Stefania Calosso
Avvocato, Cultrice della materia Data Protection Law presso l'Università di Bologna, componente della Rete Giuridica AIAS

Quali sono i principi da applicare al trattamento dei dati personali?

L'art. 5 GDPR elenca i principi generali applicabili al trattamento dei dati personali. Questa norma è considerata la spina dorsale della disciplina della protezione dei dati personali poiché ne riassume in sé tutti i criteri ispiratori, fungendo altresì da strumento interpretativo di tutte le altre norme contenute nel GDPR. Tali principi necessitano di un'interpretazione organica e sistematica e non frammentaria, in quanto ciascuno di essi dà contenuto e dettaglio agli altri.

Detti principi sono i seguenti:

- liceità, correttezza e trasparenza;
- limitazione delle finalità;
- minimizzazione dei dati;
- esattezza;
- limitazione della conservazione;
- integrità e riservatezza (*confidentiality*);
- responsabilizzazione (*accountability*).

Di seguito verranno singolarmente esaminati, ma occorre far presente sin da ora che essi sono tutti intrinsecamente connessi: si vedrà infatti che il principio di limitazione delle finalità è di ispirazione tanto al principio di minimizzazione quanto a quello di limitazione della conservazione, permeando al contempo il principio di trasparenza. A sua volta, quest'ultimo trova riscontro nel principio di correttezza e in quello dell'*accountability* e, infine, il principio di limitazione della conservazione è connesso al principio della integrità del trattamento che a sua volta è legato a quello di esattezza.

IL PRINCIPIO DI LICEITÀ, CORRETTEZZA E TRASPARENZA

Il primo principio stabilisce che i dati devono essere trattati

> «*in modo lecito, corretto e trasparente nei confronti dell'interessato*».

Si tratta quindi di un principio che contiene tre sotto-principi enunciati congiuntamente perché tutti rispondono alla esigenza di evitare trattamenti abusivi, opachi, sleali o, in una sola parola, illeciti, e anche poiché il principio di correttezza può essere veramente compreso solo congiuntamente agli altri due.

Ciò detto, vediamoli singolarmente:

- Il primo, molto generale, è **il principio della liceità** e ha lo scopo di assicurare che il trattamento dei dati personali non sia solo rispettoso delle norme del GDPR, ma di tutte le disposizio-

ni di legge, nell'ambito del corretto bilanciamento tra gli interessi del titolare del trattamento e quelli dei soggetti interessati. Questo principio è stato definito la vera e propria ragion d'essere del diritto sulla protezione dei dati personali: il trattamento di questi ultimi, infatti, non è un'attività che rientra nella libera iniziativa del titolare, ma è un'attività che è resa possibile o per la volontà del soggetto (attraverso il suo consenso), o per una specifica fonte normativa, circostanza che, nel bilanciamento tra i diversi interessi in gioco, la rende giustificata.

- Il secondo, ovvero **il principio di correttezza**, richiama la nozione civilistica di correttezza e buona fede tipica del diritto delle obbligazioni e dei contratti che, in ambito di protezione dei dati personali, si traduce nel divieto per il titolare di trattare i dati personali in un modo che, sebbene non direttamente in violazione di norme di legge, abusi di una posizione di squilibrio a danno degli interessi sostanziali del soggetto interessato; in altre parole, il titolare deve far sì che il trattamento non risulti sleale, cioè non costituisca, di fatto, un abuso della sua posizione dominante rispetto a quella dell'interessato. Per meglio comprenderlo, si suole declinare il principio di correttezza in tre variabili:
  a. considerazione degli effetti sugli individui;
  b. considerazioni sulle aspettative dei soggetti interessati;
  c. trasparenza del trattamento dei dati.
  Infine, il principio di correttezza viene altresì associato al concetto di non discriminazione, nel senso che un trattamento è corretto se, tra le altre cose, non produce effetti discriminatori nei confronti delle persone fisiche sulla base di speciali categorie di dati.

- Il terzo, ossia **il principio di trasparenza**, impone che le informazioni e le comunicazioni relative al trattamento dei dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio chiaro e semplice. In particolare, esso riguarda l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento, nonché tutte le ulteriori informazioni per assicurare loro un trattamento corretto e trasparente anche con riguardo al diritto di ottenere conferma e comunicazione di un trattamento di dati personali che li riguarda.

Si suole dire che il principio di trasparenza è un principio *user-centric*, ovvero che si basa sulle reali esigenze conoscitive e capacità di comprensione dell'interessato, onde assicurare una concreta consapevolezza in ordine alle caratteristiche del trattamento.

Infine, occorre tenere presente che il principio di trasparenza si esplica in diverse fasi del ciclo di trattamento dei dati:
a. prima o all'inizio del trattamento dei dati, al momento cioè in cui il titolare ottiene i dati personali;
b. durante l'intero periodo di trattamento;
c. in momenti specifici del ciclo di trattamento (ad esempio quando sopravviene una violazione di dati personali).

IL PRINCIPIO DI LIMITAZIONE DELLE FINALITÀ

Il principio di limitazione delle finalità prevede che i dati siano

> «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*».

Si tratta di uno dei principi più importanti dell'intero Regolamento a sua volta a fondamento di altri principi, come quello di minimizzazione, di esattezza o di limitazione della conservazione, ed espressivo a sua volta del principio di trasparenza nonché dei criteri di prevedibilità e certezza giuridica.

La *ratio* di tale principio è quella di prevenire usi di dati personali che possano apparire inaspettati, inappropriati o altrimenti discutibili; esso è profondamente radicato nella teoria della privacy come "controllo informativo", nel senso di porre limiti all'utilizzo dei dati personali da parte del titolare, così che un soggetto possa prevedere e valutare il pericolo di fornire una determinata informazione afferente la propria vita privata, personale e familiare.

Il principio di limitazione delle finalità interessa due diversi momenti del trattamento dei dati: la loro raccolta e il loro successivo trattamento.
Con riguardo alla raccolta, essa deve essere effettuata per finalità:
a. determinate al momento stesso della raccolta e dunque previste a priori;
b. esplicite, dunque rese note sin da subito all'interessato;
c. legittime, perciò tutelate o comunque permesse dal nostro ordinamento.
Per quanto concerne il successivo trattamento, esso deve essere rispettoso delle finalità inizialmente determinate ed esplicitate al momento della raccolta.

Ma vediamo nello specifico le suddette condizioni che, si badi, sono cumulative:

- *Determinatezza*: tale requisito impone al titolare di compiere una valutazione interna che sia documentata e antecedente l'inizio del trattamento (esso inizia con la raccolta dei dati personali). Il grado di dettaglio richiesto nella determinazione delle finalità è molto elevato: esse devono essere individuate con precisione e dettaglio così che l'interessato sia sempre in grado di capire che tipo di trattamento è incluso nello scopo determinato; pertanto la finalità non deve essere ampia o generica.

- *Esplicitezza*: tale concetto è strettamente connesso al principio di trasparenza e si esplica nell'obbligo di informare l'interessato in merito alle finalità del trattamento e avvisarlo in caso di nuove finalità, intendendo per tali quelle incompatibili con le finalità iniziali. Non è quindi sufficiente che il titolare determini in anticipo e con elevato grado di dettaglio le finalità, ma occorre anche che le comunichi in modo chiaro e comprensibile al soggetto interessato.

- *Legittimità*: tale requisito va interpretato in senso ampio; la finalità non deve soltanto rispettare la legge in materia di protezione di dati personali, bensì la normativa di qualsiasi altro settore normativo.

IL PRINCIPIO DI MINIMIZZAZIONE DEI DATI

Tale principio, in passato denominato anche "principio di necessità", è un corollario del principio di limitazione delle finalità sopra esaminato, in quanto prevede che i dati raccolti debbano essere

> «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*».

In altre parole, una volta determinate le finalità, i dati personali in concreto raccolti non devono essere superflui, inutili o sovrabbondanti rispetto alle finalità medesime.
Esso vincola quindi il titolare a due tipi di valutazioni: una in merito all'assenza di altri ragionevoli mezzi per raggiungere le finalità del trattamento e una sul mantenimento del rispetto di tale principio con riguardo al mutamento della realtà fattuale connaturata al trascorrere del tempo.

IL PRINCIPIO DI ESATTEZZA

Il principio di esattezza prevede che i dati trattati debbano essere «*esatti e, se necessario, aggiornati*».
Tale principio richiede, tanto nell'interesse del titolare quanto in quello dell'interessato, che i dati raccolti siano accurati e quindi corretti, e non rappresentino falsamente la realtà, in ossequio al diritto alla identità personale da intendersi quale diritto della persona a non essere falsamente rappresentata.
Conseguentemente,

> «*devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*».

Da ciò si evince che la rettifica e/o l'eventuale cancellazione dei dati inesatti da un lato costituiscono diritti dei soggetti interessati e, dall'altro, obblighi generali per i titolari.

IL PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE

Il principio della limitazione della conservazione, detta anche "*data retention*", impone la conservazione dei dati

> «*in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*».

Il che equivale a dire che, una volta perseguite le finalità, i dati devono essere eliminati o anonimizzati.
È evidente che anche tale principio costituisce diretta emanazione del principio di limitazione della finalità.
Le ragioni poste alla base di tale principio possono essere molteplici: limitare la durata del trattamento consente di prevenire usi secondari illegittimi dei dati personali; ridurre i rischi di cybersecurity (quali la perdita e/o il furto dei dati, la loro alterazione) intrinseca al protrarsi della conservazione; mitigare la limitazione di autonomia dell'interessato correlata al turbamento morale per trattamento dei dati prolungato.

IL PRINCIPIO DI INTEGRITÀ E RISERVATEZZA

Il principio di integrità e riservatezza, che costituisce una novità introdotta con il GDPR, prevede che i dati siano

> «*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*».

Questo principio, denominato altresì *confidentiality,* stabilisce la necessità di assumere, in relazione a ciascun trattamento, adeguate misture tecnico-organizzative a garanzia della sicurezza e della protezione

dei dati, facendo della cybersecurity uno dei pilastri fondamentali della tutela dei dati personali. Esso si concentra infatti sui mezzi idonei a scongiurare alterazioni dolose e/o colpose che ledano l'accuratezza di un trattamento.

Costituiscono diretta emanazione di tale principio:

— L'art. 32 "Sicurezza del trattamento", che obbliga il titolare ad adottare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto di una serie di fattori quali lo stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, fornendo alcuni esempi: pseudonimizzazione, cifratura, back-up di sistema, audit interni.

— Gli artt. 33 e 34, che individuano le azioni da intraprendere in seguito a una violazione dei dati personali c.d. *data breach*, azioni tutte strettamente connesse con tale principio.

— L'art. 35, ossia la valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali, in cui il concetto di "rischio" che il titolare deve valutare e mitigare riguarda anche e specialmente l'integrità e la riservatezza dei dati.

IL PRINCIPIO DI RESPONSABILIZZAZIONE

Il principio di *accountability* (responsabilizzazione) è il corollario di tutti i principi sin qui esaminati. Esso sancisce che il titolare del trattamento è competente per il rispetto di tutti i principi esposti all'art. 5 medesimo e che deve essere «*in grado di comprovarlo*».
Il concetto di *accountability* contiene quindi in sé la prescrizione di un duplice obbligo in capo al titolare: quello di garantire il rispetto del Regolamento e quello di essere in grado di dimostrarlo.

La *ratio* di tale principio è quella di rendere efficacemente applicabili i principi sopra esaminati mediante la responsabilizzazione del titolare del trattamento a cui l'autorità di controllo si possa direttamente rivolgere al fine di richiedere la prova del rispetto dei principi del trattamento di cui all'art. 5.
Il principio in esame si sostanzia quindi in un duplice obbligo: l'adozione di misure per implementare i principi sul trattamento dei dati e la capacità di dimostrare il rispetto di tali principi.