personali;
- per "trattamento di dati personali" si intende qualunque operazione che abbia ad oggetto uno o più dati personali (raccolta, registrazione, organizzazione, conservazione, estrazione, consultazione, uso, comunicazione, diffusione, cancellazione, ecc.) Dunque, qualsiasi attività venga svolta con dati personali rientra nell'applicazione del GDPR.

  A tal fine non rileva che il dato sia raccolto o estratto da chi pone in essere l'attività. Anche la semplice conservazione di dati raccolti da altri, o la loro mera consultazione, o la comunicazione a soggetti terzi di dati raccolti da altri costituiscono "trattamento" ai fini dell'applicazione del GDPR. Lo stesso vale anche per la cancellazione o la distruzione di dati, anche laddove questi siano stati raccolti da soggetti diversi da chi poi li cancella o li distrugge;
- ha efficacia anche extraterritoriale, nel senso che si applica:
  - a tutti i trattamenti di dati effettuati da chiunque abbia sede nel territorio dell'Unione Europea, indipendentemente dal luogo in cui avviene il trattamento (indipendentemente, dunque, dal fatto che il trattamento sia materialmente effettuato o meno nell'Unione Europea, quindi anche al caso di imprese con sede nell'Unione Europea ma che svolgano attività unicamente in territori extra-UE);
  - a tutti i trattamenti svolti all'estero (fuori dall'UE) se e quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi a interessati che si trovano, anche "virtualmente", nell'Unione Europea (indipendentemente, quindi, dalla cittadinanza o dal titolo della permanenza degli interessati nell'Unione, che potrebbe essere anche solo temporanea);
- non si applica ai trattamenti posti in essere da persone fisiche per l'esercizio di attività a carattere esclusivamente personale o domestico (è la c.d. "*household exemption*").

I "protagonisti" del trattamento di dati personali

Quali sono gli "attori" del trattamento dei dati personali? In altri termini, quali sono i soggetti che il GDPR prende in considerazione per disciplinare come devono essere trattati i dati personali? Essi sono, in sintesi:

- l'interessato (il data subject), ossia la persona fisica alla quale si riferiscono i dati (la persona fisica, dunque, in relazione alla quale il dato veicola informazioni);
- il titolare del trattamento (il data controller), ossia la persona fisica o giuridica (ivi incluse le autorità pubbliche) che, singolarmente o insieme ad altri, determina le finalità, le modalità ed i mezzi del trattamento di dati personali dell'interessato e (spesso) pone in essere il trattamento.

  N.B.: nel caso di persona giuridica (società, ente, autorità pubblica, ecc.) il titolare è l'entità nel suo complesso e non le persone fisiche che "lavorano" per quell'entità (dipendente che materialmente compie attività sul dato, l'amministratore delegato, il dirigente responsabile, ecc.).

Per un determinato trattamento vi può essere anche più di un titolare. In questo caso si parla di "contitolari del trattamento", ossia due o più soggetti che stabiliscono insieme le finalità e le modalità del trattamento mediante un accordo interno tra loro. La presenza di più titolari del trattamento deve essere resa nota all'interessato. Ad esempio, si pensi al caso in cui un cliente affida un mandato difensivo a due avvocati invece che ad uno solo: in questo caso entrambi gli avvocati sono titolari, a pari titolo, del trattamento dei dati del cliente;

- il responsabile del trattamento (il data processor), ossia la persona fisica o giuridica (ivi incluse le autorità pubbliche) che tratta dati personali per conto del titolare del trattamento. È il soggetto (o i soggetti) che il titolare del trattamento eventualmente incarica di trattare i dati secondo le proprie istruzioni. Il titolare può anche direttamente trattare i dati, senza nominare alcun responsabile del trattamento, ma, se nomina un responsabile, il titolare ha poi il dovere di vigilare sull'osservanza delle proprie istruzioni da parte del responsabile.

  Ad esempio, si pensi ad una compagnia telefonica che incarichi una specifica agenzia di porre in essere attività di call center e marketing in una determinata zona e per un bacino di utenza individuato dalla compagnia telefonica stessa: in questo caso, la compagnia telefonica è il titolare del trattamento, mentre l'agenzia è il responsabile del trattamento;

- il soggetto autorizzato, ossia la persona fisica che il titolare o il responsabile del trattamento devono espressamente individuare all'interno della propria organizzazione e che materialmente compie le operazioni del trattamento (che può, naturalmente, essere solo una persona fisica). Si tratta di un soggetto che deve essere istruito e formato sulle modalità per lo svolgimento dell'attività;

- il Data Privacy Officer (DPO), ossia una persona fisica che deve essere designata dal titolare in caso vengano posti in essere trattamenti particolarmente "sensibili" o "complessi". In particolare, il DPO deve essere designato se:

  - il trattamento è effettuato da una pubblica amministrazione;
  - il trattamento richiede un monitoraggio regolare e sistematico degli interessati su larga scala;
  - il trattamento è effettuato su larga scala su dati sensibili (compresi i dati genetici e biometrici) e/o dati giudiziari.

  Il DPO deve avere una posizione di indipendenza rispetto al titolare. La sua funzione è quella di inserire nell'organizzazione del titolare un soggetto qualificato che gli fornisca consulenza in merito agli obblighi derivanti dalla normativa in materia di data protection, che vigili sull'osservanza di tale normativa, che ponga in essere attività di sensibilizzazione e formazione del personale e che eventualmente cooperi con il Garante per la Protezione dei Dati Personali.

  L'identità ed i contatti del DPO devono essere resi noti agli interessati.

In Italia esiste una autorità pubblica indipendente alla quale è attribuito il compito di sorvegliare sull'applicazione della normativa in materia di trattamento di dati personali al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche. Si tratta del **Garante per la protezione dei dati personali** (GPDP, comunemente noto come "Garante per la privacy", anche se tale nome non è rigorosamente corretto).

I principi fondamentali del trattamento dei dati personali

Il trattamento dei dati personali è consentito solo qualora sia necessario per adempiere alle finalità per le quali i dati sono stati raccolti, nei limiti dei dati necessari per gli scopi della raccolta e delle operazioni strettamente indispensabili per gli scopi stessi. I dati personali devono essere "*trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*" (art. 5 GDPR).

Il titolare del trattamento deve mettere in atto (ed essere in grado di dimostrare di avere messo in atto) misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al GDPR.

Secondo il GDPR il trattamento di dati personali deve essere effettuato nel rispetto dei seguenti principi:

- **liceità**: occorre rispettare tutte le norme dell'ordinamento giuridico, non solo il GDPR e comunque quelle in materia di data protection;
- **trasparenza**: l'interessato deve sapere che i suoi dati sono oggetto di un trattamento, e quali dati lo sono;
- **limitazione delle finalità**: i dati oggetto di trattamento devono essere raccolti per finalità determinate ed esplicite (ossia comunicate chiaramente all'interessato) e successivamente trattati in conformità a tali finalità (ossia per gli scopi per i quali sono raccolti, e non per altri)[2];
- **esattezza dei dati**: i dati oggetto di trattamento devono essere esatti e, se necessario, aggiornati. Devono, dunque, essere adottate tutte le misure ragionevolmente esigibili per cancellare o rettificare tempestivamente dati che risultino inesatti rispetto alle finalità del trattamento;
- **minimizzazione dei dati**: i dati devono essere adeguati, pertinenti e limitati a quanto necessario per gli scopi del trattamento e non devono, dunque, eccedere rispetto alle finalità per cui sono raccolti o sono successivamente trattati;
- **limitazione della conservazione**: i dati devono essere conservati per un arco di tempo non superiore al conseguimento degli scopi per i quali sono trattati. Una volta raggiunto lo scopo del trattamento, i dati devono essere resi anonimi o cancellati.

Questi principi devono essere rispettati di default, sin dall'inizio della progettazione dell'attività in questione, prevedendo tutte le garanzie indispensabili al fine di tutelare i diritti degli interessati. Si parla, infatti, del principio della **privacy by default**, che prevede che le impostazioni di tutela della vita privata relative ai servizi e prodotti rispettino i principi generali della protezione dei dati, quali, per l'appunto, la minimizzazione dei dati e la limitazione delle finalità. Gli applicativi informatici devono, dunque, essere progettati a monte per rispettare tali principi, prima di procedere al trattamento dei dati vero e proprio.

Quanto al trasferimento dei dati all'estero (ossia, ai fini del GDPR, a soggetti situati al di fuori dell'Unione Europea), in termini generali il trasferimento è di base vietato qualora

[2] Unica eccezione considerata dal GDPR è quella dell'eventuale trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, che il GDPR considera comunque sempre compatibili con gli scopi originari del trattamento.

la legislazione del paese di destinazione non assicuri un livello di tutela adeguato (valutazione, questa, che spetta alla Commissione Europea). In caso contrario, il trasferimento verso paesi terzi può avvenire solo nel rispetto di alcune garanzie previste dal GDPR. Questo per evitare che venga aggirata la normativa di tutela prevista dal GDPR acquisendo dati in Europa e trattandoli, poi, all'estero, in paesi che non prevedano le garanzie contemplate dalla normativa UE.

Le basi giuridiche del trattamento

Il trattamento dei dati, secondo il GDPR, è lecito solo se viene svolto in presenza di una condizione che lo legittima, ossia di una base giuridica.

Le possibili basi giuridiche che legittimano il trattamento sono le seguenti:

a. il **consenso dell'interessato**, che deve essere prestato liberamente ed essere effettivo. In relazione a ciò:
    - occorre domandarsi quando possa essere definito "effettivo" e "libero" il consenso, anche in relazione alla comprensibilità delle informazioni che il titolare rende all'interessato per chiedergli il consenso (ossia l'informativa, v. sotto). Sicuramente non è libero, e dunque valido, il consenso ottenuto con violenza o minaccia o inducendo l'interessato in errore[3];
    - il consenso può essere prestato in qualunque forma, scritta od orale, fermo restando che il titolare del trattamento deve comunque essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento (il che può essere più complesso in presenza di un consenso non scritto);
b. il caso in cui il trattamento occorra per adempiere ad **obblighi legali**;
c. il caso in cui il trattamento sia **necessario per l'esecuzione di obblighi di un contratto del quale è parte l'interessato** (ossia nel caso in cui il soggetto X non possa eseguire un contratto che ha sottoscritto con Y se non trattando dei dati relativi ad Y);
d. il caso in cui il trattamento sia necessario per **perseguire un legittimo interesse del titolare del trattamento o di terzi**, ove si tratti di un interesse che, nel bilanciamento con quello alla protezione dei dati, prevalga su quest'ultimo;
e. il caso in cui il trattamento sia **necessario per l'interesse pubblico** (ad esempio, qualora il trattamento sia effettuato dalla Pubblica Amministrazione, ma solo nei limiti in cui il trattamento serva all'adempimento dei fini istituzionali dell'ente).

Nei casi di cui ai punti b., c. e d. di cui sopra, e solo in tali casi, il trattamento dei dati è legittimo anche senza il consenso dell'interessato, che costituisce, al di là di tali ipotesi, la regola generale in materia di data protection.

I dati "particolari"

Il GDPR disciplina in modo parzialmente differente, con ulteriori cautele, due categorie di dati ritenuti "particolari", ossia:

[3] L'età alla quale può essere validamente prestato il consenso è "abbassata" dall'UE a 16 anni (14 anni per l'Italia).

- **dati sensibili**: sono i dati suscettibili di rivelare l'origine etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale dell'interessato o comunque dati genetici, biometrici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona. Sono dati il cui trattamento può essere particolarmente lesivo dei diritti e delle libertà fondamentali dell'interessato, in quanto potenzialmente fonte di discriminazioni.

  Tali dati non possono essere oggetto di trattamento a meno che:

  - non vi sia il consenso esplicito dell'interessato per una o più finalità specifiche;
  - tali dati non siano stati resi manifestamente pubblici dall'interessato (il quale perde, dunque, in tal caso l'interesse al mantenimento del segreto);
  - il loro trattamento non serva per tutelare la salute di terzi;
  - il loro trattamento non serva per altre ipotesi (la gestione del rapporto di lavoro, finalità archivistiche, ecc.);
- **dati giudiziari**: sono i dati relativi alle condanne penali ed ai reati, per il cui trattamento valgono le basi giuridiche di cui sopra, ma subordinatamente al controllo dell'autorità pubblica e nei casi previsti dalla legge.

Gli adempimenti previsti in capo al titolare (o al responsabile)

I. Le misure di sicurezza

Il GDPR impone al titolare ed al responsabile di mettere in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio. Sono imposte, dunque, forme di tutela preventiva per evitare la lesione dei diritti tutelati dalla normativa.

Il principio-base è quello della gestione del rischio (risk management), in base al quale:

- occorre individuare quali sono i rischi specifici e concreti che una determinata attività o trattamento pone (ad esempio, perdita di dati, accesso ai dati da parte di soggetti non autorizzati, ecc.) e quali conseguenze possano derivarne per l'interessato (da modulare, naturalmente, in relazione alla tipologia di dati dei quali si tratta);
- individuare e porre in essere, sulla base della ricognizione di cui al precedente punto e tenendo conto dello stato dell'arte e dei costi di attuazione, le misure specificamente utili a scongiurare quegli specifici rischi, con un approccio, potremmo dire, tailormade rispetto al rischio.

Non può esistere, dunque, una "one-size-fits-all solution" e misure di sicurezza standard applicabili per tutti i casi, ma l'approccio che la normativa esige è di tipo concreto e specifico. Nella scelta delle misure tecniche ed organizzative occorre, poi, effettuare un bilanciamento tenendo conto anche della proporzionalità rispetto ai costi delle misure stesse (non è obbligatorio porre in essere soluzioni tecnologicamente avanzate ove le stesse risultino, in concreto, economicamente troppo onerose rispetto al business del titolare e, soprattutto, ai concreti rischi connessi alla sua attività).

A tal fine, è indispensabile che venga condotta una valutazione preventiva d'impatto sulla protezione dei dati, ossia il cosiddetto **Data Protection Impact Assessment**

(DPIA), volto a ponderare ex ante l'incidenza che una determinata soluzione tecnica potrà avere sulla tutela dei dati trattati, analizzando i vari possibili casi in ragione delle specificità correlate alle modalità di gestione delle informazioni. Il DPIA:

- si colloca, in primo luogo, in una fase preliminare dello sviluppo del prodotto o del servizio, ovvero quando il suo design non è delineato in maniera definitiva, bensì è ancora in uno stadio progettuale;
- deve essere ripetuto prima dell'attivazione del trattamento;
- deve essere effettuato anche successivamente con cadenza periodica.

Il DPIA può essere effettuato sempre, ma diventa obbligatorio se il rischio connesso al tema della protezione dei dati è elevato in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, specialmente in caso di utilizzo di nuove tecnologie (ad esempio, in caso di trattamento automatizzato; cfr. art. 22 GDPR), oppure quando si effettuano trattamenti di dati "particolari" (v. sopra), oppure quando il trattamento comporta la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Abbiamo già parlato sopra del principio della **privacy by default**, che deve guidare il titolare nell'approntare le misure di sicurezza idonee, che "di default" devono rispettare i principi che abbiamo già esaminato sopra.

Altro principio generale del GDPR, che si accompagna a quello di privacy by default, è quello detto della "**privacy by design**", da molti interpretato come il futuro della legislazione in materia di data protection (ma in realtà il principio del "by design" ispirerà probabilmente molta parte della legislazione delle nuove tecnologie ed in particolar modo dell'Intelligenza Artificiale, facendo della tecnologia il veicolo per garantire ex ante, a monte, il rispetto delle regole).

Si tratta di un principio secondo il quale la tutela dei dati personali deve essere incorporata a partire dalla progettazione di ogni processo aziendale (deve essere, in altri termini, uno dei presupposti sulla base dei quali si devono predisporre i processi aziendali, embedded ed incorporato "nel suo DNA", potremmo dire), anche e soprattutto nel ricorso alle relative applicazioni informatiche di supporto.

Si parla, ad esempio, della messa in atto, già nella progettazione dei sistemi informatici, di determinati meccanismi volti garantire che il sistema, a priori, non tratti dati personali per scopi diversi rispetto a quelli programmati, con apposite "barriere" e "blocchi". L'esigenza di protezione dei dati deve, dunque, essere considerata già nella fase di progettazione, e non solo a posteriori. In termini semplici: non posso progettare un determinato sistema e solo dopo chiedermi se quest'ultimo tuteli i dati personali degli interessati, ma devo pormi questa domanda prima, nel momento in cui inizio a progettare il sistema stesso.

Il principio della privacy by design richiede che la tutela dei diritti e delle libertà degli interessati con riguardo al trattamento dei dati personali comporti l'attuazione di adeguate misure tecniche e organizzative al momento sia della progettazione che dell'esecuzione del trattamento stesso, nell'intero ciclo di vita della tecnologia.

Ad esempio, a seconda dei casi le misure di sicurezza adeguate devono prevedere:

- la pseudonimizzazione e la cifratura dei dati personali;

- la capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico;
- la capacità di assicurare la resilienza dei sistemi e dei servizi di trattamento (anche in termini di cybersecurity);
- una procedura di testing periodico per valutare regolarmente l'efficacia concreta delle misure adottate.

II. La predisposizione dell'informativa da fornire all'interessato

Prima della raccolta dei dati o al momento della raccolta il titolare deve fornire all'interessato la cosiddetta "informativa", finalizzata a consentirgli di esprimere un consenso al trattamento effettivamente informato.

L'informativa può essere fornita per iscritto, oralmente o con altri mezzi, ma occorre sempre tenere in considerazione, nella scelta della modalità con la quale rendere l'informativa, che il titolare potrebbe essere chiamato a dimostrare di avere reso l'informativa all'interessato (nel qual caso, un'informativa resa per iscritto agevolerebbe sicuramente l'adempimento a tale onere probatorio). Comunque l'informativa può essere resa oralmente solo se richiesto dall'interessato.

L'informativa deve:

- recare tutte le informazioni utili ad identificare il trattamento (modalità, finalità, durata e base giuridica del trattamento);
- essere concisa, trasparente e comprensibile, con un linguaggio semplice e chiaro;
- informare sulla natura del conferimento dei dati, ossia deve specificare se il conferimento dei dati da parte del titolare è facoltativo od obbligatorio in relazione a determinate finalità. Quindi occorre anche informare sulle eventuali conseguenze del rifiuto di conferire dati (ad esempio, l'impossibilità di eseguire un determinato servizio in assenza di conferimento di dati);
- indicare i dati, inclusi i contatti, del titolare e dell'eventuale responsabile;
- informare sui soggetti ai quali i dati potranno essere comunicati e sull'eventuale trasferimento all'estero (fuori dall'UE) degli stessi;
- informare sui diritti previsti dal GDPR per l'interessato (accesso, rettifica, cancellazione, portabilità, limitazione, opposizione; v. infra, pag. 13);
- informare sulla possibilità di revocare il consenso;
- informare sulla possibilità di proporre reclamo all'autorità di controllo (il Garante per la Protezione dei Dati Personali, il quale può adottare sanzioni nei confronti di chi viola la normativa in materia di data protection ed ingiungere di modificare il proprio comportamento).

Se i dati vengono acquisiti da soggetti diversi dall'interessato, non potendosi fornire l'informativa all'interessato stesso al momento dell'acquisizione, l'informativa deve essere fornita alla persona che fornisce i dati per poi comunicarla anche all'interessato entro un mese dall'ottenimento dei dati (cosiddetta informativa postuma).

III. La nomina del DPO (v. sopra)

IV. La tenuta del Registro delle attività di trattamento

Talune tipologie di titolari del trattamento devono tenere un **Registro delle attività di trattamento**, ossia un registro nel quale tenere traccia di tutti i trattamenti svolti presso il titolare. A tale obbligo sono tenuti:

- i titolari che abbiano oltre 250 dipendenti;
- i titolari che, pur avendo meno di 250 dipendenti, effettuano trattamenti:
    - che possano presentare rischi per i diritti e le libertà degli interessati; oppure
    - che non siano occasionali; oppure
    - che includano dati di natura particolare.

Il Registro può essere conservato anche solo in formato elettronico e deve contenere, tra l'altro, le seguenti indicazioni:

- finalità del trattamento;
- descrizione delle categorie di interessati e delle categorie di dati personali trattati;
- categorie di destinatari ai quali i dati saranno eventualmente comunicati;
- eventuali trasferimenti di dati verso paesi non UE;
- descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

V. La segnalazione all'autorità di controllo in caso di data breach

Il titolare è obbligato a notificare all'autorità di controllo e, nei casi più rilevanti, ai diretti interessati le violazioni dei dati personali dell'interessato dovute a violazioni dei propri sistemi informatici. La notifica deve essere effettuata senza ritardo e, comunque, entro 72 ore dal momento in cui il titolare è venuto a conoscenza del data breach.

La notifica non è obbligatoria sempre, ma la sua effettuazione è subordinata alla **valutazione del rischio per gli interessati**, che spetta al titolare, il quale la effettua sotto la propria responsabilità.

I trattamenti interamente automatizzati (e la profilazione)

Il GDPR prevede il diritto dell'interessato di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, laddove la decisione in questione produca effetti giuridici che lo riguardano o incida in modo significativo sulla sua persona (**art. 22 del GDPR**).

È un trattamento automatizzato di dati anche la cosiddetta **profilazione**. Per "profilazione" si intende l'insieme di attività di raccolta ed elaborazione automatizzata di dati inerenti alle persone fisiche che utilizzano un certo servizio al fine di suddividerli in gruppi a seconda del loro comportamento, con conseguente possibilità di adottare decisioni che li riguardano ed analizzare e prevedere le loro preferenze e i loro comportamenti futuri. In ambito commerciale, ad esempio, tale attività coincide con la definizione dei gusti e delle propensioni all'acquisto di un determinato consumatore mediante il monitoraggio delle attività che quest'ultimo compie sul web. Ciò al fine di consentire, ad esempio, offerte targettizzate o anche solo al fine di compiere indagini di

mercato o di ricerca e sviluppo, oppure di individuare su quali prodotti o settori è preferibile investire.

Sono automatizzati, fra gli altri, anche i trattamenti effettuati per l'analisi dei Big data, i quali sono analizzati ed elaborati grazie a sistemi di Intelligenza Artificiale.

L'assunzione di decisioni unicamente sulla base di un trattamento automatizzato, anche laddove comporti effetti significativi, è possibile solo in tre casi:

- se lo prevede la legge;
- se l'interessato ha dato il proprio espresso (effettivo e consapevole) consenso in tal senso (inteso come espresso, effettivo e consapevole consenso a sottoporsi al trattamento interamente automatizzato, non al trattamento in generale) → indispensabile se sono oggetto di trattamento automatizzato dati "particolari" (v. sopra);
- se è necessaria per l'esecuzione di un contratto sottoscritto dall'interessato.

In tali casi, deve comunque essere garantito il diritto dell'interessato:

- di **ottenere l'intervento umano** da parte del titolare;
- di **contestare la decisione** raggiunta mediante trattamento interamente automatizzato.

In ogni caso, l'interessato deve essere sempre informato non solo sull'esistenza del trattamento interamente automatizzato, ma anche sulle logiche e sui meccanismi mediante i quali il trattamento interamente automatizzato funziona (**diritto alla spiegazione**). L'informazione fornita deve essere **significativa** (quindi illustrativa delle caratteristiche del sistema e funzionale a garantirne la conoscibilità e la comprensibilità da parte dell'interessato)

Ma quale spiegazione è necessaria e sufficiente? In altri termini, sino a dove occorre spingersi nello spiegare all'interessato i meccanismi (talora anche molto complessi) sulla base dei quali il trattamento automatizzato è effettuato, le logiche seguite dall'algoritmo, ecc.? Quanto dettagliata deve essere l'informativa al riguardo?

Occorre anche considerare che l'informativa deve essere sempre **comprensibile** da chiunque, quindi anche da soggetti non esperti di tecnologie informatiche.

→ Esiste, dunque, l'esigenza di tenere in considerazione il **trade-off tra completezza dell'informazione resa e sua comprensibilità**.

→ La Corte di Cassazione ha recentemente (maggio 2021) affermato, con riguardo ad un caso concernente un sistema automatizzato utilizzato da una piattaforma per la definizione del rating reputazione[4], che:

- il consenso dell'interessato è fondamentale per la liceità del trattamento in questione;

[4] In particolare, il caso aveva ad oggetto un sistema informatico costituito da una piattaforma web (con annesso archivio informatico) il cui scopo era la elaborazione di profili reputazionali concernenti persone fisiche e giuridiche al fine di contrastare fenomeni basati sulla creazione di profili artefatti o "fasulli" e di calcolare, invece, in maniera imparziale il cd. "rating reputazionale" dei soggetti censiti, per modo da consentire a eventuali terzi una verifica di reale credibilità.

- il consenso dell'interessato deve essere effettivo e, a tal fine, deve essere consapevole e informato;
- di conseguenza, l'adesione ad una piattaforma da parte dell'interessato non comprendere di per sé anche l'accettazione di un sistema automatizzato che si avvale di un algoritmo per la valutazione di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati.

Il problema è, dunque, quello della **trasparenza vs. opacità dell'algoritmo** e dei processi decisionali "animati" dall'algoritmo. Il problema è particolarmente incidente per quei sistemi complessi per i quali lo stesso creatore o utilizzatore (dunque lo stesso titolare del trattamento) del sistema potrebbe avere problemi nella identificazione del processo decisionale e della motivazione sulla base della quale il sistema ha raggiunto una determinata conclusione.

Settori ed attività particolarmente interessati dalla problematica sono, ad esempio, i seguenti:

- attività di *credit scoring* (ai fini, ad esempio, del riconoscimento di un mutuo);
- attività della Pubblica Amministrazione che assuma decisioni sulla persona (provvedimenti) mediante trattamento automatizzato;
- attività giudiziaria ("sentenze robotiche");
- attività sanitarie (diagnostica).

I diritti dell'interessato

Il GDPR disciplina specifici diritti che possono essere esercitati dall'interessato in relazione al trattamento dei propri dati personali. In generale, questi diritti non sono "assoluti", ma devono essere sempre bilanciati con altri eventuali diritti del titolare del trattamento (ad esempio, l'esercizio del diritto di difesa in tribunale, oppure motivi di interesse pubblico rilevante, oppure per tutelare i diritti di un'altra persona fisica).

In particolare, tali diritti sono:

- diritto di **ottenere la conferma dell'esistenza di un trattamento di dati che lo riguardano**;
- diritto di **accedere ai dati** ed alle informazioni concernenti il trattamento (finalità, categorie di dati trattati, destinatari ai quali i dati saranno o sono stati comunicati, periodo di conservazione dei dati ed in generale le informazioni che devono essere oggetto dell'informativa);
- diritto di chiedere la **rettifica dei dati**, ossia il diritto di domandare la modifica dei dati trattati e la loro integrazione (aggiungendo dati a quelli già trattati dal titolare). Tale diritto può essere esercitato sempre in relazione alla finalità del trattamento (in altri termini, non posso ottenere la rettifica o l'integrazione dei dati se la modifica richiesta non ha nulla a che vedere con lo scopo del trattamento e non serva al miglior perseguimento di tale scopo);
- diritto di ottenere la **cancellazione dei dati**, qualora i dati non siano più necessari rispetto alla finalità del trattamento o in caso di trattamento illecito o qualora l'interessato abbia revocato il proprio consenso;

- diritto di chiedere la **limitazione del trattamento**, ossia il diritto di chiedere che i dati vengano soltanto conservati, con impossibilità di svolgere qualsiasi altra operazione mediante o in relazione ad essi;
- diritto di **opposizione**, ossia il diritto di chiedere che il trattamento venga cessato quando si tratta di trattamento svolto per finalità di marketing;
- diritto alla **portabilità dei dati**, a fronte del quale l'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da un dispositivo automatico, i dati personali che lo riguardano ed ha diritto di trasmettere tali dati ad un altro soggetto che ne diventa il titolare del trattamento[5].

Le conseguenze di eventuali violazioni della normativa in materia di data protection

- responsabilità civile: obbligo in capo al titolare del trattamento (o al responsabile del trattamento, a seconda dei casi) di **risarcire all'interessato il danno** da quest'ultimo subito per effetto delle violazioni.

  Il risarcimento del danno viene determinato in base alle regole generali previste dal codice civile (sia danno patrimoniale che danno non patrimoniale; spesso si tratta di danno morale). L'obbligazione al risarcimento del danno sorge in qualunque caso in cui il danno subito dall'interessato sia in rapporto di causa-effetto con la violazione di una delle norme in materia di data protection.

  Per andare esente dall'obbligo di risarcimento, il titolare del trattamento deve dimostrare di avere adottato tutti gli accorgimenti previsti dalle norme in materia.

  Il trattamento di dati personali è "attività pericolosa"?

- responsabilità amministrativa: in caso di violazioni, il Garante per la protezione dei dati personali può imporre **sanzioni amministrative** in capo al titolare del trattamento.

  L'ammontare delle sanzioni, da 10 a 20 milioni di Euro, è proporzionato al fatturato mondiale annuo (2% o 4% del fatturato mondiale annuo, secondo il GDPR, a seconda della gravità della violazione e delle specifiche norme violate).

Profili di data protection online: i deepfake, le regole sui cookies, il trasferimento dei dati all'estero e il diritto alla deindicizzazione

1. Il fenomeno del deepfake

Il termine "*deepfake*", neologismo nato dalla combinazione di "*deep learning*" e "*fake*", si riferisce ad immagini, video o contenuti audio creati utilizzando tecniche di Intelligenza Artificiale (A.I.) - tra cui Generative Adversarial Networks (GANs) o Variational Auto-Encoders (VAEs) - volte a combinare, alterare, sovrapporre immagini o video originali ritraenti una persona con materiali ritraenti soggetti diversi, e dunque a simulare in modo estremamente realistico la voce, il volto, il corpo ed i movimenti di una persona. Vengono, così, generati audio, immagini o video **completamente falsi** che sono,

[5] Tale diritto può essere esercitato solo se il trattamento ha come base giuridica il consenso o l'esecuzione di un contratto e solo se i dati in questione sono oggetto di trattamento automatizzato (altrimenti l'onere imposto al titolare sarebbe eccessivo).

tuttavia, **difficilmente riconoscibili come tali**, anche ad occhio esperto (ed anche per gli stessi algoritmi impiegati per il deepfake detection).

Mediante tali sistemi, dunque, il volto di una persona può essere innestato sul corpo di un'altra, la voce di un soggetto può essere associata ad una persona diversa, i movimenti del corpo possono essere manipolati ed artefatti, le persone possono essere collocate in luoghi e contesti non reali, o comunque nei quali non si sono mai trovate, o possono sembrare pronunciare parole mai effettivamente pronunciate. I sistemi in questione possono, quindi, diventare lo strumento per la realizzazione di gravi forme di **furto d'identità** ai danni delle persone che compaiono in un prodotto deepfake, i quali subiscono una perdita di controllo non solo sulla (circolazione della) propria immagine, spesso carpita dai social network, ma anche delle proprie idee e dei propri pensieri, che possono essere oggetto di falsificazione e travisamento agli occhi di terzi; il tutto, sovente all'insaputa dell'interessato.

Accanto ad impieghi "virtuosi" delle tecnologie di deepfake (si pensi, ad esempio, in ambito sanitario, ai documentati impieghi di tali sistemi per "ridare la voce" a pazienti la cui capacità di parola era stata compromessa per effetto di malattie irrimediabilmente invalidanti; o, ancora, agli impieghi nel settore cinematografico o lato sensu artistico, oppure a fini satirici o parodistici), suscitano seria preoccupazione - anche in materia di data protection - i sempre crescenti fenomeni di applicazione di sistemi di deepfake con finalità decisamente meno edificanti ed addirittura lesive. Si pensi, ad esempio:

- al contributo che tali tecnologie forniscono ai dilaganti fenomeni di disinformazione ed alla creazione e diffusione di fake news, la cui circolazione, peraltro, è suscettibile di minare non soltanto la generale capacità del pubblico di distinguere il falso dal vero, ma anche di fidarsi di ciò che è effettivamente reale (è il fenomeno del c.d. liar's dividend);
- agli effetti che tali pratiche possono sortire in termini di distorsione dell'opinione pubblica, con immagini, audio o video deepfake suscettibili di essere mostrati od inviati agli elettori per dissuaderli dal votare un determinato candidato o per indurli a votarne uno diverso;
- all'impiego di tecnologie di deepfake per l'esecuzione di truffe mirate, ad esempio per raggirare la vittima e persuaderla a fornire dati personali o a compiere atti di disposizione patrimoniale (c.d. "spoofing"), o per aggirare sistemi di identificazione e riconoscimento facciale (il c.d. "morphing");
- all'utilizzo di tali sistemi per produrre pornografia, creando immagini e video falsi ma estremamente realistici di persone in atti sessuali, in situazioni compromettenti mai verificatesi, oppure ricostruendo in modo verosimile l'aspetto che avrebbe un determinato corpo umano sotto gli abiti, realizzando immagini di nudo adattate alla corporatura ed alle proporzioni del soggetto: è il c.d. "deepnude" (si stima che più del 95% delle applicazioni di tecnologie deepfake disponibili sul mercato sia attualmente impiegato per la produzione di varie forme di pornografia, realizzando prodotti che possono essere usati anche a finalità ricattatorie, o per screditare avversari politici). E si pensi, ancora, alle possibili ricadute su fenomeni quali il c.d. "revenge porn" o il cyberbullismo.

Non v'è dubbio che **i contenuti utilizzati per la creazione di deepfake (audio, immagini, video) possano costituire "dati personali" ai sensi del GDPR**, se ed in quanto idonei a consentire l'identificazione dei soggetti ai quali sono riferiti, e che la loro

manipolazione ad opera dei sistemi di A.I. usati per creare deepfake rappresenti un **"trattamento di dati"**[6].

Emergono due problemi principali al riguardo:

- Un primo tema concerne l'applicabilità delle regole, e delle tutele, previste dal GDPR a fattispecie quali quelle in esame, anche alla luce della c.d. "*household exemption*" prevista dal Regolamento, in virtù della quale, come si è visto, il GDPR non si applica ai trattamenti effettuati da una persona fisica "*per l'esercizio di attività a carattere esclusivamente personale o domestico*", in assenza, dunque, di "*una connessione con un'attività commerciale o professionale*".

→ Nell'interpretare l'estensione dell'ambito applicativo del GDPR, la Corte di Giustizia dell'Unione Europea tiene in considerazione, tra gli altri fattori, anche la fonte dalla quale i dati trattati vengono raccolti. Si è, ad esempio, affermato che la "*household exemption*" non può applicarsi laddove i dati personali in questione siano stati raccolti da una fonte di dominio pubblico, come i social media; e nemmeno se essi siano poi condivisi online, anche sui social media stessi. L'applicabilità dell'esenzione in parola deve, quindi, essere necessariamente valutata in considerazione delle specificità del caso concreto, ma non sembra possibile escludere a priori l'applicabilità del GDPR ai fenomeni in esame.

- Un secondo tema attiene alla individuazione di quale debba essere la sottostante base giuridica idonea a legittimare tali trattamenti di dati. Fermo restando che in ipotesi quali quelle di impiego di sistemi di deepfake per l'esecuzione di truffe o per la creazione e diffusione di deepnude nessuna base giuridica può legittimare siffatti trattamenti, nella maggior parte dei casi, l'unica base giuridica ammissibile non potrà che essere il consenso dell'interessato, mentre in altri casi ancora potrebbe valutarsi la possibilità di invocare la sussistenza di un interesse legittimo del titolare del trattamento all'utilizzo di tali dati (ad esempio, in caso di utilizzo per finalità satiriche o di critica politica); interesse, questo, in relazione al quale, tuttavia, deve sempre essere effettuata una operazione di bilanciamento con diritti ed interessi altrui, ed in particolare con i diritti dell'interessato.

Riconosciuta l'applicabilità delle norme di data protection ai casi in esame, l'interessato che veda la propria immagine e/o la propria voce utilizzata in prodotti deepfake in assenza del proprio consenso (o comunque in assenza di un legittimo interesse dell'utilizzatore ad effettuare tale trattamento) può ricorrere ai **rimedi** previsti dalla normativa, tra cui:

- il diritto ad ottenere la cancellazione dei propri dati;
- il diritto ad ottenere il risarcimento dei danni subiti.

L'esercizio di tali diritti può, tuttavia, rivelarsi, nella pratica, complesso, specialmente in considerazione delle difficoltà nel risalire al creatore dei deepfake e/o a colui che per la prima volta lo abbia messo in circolazione online. È probabile, dunque, che gli interessati rivolgano le proprie iniziative in via principale nei confronti delle piattaforme che dovessero ospitare tali contenuti, anche quali co-titolari del trattamento di dati in questione.

[6] Peraltro, è stato osservato come non soltanto i dati di input utilizzati per la creazione del deepfake possano costituire "dato personale" secondo la definizione del GDPR, ma come anche gli stessi prodotti deepfake possano diventare (veicolo di) dati personali relativi all'interessato che vi è ritratto.

Quanto ai fenomeni di **utilizzo di sistemi di deepfake a scopi di revenge porn**, ai sensi dell'**art. 612-ter del codice penale** ("*Diffusione illecita di immagini o video sessualmente espliciti*"), è punita la condotta di chi, "*dopo averli realizzati o sottratti*", "*invia, consegna, cede, pubblica o diffonde*" immagini o video a contenuto sessualmente esplicito destinati a rimanere private, senza il consenso della persona ritratta. Da più parti si dubita, tuttavia, della possibilità che la tutela offerta da tale norma possa estendersi anche alla diffusione di immagini o video non autentici, ma creati artificialmente (motivo per il quale è stata presentata una più specifica proposta di legge per punire l'impiego di sistemi quali quelli di deepfake per scopi di revenge porn; proposta che è, però, ancora all'esame del Parlamento).

Sul tema si sta muovendo anche il legislatore dell'Unione europea:

- la **proposta di Regolamento UE per un *Artificial Intelligence Act*** si limita a prevedere, allo stato, obblighi di trasparenza, e in particolare l'obbligo, in capo agli utenti di un sistema di A.I. "*che genera o manipola immagini o contenuti audio o video che assomigliano notevolmente a persone, oggetti, luoghi o altre entità o eventi esistenti e che potrebbero apparire falsamente autentici o veritieri per una persona ('deep fake')*", di rendere noto che il contenuto è stato generato o manipolato artificialmente → è un feature che deve essere aggiunto "by design" alle applicazioni di A.I. volte alla realizzazione di deepfake?;
- il ***Digital Services Act*** impone alle "*piattaforme online di dimensioni molto grandi*" che si avvedano della presenza di contenuti deepfake un obbligo di "etichettarli" come tali, "*in modo da informare in maniera chiaramente visibile per il destinatario dei servizi che si tratta di contenuti non autentici*".

2. La disciplina dei cookies

Esistono diverse tecniche utilizzate per raccogliere dati online e costituire, attraverso esse, un profilo dell'utente. Una di queste prevede l'utilizzo di **cookies**, ossia stringhe di testo che il browser colloca all'apertura di una pagina web sul terminale (computer) dell'utente e che salvano i dati dell'utente durante la visita di un sito web agevolandone l'utilizzo (ad esempio, memorizzando le preferenze linguistiche o i dati di login). I dati vengono memorizzati per essere poi ritrasmessi agli stessi siti alla visita successiva del medesimo utente.

Mediante i cookies è anche possibile monitorare la navigazione e raccogliere dati inerenti i gusti, le abitudini e le scelte personali degli utenti, consentendo così la ricostruzione di profili degli utenti medesimi anche molto dettagliati (ad esempio, permettendo la personalizzazione delle inserzioni pubblicitarie sul browser).

Anche queste modalità comportano un trattamento di dati. Ma si tratta di dati "personali"?

Generalmente un cookie contiene l'indicazione sulla sua "durata di vita" e un numero generato in modo casuale che consente il riconoscimento del computer dell'utente. Di regola, la memorizzazione dei dati dei cookies avviene in modo anonimo. Quindi potremmo non essere in presenza di "dati personali" nel senso che prevede il GDPR, che potrebbe quindi non applicarsi a queste tipologie di trattamento.

Esiste, tuttavia, una specifica normativa, di derivazione europea, che disciplina l'utilizzo dei cookies al fine di tutelare l'utente da forme di profilazione "occulta" e di consentirgli di controllare la circolazione dei dati inerenti alla propria navigazione online,

subordinando la memorizzazione di tali mediante cookies al consenso dell'utente (principio dell'opt-in).

Esistono due tipologie di cookies:

- **cookies tecnici**, ossia quelli che sono necessari per motivi, per l'appunto, tecnici e comportano una forma indispensabile (e spesso solo temporanea) di memorizzazione di dati. Essi consentono la normale navigazione di un sito o la implementazione di un servizio desiderato dall'utente, limitandosi a salvare le preferenze ed i criteri di navigazione di ogni utente. Ad esempio, si pensi ai cookies di sessione per la memorizzazione delle preferenze linguistiche, o quelli che salvano i dati di login e del "carrello" per siti di e-shopping, e che possono essere eliminati una volta semplicemente chiuso il browser;
- **cookies di profilazione**, ossia quelli che non sono tecnicamente necessari per il funzionamento del sito. Si pensi, ad esempio, ai cookies di tracciamento, oppure ai cookies che creano profili personalizzati relativi all'utente per finalità pubblicitarie e vengono utilizzati principalmente per finalità di marketing (cookies di profilazione).

  Talora i cookies di profilazione possono essere anche cookies di terze parti, ossia di soggetti diversi dal gestore del sito nel quale vengono utilizzati che abbiano fatto un accordo con il gestore del sito per potervi installare propri cookies.

→ Secondo la normativa, i cookies tecnici possono essere usati anche senza chiedere il consenso dell'utente. Per gli altri cookies, invece, è necessario:

- che all'utente venga fornita una informativa chiara e completa in merito all'utilizzo dei cookies;
- che l'utente esprima un valido consenso, prima del trattamento.

Tali obblighi incombono sul gestore del sito web che usa i cookies.

Sono previste modalità "semplificate" di trasmissione della informativa e di raccolta del consenso, che si articolano su due livelli di approfondimento successivi:

1. nel momento in cui l'utente accede ad un sito web deve essergli presentata una prima informativa "breve", contenuta in un banner a comparsa immediata e ben visibile sulla home page o su ogni altra pagina alla quale sia possibile accedere direttamente. La richiesta di consenso all'uso dei cookie deve essere inserita già nel banner contenente l'informativa breve;
2. il banner contenente l'informativa breve deve, poi, contenere il link ad una informativa "estesa", letta la quale gli utenti possono differenziare le proprie scelte in merito ai diversi tipi di cookies archiviati tramite il sito in questione.

L'informativa "breve" deve già contenere, oltre al link all'informativa "estesa", l'informazione che il sito utilizza cookies di profilazione al fine di inviare messaggi pubblicitari in linea con le preferenze dell'utente manifestate nel corso della navigazione, l'indicazione dell'eventuale utilizzo di cookies di terze parti e l'indicazione che la prosecuzione della navigazione comporta la prestazione del consenso all'utilizzo dei cookies.

Dell'avvenuta prestazione del consenso all'utilizzo di cookies di profilazione occorre tenere traccia (anche mediante appositi cookies tecnici), il che consente poi al gestore

del sito di non riproporre l'informativa "breve" ad ogni successiva visita dello stesso utente al sito.

Particolare attenzione va riservata ai **cookies analitici**, che consentono di monitorare l'uso del sito da parte degli utenti (ad esempio, quali pagine visitano e qual è il sito di provenienza) e consentono di migliorare il sito stesso. Talora anche i cookies analitici possono essere di terze parti, e non dunque del "titolare" del sito.

Ci si è interrogati molto sulla possibilità o meno di considerare i cookies analitici come cookies tecnici, oppure come cookies di profilazione o comunque non aventi finalità meramente tecnica (in fin dei conti, si diceva, il titolare del sito trae un'utilità apprezzabile anche economicamente dal loro utilizzo, posto che grazie ad essi può migliorare il proprio sito, il suo funzionamento, la sua attrattività, ecc.). In generale si distingue tra:

- cookie analitici "di prima parte", ossia facenti capo al titolare del sito → sono assimilabili a quelli tecnici, e dunque utilizzabili senza consenso dell'utente del sito (ma sempre con informativa);
- cookie analitici di terze parti, per i quali è possibile una equiparazione ai cookie tecnici solo laddove i dati siano anonimizzati; in caso contrario, occorrerà ottenere il consenso dell'utente del sito.

3. Il trasferimento dei dati all'estero

I trasferimenti di dati personali verso Paesi non appartenenti allo Spazio Economico Europeo (ossia Unione europea + Norvegia, Liechtenstein, Islanda) o verso un'organizzazione internazionale sono **consentiti** se ricorre una delle seguenti condizioni:

a. l'adeguatezza del Paese terzo o dell'organizzazione è riconosciuta tramite decisione della Commissione europea (che successivamente alla decisione monitora al fine di controllare che le condizioni che hanno giustificato tale decisione continuino a permanere);
b. in assenza di tale decisione, ove il titolare o il responsabile del trattamento forniscano garanzie adeguate che prevedano diritti azionabili e mezzi di ricorso effettivi per gli interessati.

4. Il trattamento dei dati da parte dei motori di ricerca: il diritto alla deindicizzazione

Il tema della deindicizzazione, che si inserisce nel più ampio tema della cancellazione dei dati presenti online, riguarda una serie di problematiche anche molto incidenti sui diritti individuali: dal diritto del pubblico a reperire informazioni a problemi di *data protection* e di diritto all'identità personale, sino ai limiti del diritto dell'interessato alla cancellazione dei propri dati.

In estrema sintesi, il diritto alla deindicizzazione è il diritto dell'individuo ad ottenere, se ne ricorrono i presupposti, che un motore di ricerca **rimuova taluni risultati** da quelli che il motore stesso mostra all'utente all'esito di ricerche compiute usando come chiave il proprio nome. È il diritto a ottenere la rimozione di alcuni URL dai risultati di ricerca forniti dal motore all'esito di una *query* formulata a partire dal nome dell'interessato. In altri termini, è il diritto a rimuovere un determinato dato dalla rete, o da un suo particolare segmento, sottraendolo alla disponibilità degli internauti o rendendone meno agevole la reperibilità online.

I presupposti di tale diritto sono:

- il decorso di un significativo lasso di tempo dall'evento al quale il contenuto si riferisce (l'evento non deve essere più "attuale");
- la carenza di un generale interesse del pubblico;
- la lesività del contenuto, ossia la sua idoneità a danneggiare il soggetto al quale si riferisce.

La deindicizzazione è una attuazione del diritto individuale a chiedere che determinati dati e notizie non restino perennemente suscettibili di nuova e ingiustificata divulgazione online, anche per non vedersi attribuita una "biografia telematica" diversa da quella reale e costituente oggetto di notizie ormai superate.

Il gestore del motore di ricerca ha assunto un ruolo sempre meno "passivo" nella erogazione del servizio. Tanto che - come ribadito dalla giurisprudenza - l'attività del motore di ricerca consistente nel trovare informazioni pubblicate online da terzi, indicizzarle, memorizzarle temporaneamente e metterle a disposizione degli utenti secondo un ordine di preferenza deve essere qualificata come "trattamento di dati personali" del quale il gestore del *search engine* è il titolare; trattamento, questo, diverso e distinto da quello posto in essere dal gestore del sito sorgente sul quale il dato è stato originariamente pubblicato.

L'attività dei motori di ricerca comprende anche la realizzazione di copie delle pagine web indicizzate, dette **copie *cache***, le quali vengono conservate per un limitato periodo di tempo presso i server del *provider*. Tale sistema ha lo scopo di migliorare l'efficienza del servizio, consentendo, ad esempio, di fornire i risultati di ricerca in tempi più rapidi, quantomeno per le *keyword* più frequenti. Grazie alla funzione "copia *cache*" i motori di ricerca svolgono, di fatto, una vera e propria attività di memorizzazione di gran parte dei contenuti della rete dagli stessi indicizzati. La cancellazione dalla memoria del *provider* della copia *cache* degli URL a determinate pagine web ha l'effetto di precludere la possibilità di rinvenire tali contenuti all'esito di una interrogazione del motore di ricerca effettuata con qualsivoglia parola chiave. Laddove, per contro, la mera deindicizzazione sortisce il più limitato effetto di escludere che un contenuto compaia tra i risultati di un motore di ricerca in esito a una interrogazione basata sul mero nome di una persona, eliminando, così, una particolare modalità di ricerca del dato, il quale resta comunque raggiungibile attraverso il *search engine* mediante ricerche più articolate e diverse rispetto alla mera *query* "nominale".

→ Come chiarito dalla Cassazione, non è automatico che alla deindicizzazione di un URL debba sempre corrispondere anche la cancellazione della relativa **copia *cache***, ma occorre valutare caso per caso le singole situazioni ed effettuare un bilanciamento degli interessi in gioco, ossia, da un lato, dell'interesse del pubblico a reperire una determinata informazione e, dall'altro, del diritto del soggetto interessato alla protezione della propria riservatezza ma, ancor più, la propria reputazione.

Sempre in materia di motori di ricerca, è altresì noto il caso del *tool* fornito da uno dei principali *search engine* che contempla l'automatico accostamento alle prime parole della *query* di altri termini ritenuti pertinenti sulla base delle più diffuse ricerche effettuate sul web anche da altri utenti. Al riguardo, è stato in più occasioni sollevato il tema della lesività di taluni degli accostamenti effettuati dal motore di ricerca, con riferimento in particolare all'affiancamento di taluni vocaboli più o meno "denigratori" a nomi di personaggi noti (ad esempio, a fronte dell'inserimento nella barra di ricerca del nome

“Mario Rossi”, il motore di ricerca suggerisce la ricerca “Mario Rossi truffatore”). In termini generali, la giurisprudenza ha qualificato tale funzionalità come ulteriore e accessoria rispetto al semplice servizio di *search engine*, ritenendo, quindi, che, limitatamente a tale funzione, il *provider* non operi come mero intermediario, bensì come produttore diretto dell’informazione, e dunque possa essere responsabile per danni creati da quell’informazione se lesiva dell’onore e della reputazione.