La disciplina dell'attività di trattamento

Chiara Angiolini, Antonello Iuliani[1]

Abstract: The first section of the chapter illustrates the legal bases for processing personal data and exceptions to the prohibition of processing special categories of personal data. In the second section, the principles governing data processing are analyzed through a systematic and structured legal framework. In the last section, rules on data breach are analysed showing the relevance of EDPB guidelines on this subject.

Keywords: Principles relating to processing of personal data, rules on data breach

Sez. I. Le basi giuridiche del trattamento

1. Le basi giuridiche del trattamento dei dati personali

Il trattamento dei dati personali può essere svolto lecitamente se si fonda su una base giuridica del trattamento. Tali basi giuridiche sono previste dal Reg. UE 2016/679 (d'ora in avanti: GDPR) all'art. 6 che, nell'interpretazione della Corte di Giustizia dell'UE "prevede un elenco esaustivo e tassativo dei casi nei quali un trattamento di dati personali può essere considerato lecito" (CGUE, 9 gennaio 2025, C-394/23, § 25; così anche CGUE, 4 ottobre 2024, C-621/22, § 29, CGUE, 4 luglio 2023, C-252/21 § 90, CGUE, 22 giugno 2021, C-439/19, § 99). In particolare, l'art. 6 GDPR prevede le seguenti basi giuridiche:

[1] Chiara Angiolini ha scritto la prima sezione del presente capitolo, Antonello Iuliani la seconda e la terza.

Chiara Angiolini, University of Siena, Italy, chiara.angiolini@unisi.it
Antonello Iuliani, Università digitale Pegaso, Italy, antonello.iuliani@unipegaso.it, 0000-0001-9931-6934

Referee List (DOI 10.36253/fup_referee_list)
FUP Best Practice in Scholarly Publishing (DOI 10.36253/fup_best_practice)

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;

b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;

e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Con riguardo all'interpretazione dell'art. 6, par. 1, GDPR è di particolare interesse l'orientamento della Corte di Giustizia dell'UE secondo cui le basi giuridiche previste dalla lett. b) alla lett. f) sono da interpretare restrittivamente "nella misura in cui consentono di rendere lecito un trattamento di dati personali effettuato in assenza del consenso dell'interessato" (CGUE, 9 gennaio 2025, C-394/23, § 27; così anche CGUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21, § 93)

Inoltre, la CGUE ha affermato che il requisito della necessità previsto nelle basi giuridiche da b) ad f) dell'art. 6, par. 1, GDPR

> non è soddisfatto quando l'obiettivo perseguito da tale trattamento di dati potrebbe ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti agli articoli 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di tali dati devono avere luogo nei limiti dello stretto necessario.

2. *Segue*. Il consenso dell'interessato

La disciplina della base giuridica del consenso al trattamento è frutto della lettura sistematica di varie norme, e *in primis* dell'art. 6, par. 1, lett. a), dell'art. 4 e dell'art. 7 GDPR.

L'art. 6, par. 1, lett. a) GDPR prevede che il consenso al trattamento dei dati personali per una o più specifiche finalità sia una base giuridica del trattamento. L'art. 7 GDPR chiarisce che se il trattamento è fondato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato l'ha validamente prestato.

Il consenso al trattamento è strumento che attribuisce all'interessato un ruolo nella determinazione della possibilità e delle finalità del trattamento, e può essere letto come esercizio del diritto alla riservatezza e tecnica di tutela e partecipazione dell'interessato rispetto alla costruzione del regime dei dati personali, e dunque espressione dell'art. 8 CDFUE che sancisce il diritto alla protezione dei dati personali, e che infatti ne fa menzione (sull'art. 8 CDFUE, v. cap. *Le fonti della disciplina in materia di dati personali*).

La riflessione sul ruolo e sulla qualificazione del consenso al trattamento è stata per lungo tempo la chiave di volta del sistema della disciplina dei dati personali (Caggia 2019). È qui sufficiente dire che il consenso è un atto di autonomia privata, attraverso cui l'interessato esercita il diritto alla vita privata e alla protezione dei dati personali (Resta 2000, 307).

Una definizione generale di consenso al trattamento è data dall'art. 4, par. 1, n. 11 GDPR, ed è la seguente:

> «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

Dunque, il consenso al trattamento per fondare validamente il trattamento deve essere: i) libero; ii) informato; iii) specifico, in particolare con riguardo alle finalità; iv) prestato attraverso una dichiarazione o un'azione positiva inequivocabile.

Con riguardo alle forme di prestazione del consenso, occorre aggiungere che l'art. 7 GDPR dispone che se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Inoltre, l'articolo appena richiamato prevede che nessuna parte di una tale dichiarazione che costituisce una violazione del GDPR può essere ritenuta vincolante.

Di sicura importanza sono poi le norme che attengono alla libertà del consenso, che conferiscono rilevanza alle circostanze in cui questo è prestato. In proposito, secondo l'art. 7 GDPR, nel valutare se il consenso sia stato liberamente prestato, si deve tenere nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Ancora, l'articolo appena richiamato disciplina la revoca del consenso, che può essere letta come lo specchio della sua libertà. Infatti, l'art. 7 GDPR sancisce il diritto dell'interessato a revocare il proprio consenso in qualsiasi momento, con la stessa facilità con cui l'ha prestato. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca e prima di esprimere il proprio consenso, e l'interessato deve essere informato di tale aspetto.

Ancora in tema di libertà del consenso, i considerando 42 e 43 GDPR recitano:

> (42) [...] Il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio.
> (43) Per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte

> le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

Anche alla luce di quanto si legge nel considerando 43 GDPR, si può affermare l'esistenza di una presunzione di non libera espressione del consenso quando non sia possibile prestarlo separatamente per distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o qualora l'esecuzione di un contratto, compresa la prestazione di un servizio, sia subordinata al consenso sebbene esso non sia necessario per tale esecuzione. L'onere della prova è in capo al titolare del trattamento, come confermato dalla Corte di Giustizia (CGUE, 11 novembre 2020, C-61/19) e ritenuto dal Comitato Europeo per la Protezione dei Dati (d'ora in avanti: EDPB) nelle linee guida in materia di consenso (EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, 4 maggio 2020, p. 11).

L'interpretazione del requisito della libertà del consenso è dibattuta in dottrina e in giurisprudenza, in particolare con riguardo alle ipotesi in cui il consenso e l'ottenimento di una prestazione da parte dell'interessato sono correlate.

In proposito, il Comitato Europeo per la Protezione dei Dati ritiene eccezionali i casi in cui il consenso è da considerare libero anche se l'esecuzione del contratto è subordinata alla sua prestazione (EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679,* 4 maggio 2020). Inoltre, secondo tali linee guida, la prova della libertà del consenso potrà essere data dimostrando che il titolare del trattamento offre, oltre a un servizio subordinato alla prestazione del consenso, anche un altro servizio effettivamente equivalente e non «condizionato».

In questo senso si è espressa anche la Corte di Giustizia (CGUE, 4 luglio 2023, C-252/21), secondo cui gli interessati devono disporre della libertà di rifiutare di prestare il loro consenso a operazioni particolari di trattamento di dati non necessarie all'esecuzione del contratto d'uso del social network (com'è la profilazione per finalità di personalizzazione dei contenuti, anche pubblicitari), senza essere per questo tenuti a rinunciare integralmente alla fruizione del servizio offerto dal social network online, il che implica che a detti utenti venga proposta, se del caso a fronte di un adeguato corrispettivo, un'*alternativa equivalente* non accompagnata da simili operazioni di trattamento di dati (dunque, un'alternativa che non comporti la profilazione per finalità di personalizzazione dei contenuti).

Con riguardo alla nozione di «alternativa equivalente» è di interesse anche il *Parere dell'EDPB 8/2024 sul consenso valido nel contesto dei modelli «consenso o pagamento» attuati dalle piattaforme online di grandi dimensioni*. Per comprendere la portata di tale documento occorre innanzi tutto chiarire la definizione di «piattaforma online di grandi dimensioni». È l'EDPB stesso a dare una definizione della nozione nell'ambito del parere, chiarendo che la nozione di «piattaforme online» comprende quella prevista dall'art. 3 del Regolamento 2022/2065 sui servizi digitali, ma non è a questa limitata e individuando i seguenti criteri, non cumulativi né esaustivi, utili per qualificare un soggetto come piattaforma online di grandi dimen-

sioni: i) il grande numero di interessati in qualità di utenti; ii) la posizione della società sul mercato; iii) l'esistenza di un trattamento su larga scala di dati personali; iv) la qualificazione del titolare del trattamento come «piattaforma online di dimensioni molto grandi» ai sensi del Regolamento 2022/2065 sui servizi digitali, o come *gatekeeper* ai sensi del Regolamento 2022/1925 sui mercati digitali. A tal riguardo l'EDPB afferma innanzi tutto che:

> se la versione alternativa si differenzia dalla versione con pubblicità comportamentale soltanto nella misura necessaria in considerazione dell'incapacità del titolare del trattamento di trattare dati personali per finalità di pubblicità comportamentale, tale versione alternativa può essere considerata equivalente.

Con riguardo agli altri possibili casi, l'EDPB ritiene che l'interessato debba poter comparare le due versioni e che tali versioni non debbano essere necessariamente identiche, ma che nel caso in cui la qualità sia inferiore e vi siano funzionalità soppresse, la versione non dovrebbe essere ritenuta equivalente. Un profilo di particolare rilevanza attiene al pagamento di un corrispettivo nella versione alternativa offerta dal titolare del trattamento. In proposito, nel parere appena citato l'EDPB, rispetto alla valutazione del requisito della libertà del consenso al trattamento per finalità di pubblicità comportamentale, ritiene che «quando sviluppano l'alternativa alla versione del servizio con pubblicità comportamentale, i titolari del trattamento dovrebbero prendere in considerazione la possibilità di fornire agli interessati una "alternativa equivalente" che non comporti il pagamento di un corrispettivo, come l'alternativa gratuita priva di pubblicità comportamentale». In proposito, l'EDPB afferma anche che, pur non essendoci alcun obbligo per le piattaforme online di grandi dimensioni di offrire sempre servizi gratuiti, la messa a disposizione degli interessati di tale ulteriore alternativa rafforza la loro libertà di scelta e questo rende più facile per i titolari del trattamento dimostrare che il consenso è liberamente prestato. Più in dettaglio, l'EPDB, con riguardo al possibile pregiudizio subito dagli interessati in assenza di un'alternativa gratuita in caso di mancato consenso al trattamento per pubblicità comportamentale, pregiudizio che può inficiare la libertà del consenso al trattamento ai sensi del GDPR, considera la possibile importanza del ruolo delle piattaforme nell'accesso alle informazioni e ai servizi, così come in ambito professionale e nella vita quotidiana e sociale e tiene conto della loro possibile difficile fungibilità che può derivare anche dai c.d. «effetti di rete» ed «effetti di dipendenza» (si pensi ad esempio alla fruizione di un noto social network su cui l'interessato ha un nutrito seguito di *followers*; cfr. le citate Linee guida, pp. 26 ss.).

Dunque, secondo l'EDPB la fornitura di un'alternativa gratuita priva di pubblicità comportamentale costituisce un fattore particolarmente importante da considerare nel valutare se gli interessati possano esercitare una scelta effettiva e quindi se il consenso sia valido. Rispetto alla previsione di un corrispettivo, l'EDPB nel *Parere 8/2024* già citato ritiene che:

> i titolari del trattamento dovrebbero valutare, caso per caso, tanto se un corrispettivo sia in effetti adeguato e quale sia l'importo adeguato in determinate circostanze, tenendo presenti i requisiti per un consenso valido ai sensi del GDPR, nonché la

> necessità di evitare che il diritto fondamentale alla protezione dei dati sia trasformato in una caratteristica il cui godimento è soggetto a pagamento da parte degli interessati oppure in una caratteristica premium riservata ai benestanti o agli abbienti.

Il Comitato prende in esame anche il profilo dello squilibrio di potere fra interessato e titolare del trattamento in relazione alla valutazione della libertà del consenso. In particolare, l'EDPB individua, nel caso in cui il titolare del trattamento sia una «piattaforma online di grandi dimensioni», alcuni elementi non esaustivi e non cumulativi, che possono essere tenuti in conto per valutare la sussistenza di una situazione di evidente squilibrio di potere capace di minare la libertà del consenso. Tali fattori sono: i) la posizione della società sul mercato, anche rispetto all'esistenza di una eventuale sua posizione dominante nel mercato o di un suo rilevante potere di mercato, e della presenza di effetti di rete o di dipendenza; ii) la misura in cui l'interessato fa affidamento sul servizio fornito, in relazione ad esempio alla ricerca di lavoro, all'accesso a informazioni essenziali per la vita quotidiana degli interessati o alla partecipazione al dibattito pubblico; iii) il pubblico destinatario o predominante della piattaforma, ad esempio in relazione alla presenza di minori. L'EDPB ritiene anche che una valutazione caso per caso di tali fattori dovrebbe essere sempre necessaria.

Guardando all'ambito nazionale, il Garante per la Protezione dei Dati Personali (GPDP) da tempo afferma che il consenso non può essere qualificato come libero quando la fornitura di un servizio sia a esso subordinato (ad esempio: GPDP, 10 gennaio 2019, n. 9080914; GPDP, 20 giugno 2019, n. 9124420).

Vi è poi una parte della dottrina e della giurisprudenza secondo cui il consenso può talvolta essere ritenuto libero pur se a questo è subordinata la fornitura di un servizio, e che quanto più il servizio è infungibile e irrinunciabile, quanto più il condizionamento che incide sulla libertà del consenso deve ritenersi sussistente (Cass., 2 luglio 2018, n. 17278).

Infine, la valutazione della libertà del consenso al trattamento può anche essere letta adottando una prospettiva che consideri il carattere massivo dei trattamenti, e che sia volta a garantire, in ossequio anche al principio di uguaglianza sostanziale sancito dall'art. 3 Cost., la necessità di una pari opportunità di soddisfacimento e di esercizio, in concreto, dei diritti fondamentali, e in particolare del diritto alla protezione dei dati personali e alla riservatezza, rispetto ai quali il consenso al trattamento costituisce una modalità di esercizio. Secondo tale punto di vista, la presunzione di cui al considerando 43 GDPR può essere vinta quando il titolare del trattamento dimostri di offrire un servizio non subordinato al consenso al trattamento, alle stesse condizioni economiche di quello condizionato al consenso (Angiolini 2020).

3. *Segue*. L'esecuzione di un contratto di cui l'interessato è parte

L'art. 6, par. 1, lett. b) GDPR prevede la base giuridica della necessità del trattamento per l'esecuzione di un contratto di cui l'interessato è parte o di misure precontrattuali adottate su richiesta dello stesso.

Il contratto diventa qui un elemento da valutare ai fini dell'operatività della base giuridica del trattamento. Il trattamento dei dati è in quest'ipotesi strumentale alla

messa in opera fisiologica del contratto: i dati possono essere trattati solo in virtù della necessità del loro trattamento rispetto a quanto previsto nel regolamento negoziale.

La definizione dei trattamenti necessari all'esecuzione del contratto non sempre è agevole. In alcuni casi il criterio della necessità risulta chiaro; si immagini il caso del trattamento dei dati consistenti nell'indirizzo del cliente-interessato volti all'adempimento dell'obbligazione di consegna di una merce in capo all'altra parte contrattuale. Più complesse sono le ipotesi in cui il trattamento è menzionato nel contratto, e in cui quindi sono le parti a includere il trattamento dei dati all'interno del testo contrattuale. Qui emerge il rischio, sottolineato anche dal EDPB, di aggirare le regole relative alla base giuridica del consenso al trattamento, includendo il trattamento nell'oggetto del contratto. A tal proposito, è utile richiamare l'indirizzo dell'EDPB, che ha escluso che tramite il contratto si possa espandere «artificiosamente» il novero dei trattamenti resi leciti dall'art. 6, par. 1, lett. b) GDPR, e ha elaborato delle linee guida in materia (EDPB, *Linee guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6*, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati, versione 2.0, 8 ottobre 2019, p. 6). L'EDPB interpreta il requisito della necessità come oggettivo, e afferma che per utilizzare la base giuridica di cui all'art. 6, par. 1, lett b) GDPR, il titolare del trattamento deve dimostrare che il contratto non può essere eseguito, con riguardo al suo oggetto principale, senza che i dati personali siano trattati. Inoltre, se vi sono alternative meno intrusive, il trattamento non può avere come base giuridica quella dell'esecuzione del contratto. Poi, quando il contratto termina la liceità del trattamento viene meno e il titolare del trattamento non potrà trattare i dati facendo riferimento a una diversa base giuridica per il trattamento, a meno che non vi fossero distinte basi giuridiche comunicate ab initio all'interessato.

La Corte di Giustizia dell'UE è intervenuta sul tema, statuendo che

> affinché un trattamento di dati personali sia considerato necessario all'esecuzione di un contratto […] esso deve essere oggettivamente indispensabile per realizzare una finalità che è parte integrante della prestazione contrattuale destinata all'interessato. Il [titolare] del trattamento deve, quindi, essere in grado di dimostrare in che modo l'oggetto principale del contratto non potrebbe essere conseguito in assenza del trattamento di cui è causa. (CGUE, 4 luglio 2023, C- 252/21; così anche CGUE, 9 gennaio 2025, C-394/23, § 33)

Inoltre, la Corte di Giustizia dell'UE ha affermato che l'elemento determinante ai fini dell'applicazione dell'art. 6, paragrafo 1, lettera b), del RGPD è che il trattamento sia essenziale per consentire la corretta esecuzione del contratto stipulato tra il titolare e l'interessato e, pertanto, che non esistano altre soluzioni percorribili e meno invasive (CGUE, 9 gennaio 2025, C-394/23, § 34; v. anche: CGUE, 12 settembre 2024, C-17/22 e C-18/22; CGUE, 4 luglio 2023, C-252/21, § 99) e che se il contratto consiste in più servizi o in più elementi distinti di uno stesso servizio che possono essere prestati indipendentemente gli uni dagli altri, l'applicabilità dell'articolo 6, par. 1, lett. b), GDPR deve essere valutata separatamente nel contesto di ciascuno di tali servizi (CGUE, 9 gennaio 2025, C-394/23, § 35 e CGUE, 4 luglio 2023, C-252/21, § 100).

Rispetto all'applicazione di tali principi in un caso concreto, si può citare l'indirizzo della CGUE secondo cui

> il trattamento di dati personali relativi all'appellativo dei clienti di un'impresa di trasporto, avente la finalità di personalizzare la comunicazione commerciale fondata sulla loro identità di genere, non sembra essere né oggettivamente indispensabile né essenziale al fine di consentire la corretta esecuzione di un contratto e, pertanto, non può essere considerato necessario all'esecuzione di tale contratto. (CGUE, 9 gennaio 2025, C-394/23, § 43).

4. L'adempimento di un obbligo legale al quale è soggetto il titolare del trattamento

L'art. 6, par. 1, lett. c) GDPR prevede che il trattamento possa avvenire quando è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.

Rispetto al requisito della necessità, la Corte di Giustizia dell'UE ha affermato che questo non è soddisfatto quando l'obiettivo di interesse generale sotteso all'obbligo di legge

> può ragionevolmente essere raggiunto in modo altrettanto efficace mediante altri mezzi meno pregiudizievoli per i diritti fondamentali degli interessati, in particolare per i diritti al rispetto della vita privata e alla protezione dei diritti personali garantiti agli articoli 7 e 8 della Carta, atteso che le deroghe e le restrizioni al principio della protezione di simili dati devono avere luogo nei limiti dello stretto necessario. (CGUE, 22 giugno 2021, *B*, C-439/19, § 110)

In virtù dell'art. 6, par. 3, GDPR, perché tale base giuridica possa fondare il trattamento, ci deve essere una norma di diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento che determini tale base giuridica.

Inoltre, in ogni caso, la norma che stabilisce tale base giuridica deve perseguire un obiettivo di interesse pubblico e il trattamento deve essere proporzionato a tale obiettivo. Con riguardo alla proporzionalità, la Corte di Giustizia ha affermato che:

> al fine di valutare la proporzionalità del trattamento […] occorre misurare la gravità dell'ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali che tale trattamento comporta e verificare se l'importanza dell'obiettivo di interesse generale da quest'ultimo perseguito sia in relazione con tale gravità. Al fine di valutare la gravità di tale ingerenza, si deve segnatamente tener conto della natura dei dati personali in questione, e in particolare della loro natura eventualmente sensibile, nonché della natura e delle modalità concrete del trattamento dei dati di cui trattasi, in particolare del numero di persone che hanno accesso a tali dati e delle modalità di accesso a questi ultimi. (CGUE, 1° agosto 2022, C-184/20).

Poi, l'art. 6, GDPR prevede che gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione del GDPR con riguardo al trattamento, determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto fra cui: i) le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; ii)

le tipologie di dati oggetto del trattamento; iii) gli interessati; iv) i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; v) le limitazioni della finalità, vi) i periodi di conservazione; vii) le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto.

Sul piano nazionale, l'art. 2 *ter* d.lgs. 196/2003 (d'ora in avanti: cod. privacy) prevede che il trattamento, quando si applicano le basi giuridiche dell'art. 6, comma 1, lett. c) ed e) GDPR deve essere previsto da una norma di legge, di regolamento, o da atti amministrativi generali (sulla base giuridica di cui alla lett. e) dell'art. 6 GDPR si veda, in questo capitolo, il § 6.).

Inoltre, secondo quanto dispone l'art. 2 *quater* cod. privacy il Garante per la Protezione dei Dati personali può adottare delle regole deontologiche relative ai trattamenti fondati sulla base giuridica qui oggetto di commento.

5. La salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica

L'art. 6, comma 1, lett. d) GDPR prevede come base giuridica quella del trattamento necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica. Tale ipotesi è senz'altro residuale e potrà essere applicata in ipotesi residuali, come conferma anche la lettura del 46 GDPR, secondo cui:

> Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Alcuni tipi di trattamento dei dati personali possono rispondere sia a rilevanti motivi di interesse pubblico sia agli interessi vitali dell'interessato, per esempio se il trattamento è necessario a fini umanitari, tra l'altro per tenere sotto controllo l'evoluzione di epidemie e la loro diffusione o in casi di emergenze umanitarie, in particolare in casi di catastrofi di origine naturale e umana.

6. L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento

L'art. 6, par. 1, lett. e) GDPR prevede come base giuridica del trattamento quella della sua necessità per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Rispetto alla definizione delle specifiche ipotesi da parte del diritto dell'UE o nazionale, si applica quanto illustrato in relazione all'art. 6, par. 3 GDPR e all'art. 2 *ter* cod. privacy in relazione alla base giuridica relativa all'esistenza di un obbligo legale (v. *supra*, § 4).

Inoltre, l'art. 2 *ter* cod. privacy, prevede alcune regole specifiche. In particolare:

a) Secondo quanto dispone il comma 1 *bis* di tale norma il trattamento dei dati personali è consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri attribuiti a una autorità pubblica che tratti tali dati e che sia: i) un'amministrazione pubblica di cui all'articolo 1, com-

ma 2, del d.lgs. 165/2001, ivi comprese le autorità indipendenti e le amministrazioni inserite nell'elenco di cui all'articolo 1, comma 3, della l. n. 196/2009; ii) una società a controllo pubblico statale; iii) limitatamente ai gestori di servizi pubblici, locale, di cui all'articolo 16 del testo unico in materia di società a partecipazione pubblica (d.lgs. n. 175/2016), con esclusione, per le società a controllo pubblico, dei trattamenti correlati ad attività svolte in regime di libero mercato;

b) la comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli che rientrano nelle categorie particolari di dati (v. cap. *Le definizioni fondamentali*) e da quelli relativi a condanne penali e reati di cui all'articolo 10 GDPR, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è ammessa se prevista da una norma di legge, di regolamento, o da atti amministrativi generali, o se necessaria ai sensi del comma 1-*bis* dell'art. 2 *ter* cod. privacy (su cui si veda la lettera precedente di questo elenco);

c) La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalità sono ammesse unicamente se previste ai sensi del comma 1 o se necessarie ai sensi del comma 1-*bis*. In tale ultimo caso, ne viene data notizia al Garante almeno dieci giorni prima dell'inizio della comunicazione o diffusione.

Inoltre, secondo quanto dispone l'art. 2 *quater* cod. privacy il Garante per la Protezione dei Dati personali può adottare delle regole deontologiche relative ai trattamenti fondati sulla base giuridica qui oggetto di commento.

7. Il perseguimento del legittimo interesse del titolare del trattamento o di terzi

L'art. 6, par. 1, lett. f) GDPR prevede che i dati possano essere trattati se sono necessari per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Un punto chiave nell'applicazione della norma è la valutazione sul giudizio di prevalenza degli interessi o dei diritti e delle libertà fondamentali dell'interessato.

Per quanto riguarda la base giuridica del legittimo interesse la CGUE (CGUE, 9 gennaio 2025, C-394/23; CGUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21, § 106; In precedenza, con riguardo all'art. 7, lett. f), della direttiva 95/46, si vedano: CGUE, 11 dicembre 2019, C-708/18; 4 maggio 2017, C-13/16, §28; 17 giugno 2021, C-597/19, § 106; CGUE, 29 luglio 2019, C-40/17) ha affermato che tale disposizione prevede tre condizioni cumulative affinché il trattamento dei dati personali sia legittimo:

1) il perseguimento di un legittimo interesse da parte del titolare del trattamento o del terzo o dei terzi ai quali i dati sono comunicati. In proposito, la CGUE ha affermato che l'interesse deve essere considerato attuale ed effettivo (CGUE, 11 dicembre 2019, C-708/18). A titolo di esempio, la Corte di Giustizia ha considerato un legittimo interesse quello del titolare del trattamento o di terzi a ottenere un dato personale di una persona che ha asseritamente danneggiato la sua proprietà, al fine

di agire nei confronti di quest'ultima per ottenere il risarcimento dei danni (CGUE, 17 giugno 2021, C-597/19);

2) la necessità di trattare i dati personali ai fini degli interessi legittimi perseguiti. A questo proposito, la CGUE (CGUE, 9 gennaio 2025, C-394/23, § 48; CGUE, 4 maggio 2017, C-13/16, §30; CGUE, 11 dicembre 2019, C-708/18) ha affermato che le deroghe e le limitazioni in materia di protezione dei dati personali devono essere applicate solo nella misura strettamente necessaria. In particolare, ai fini dell'applicazione della base giuridica del legittimo interesse, occorre valutare che tale interesse non possa ragionevolmente essere raggiunto in modo altrettanto efficace con altri mezzi meno restrittivi dei diritti e delle libertà fondamentali degli interessati, in particolare i diritti al rispetto della vita privata e alla protezione dei dati personali garantiti dagli articoli 7 e 8 della Carta (CGUE, 9 gennaio 2025, C-394/23; GUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21,). Inoltre, la CGUE ha interpretato il criterio della necessità alla luce del principio di minimizzazione (CGUE, 9 gennaio 2025, C-394/23, § 49; GUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21; sul principio di minimizzazione v. la sezione successiva di questo capitolo).

3) i diritti e le libertà fondamentali della persona interessata dalla protezione dei dati non prevalgono sull'interesse legittimo perseguito. Secondo l'indirizzo della CGUE (CGUE, 11 Dicembre 2019, C-708/18) la valutazione relativa all'esistenza di diritti e libertà fondamentali della persona interessata che prevalgono sugli interessi legittimi perseguiti dal responsabile del trattamento o dal terzo o dai terzi a cui vengono comunicati i dati, richiede un bilanciamento dei diritti e degli interessi contrapposti, che dipende dalle circostanze specifiche del caso concreto, in cui si deve tenere conto dell'importanza dei diritti dell'interessato derivanti dagli articoli 7 e 8 della Carta.

Inoltre, la CGUE ha affermato che il criterio della gravità della violazione dei diritti e delle libertà dell'interessato è una componente essenziale dell'esercizio di ponderazione o di bilanciamento caso per caso. A questo proposito, la Corte (CGUE, 11 dicembre 2019, C-708/18; CGUE, 24 novembre 2011, cause riunite C-468/10 e 469/10) ha affermato che nella valutazione della gravità della violazione dei diritti fondamentali dell'interessato derivante da tale trattamento devono essere considerati i seguenti elementi:

a) la disponibilità dei dati personali in questione in fonti pubbliche. A tal proposito, la Corte ha osservato che la violazione dei diritti dell'interessato sanciti dagli articoli 7 e 8 della Carta è più grave in caso di trattamento di dati provenienti da fonti non pubbliche, in quanto le informazioni relative alla vita privata dell'interessato saranno successivamente conosciute dal responsabile del trattamento e, a seconda dei casi, dal terzo o dai terzi a cui i dati sono comunicati;

b) la natura dei dati personali in questione, in particolare la loro natura potenzialmente sensibile;

c) la natura e le modalità specifiche del trattamento;

d) il numero di persone che hanno accesso ai dati e le modalità di accesso;

e) alla luce del considerando 47 del GDPR, la ragionevole aspettativa dell'interessato che i suoi dati personali non saranno trattati quando, nelle circostanze del

caso, non può ragionevolmente aspettarsi un ulteriore trattamento di tali dati (così anche: CGUE, 9 gennaio 2025, C-394/23; CGUE, 4 ottobre 2024, C-621/22; CGUE, 4 luglio 2023, C-252/21).

Inoltre, nella sentenza CGUE, 4 luglio 2023, C-252/21 la Corte ha rilevato che occorre considerare se l'interessato è un minore.

La CGUE ha ritenuto che tali fattori debbano essere bilanciati rispetto all'importanza degli interessi legittimi perseguiti nel caso di specie.

In tale valutazione, la specificità del contesto di raccolta potrebbe, almeno in alcune ipotesi, essere considerato rilevante nell'interpretazione delle basi giuridiche del trattamento. In particolare, l'ambiente entro cui i dati sono raccolti potrebbe influire sulla valutazione della posizione dell'interessato nel test comparativo che deve precedere l'uso di questa base giuridica. Ad esempio, rispetto alla raccolta dei dati presso l'abitazione dell'interessato, crescente in ragione dell'espansione del cosiddetto «Internet delle cose», può assumere importanza la tutela costituzionale del domicilio di cui all'art. 14 Cost., anche ai fini dell'esito della valutazione della prevalenza degli interessi, dei diritti e delle libertà dell'interessato.

8. Il trattamento delle categorie particolari di dati personali e le eccezioni di cui all'art. 9 GDPR

Nel capitolo 3 si è trattato della definizione di «categorie particolari di dati personali», che sono definiti dall'art. 9 GDPR come quei dati che rivelano «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» (v. cap. *Le definizioni fondamentali*).

L'art. 9 GDPR prevede anche alcune regole specifiche che si applicano a questa categoria di dati.

In primo luogo, il primo paragrafo dell'art. 9 GDPR prevede un divieto generale di trattamento di queste categorie di dati, mentre il secondo paragrafo della medesima norma sancisce alcune eccezioni a tale divieto. Da questa formulazione normativa si deduce *in primis* che le eccezioni ai divieti, in quanto tali, sono norme di stretta interpretazione (così CGUE, 4 luglio 2023, C-252/21, § 76; CGUE, 21 dicembre 2023, C-667/21, § 50).

Le eccezioni previste sono le seguenti:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di trattamento delle categorie particolari di dati personali previsto dall'art. 9, par. 1 GDPR.

b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

c) il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso.

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato.

e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato.

f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali.

g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3. In questa ipotesi i dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale.

l) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1 GDPR, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Inoltre, ai sensi dell'art. 9, comma 4, GDPR, a livello nazionale possono essere mantenute o introdotte ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute.

Come ben si evince dalla lettura della norma, il diritto dell'Unione e quello nazionale hanno un ruolo significativo nel definire, entro i limiti posti dall'art. 9 GDPR, i trattamenti possibili di categorie particolari di dati personali.

Sul piano nazionale, a titolo di esempio, l'art. 2 *sexies* cod. privacy prevede che i trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Da ultimo, occorre affrontare il tema del rapporto fra le basi giuridiche di cui all'art. 6 GDPR (su cui v. *supra*, §§ 1-7) e quanto disposto dall'art. 9 GDPR. Sul punto, è da ritenere che per trattare lecitamente categorie particolari di dati, è necessario che sia applicabile sia un'eccezione al divieto di cui all'art. 9 che una base giuridica per il trattamento, tra quelle previste dall'art. 6 del GDPR (così CGUE 21 dicembre 2023, C-667/21, §§ 71 ss.). In altre parole, il trattamento di categorie particolari di dati personali che rientrano nell'art. 9 GDPR può essere effettuato solo se i) è applicabile un'eccezione al divieto di trattamento previsto dall'Art. 9 GDPR e ii) si applica una base giuridica prevista dall'art. 6 GDPR.

9. La disciplina sui c.d. cookies

Una disciplina specifica è prevista in relazione ai c.d. *cookies* e più tecnicamente all'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente e all'accesso a informazioni già archiviate.

Per comprendere cosa siano i cookie si può far riferimento alle linee guida in proposito adottate dal Garante per la Protezione dei Dati personali del 10 giugno 2021; nella scheda di sintesi allegata a dette linee guida si legge che:

> I *cookie* sono di regola stringhe di testo che i siti web (cd. publisher o «prima parte») visitati dall'utente ovvero siti o web server diversi (cd. «terze parti») posizionano e archiviano all'interno di un dispositivo terminale nella disponibilità dell'utente (cd. identificatori «attivi»). Analoghe funzioni possono essere svolte da altri strumenti che, pur utilizzando una tecnologia diversa (c.d. identificatori «passivi»), consentono di effettuare trattamenti analoghi a quelli svolti per il tramite dei *cookie*.

La disciplina di tali strumenti è data *in primis* dalla dir. 2002/58 (d'ora in avanti: direttiva e-privacy), recepita nell'ordinamento italiano all'art. 122 cod. privacy.

Con riguardo ai rapporti fra il GDPR e la direttiva e-privacy – e la relativa disciplina di recepimento –, l'art. 1, par. 2, direttiva e-privacy prevede che le disposizioni della direttiva precisino e integrino quanto previsto dalla dir. 95/46/CE; l'art. 94 GDPR prevede l'abrogazione di tale direttiva, e che i riferimenti fatti alla direttiva si devono intendere come riferiti al regolamento stesso.

Guardando alla disciplina nazionale di recepimento, l'art. 122 cod. privacy:

a) ammette testualmente l'eventuale archiviazione tecnica o l'accesso alle informazioni già archiviate se finalizzati unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell'informazione, esplicitamente richiesto dal contraente o dall'utente a erogare tale servizio;

b) salvo quanto detto nella lettera a), prevede che sia necessario il consenso del contraente o dell'utente, reso dopo che questi è stato informato con modalità semplificate, per l'archiviazione delle informazioni nell'apparecchio terminale di un contraente o di un utente o per l'accesso a informazioni già archiviate.

c) in tutti gli altri casi che non rientrano nelle ipotesi di cui alle lett. a) e b), è vietato l'uso di una rete di comunicazione elettronica per accedere a informazioni archiviate nell'apparecchio terminale di un contraente o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

Con riguardo ai caratteri del consenso da parte dell'interessato, è la stessa direttiva e-privacy a far riferimento alla disciplina generale in materia di dati personali dettata dal GDPR (v. *supra*, § 2). Infatti, l'art. 2 direttiva e-privacy dispone che il «"consenso" dell'utente o dell'abbonato corrisponde al consenso della persona interessata di cui alla direttiva 95/46/CE» e in virtù dell'art. 94 GDPR, il riferimento alla dir. 95/46 deve intendersi fatto al GDPR.

Con riguardo alla possibilità di adottare basi giuridiche diverse dal consenso nell'ipotesi *sub* b) il Garante per la Protezione dei Dati Personali, sulla base del principio di specialità, ha affermato che:

> la disciplina di carattere speciale applicabile [...] non contempla ulteriori basi giuridiche che rendano legittimo il trattamento se non in presenza del consenso dell'interessato ovvero al ricorrere di una delle ipotesi di deroga rispetto all'obbligo della sua raccolta previste proprio da tale disciplina speciale. (GPDP, *Linee guida* cookie *e altri strumenti di tracciamento,* 10 giugno 2021, punto 5)

Rispetto alle modalità di prestazione del consenso, il comma 2 dell'art. 122 prevede che possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente. In proposito, la Corte di Giustizia dell'Unione Europea ha affermato che il consenso

> non è validamente espresso quando l'archiviazione di informazioni o l'accesso a informazioni già archiviate nell'apparecchiatura terminale dell'utente di un sito Internet sono autorizzati mediante una casella preselezionata che l'utente deve deselezionare al fine di negare il proprio consenso (CGUE, 1° ottobre 2019, C-673/17).

La Corte di Giustizia arriva a tale soluzione anche richiamando il considerando 32 GDPR, secondo cui «non dovrebbe [...] configurare consenso il silenzio, l'inattività o la preselezione di caselle». Alcuni altri esempi e alcune considerazioni in proposito si trovano nelle *Linee guida* cookie *e altri strumenti di tracciamento,* del 10 giugno 2021 del Garante per la Protezione dei Dati Personali.

Con riguardo alle modalità semplificate dell'informazione, il Garante per la Protezione dei Dati personali nelle *Linee guida* cookie *e altri strumenti di tracciamento,* del 10 giugno 2021, ha dato alcune indicazioni, fra cui quella relativa alla necessità che questa sia fruibile, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari.

Sez. II. I principi del trattamento

10. I principi di liceità, correttezza e trasparenza

L'art. 5 GDPR, accedendo ad una prospettiva della disciplina dei dati personali di tipo relazionale e dinamico, che riflette la trasformazione dell'interferenza nell'altrui sfera informativa, da occasionale a fisiologica, fissa presupposti, criteri organizzativi e limiti dell'attività di trattamento, obblighi di condotta, per lo più aventi natura procedimentale, che attribuiscono all'interessato il *potere* di compartecipare nell'utilizzazione dei propri dati personali seguendo, controllando, rettificando il dato personale – così da plasmare la propria identità personale – fino all'estremo della riappropriazione (mediante la revoca del consenso o l'esercizio del diritto di opposizione) delle informazioni che lo riguardano.

Si può dire, in maniera sintetica, che i c.d. principi del trattamento – così designati per la loro indeterminatezza e il carattere di direttive fondamentali della disciplina – dettano le condizioni di liceità del trattamento: la liceità, infatti, cui fa menzione l'art. 5, co. 1, lett. a) GDPR, non si esaurisce nell'esistenza di una delle basi giuridiche previste dall'art. 6 (rubricato, per l'appunto, condizioni di liceità) che consentono, in conformità agli artt. 52 della Carta di Nizza e 8, par. 2 della Convenzione Edu, l'ingerenza nella sfera giuridica dell'interessato – *i.e.*: consenso dell'interessato/necessarietà del trattamento rispetto a determinate finalità – né nella non contrarietà della finalità del trattamento all'ordine pubblico, al buon costume o ad una norma imperativa (secondo un controllo che ricalca quello affidato alla causa del contratto; si pensi all'ipotesi in cui il titolare intenda trattare dati personali dei propri clienti per la gestione di una casa di prostituzione: la raccolta del consenso presso l'interessato e, dunque, la ricorrenza di una delle basi giuridiche previste all'art. 6 GDPR, non scolora la illiceità del trattamento).

La liceità, invero, esprime più in generale la conformità del trattamento a tutte le prescrizioni contenute nel regolamento, o, perlomeno, a quelle contenute negli artt. da 5 a 11 [così, infatti, CGUE, 4 maggio 2023, C-60/22, che ha escluso dal novero dei «trattamenti illeciti», capace di fondare la cancellazione o la limitazione dei dati, «la violazione, da parte del titolare del trattamento, degli obblighi previsti agli articoli 26 e 30 di tale regolamento, relativi, rispettivamente, alla conclusione di un accordo che determina la contitolarità del trattamento e alla tenuta del registro delle attività di trattamento»].

In posizione dialettica con la liceità si pone la clausola generale di correttezza – anch'essa richiamata dall'art. 5, co. 1, lett. a) – la quale si inserisce negli spazi non compiutamente definiti dal regolamento, sanzionando, *ex post*, le modalità concrete con le quali il trattamento è stato eseguito. Prendendo in prestito le parole delle *Linee guida EDPB 4/2019 sull'art. 25 Protezione dei dati fin dalla progettazione e per*

impostazione predefinita, «La correttezza è un principio di natura trasversale secondo cui i dati personali non devono essere trattati in modo ingiustificatamente dannoso, illegittimamente discriminatorio, imprevisto o fuorviante per l'interessato». E così, a esempio, è stato giudicato contrario al canone della correttezza lo svolgimento di un'attività di *marketing* diretto, attuata per il tramite di chiamate mute (cioè a dire senza che ad essa faccia seguito una risposta dall'operatore) tale da ribaltare sull'interessato l'inefficienza del *call center* (Cass. 04 febbraio 2016, n. 2196). E alla stessa stregua deve essere giudicato il comportamento del titolare, che, al momento della raccolta del consenso, presenti le diverse opzioni del trattamento in modo da indurre l'interessato a consentirgli di raccogliere più dati personali di quanto avverrebbe se le opzioni fossero presentate in modo corretto e neutrale (cfr., a riguardo, anche EDPB *Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them*), o che ometta di fornire all'interessato informazioni, ulteriori rispetto a quelle elencate agli artt. 13 e 14 GDPR, ma necessarie nel caso concreto (così il considerando 60 GDPR, a mente del quale «il titolare del trattamento dovrebbe fornire all'interessato eventuali ulteriori informazioni necessarie ad assicurare un trattamento corretto e trasparente, prendendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati»). La regola della correttezza svolge dunque le consuete funzioni, valutativa (che consiste nella paralisi, in quanto abusiva, della pretesa avanzata dall'interessato) e integrativa (che si risolve nel riconoscimento della sussistenza di un obbligo ulteriore in capo al titolare), senza però esaurirsi in una soltanto delle due.

La prima terna di principi è completata dal dovere di trasparenza, il quale riveste preminente importanza nel contesto del regolamento giacché innerva di contenuto quel diritto alla protezione dei dati personali che si manifesta anzitutto nel potere di controllo sulle proprie informazioni. Al dovere di trasparenza sono infatti primariamente riconducibili le norme che prescrivono il contenuto dell'obbligo informativo che grava sul titolare al più tardi al momento della raccolta presso l'interessato o un terzo (artt. 13 e 14 GDPR), le modalità di trasmissione delle informazioni (art. 12 GDPR), il diritto di accesso alle proprie informazioni e, quello conseguente, di ottenere una copia dei dati personali (art. 15 GDPR) nonché l'obbligo di comunicare all'interessato una violazione dei dati personali (art. 34 GDPR).

11. Il principio di finalità

La liceità del trattamento, nel senso minimale di ricorrenza di una base giuridica, non si apprezza isolatamente, ma rispetto alla finalità che il titolare intende perseguire: quest'ultima, infatti, costituisce una limitazione interna al trattamento che, una volta determinata, si impone allo stesso titolare per tutta la durata del trattamento. Per consentire all'interessato di controllare la permanenza del nesso di strumentalità si prevede che la finalità debba essere *determinata*, *esplicita* e *legittima*. La *legittimità* assume diverse coloriture: rispetto al trattamento basato sul consenso o sull'esecuzione di un contratto, essa si risolve nella liceità dell'interesse che il titolare intende perseguire riguardata alla luce dei consueti parametri offerti dalle norme imperative, dal buon costume e dall'ordine pubblico. Nel caso di trattamento necessario per l'e-

secuzione di un contratto, l'adempimento di un obbligo legale, la salvaguardia di un interesse vitale dell'interessato, l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare, la delimitazione dell'ambito degli interessi e, dunque, delle finalità legittimamente perseguibili dal titolare è sostanzialmente data dalla tipizzazione in chiave funzionale delle condizioni di liceità del trattamento. Nel caso, invece, di trattamento fondato sul legittimo interesse del titolare la legittimità della finalità si risolve nella meritevolezza comparativa tra l'interesse perseguito dal titolare e l'istanza protezionistica dell'interessato.

I requisiti della *determinatezza* – la finalità deve essere definita con sufficiente precisione, di talché «a purpose that is vague or general, such as for instance 'improving users' experience', 'marketing purposes', 'IT-security purposes' or 'future research' will – without more detail – usually not meet the criteria of being 'specific'» (così WP29 *Opinion 03/2013 on purpose limitation*) – e del *carattere esplicito* – la finalità non può essere affidata ad una ricostruzione ermeneutica implicita o a fatti concludenti – testimoniano lo stretto rapporto che corre tra il dovere di trasparenza e la liceità del trattamento: un trattamento che si dovesse, ad esempio, basare su un consenso raccolto per una finalità non esplicitata o non determinata sarebbe evidentemente un trattamento illecito.

L'art. 5, co. 1, lett. b) GDPR prosegue disponendo che i dati personali (originariamente raccolti per finalità determinate, esplicite e legittime) possono essere trattati ulteriormente – si intende, per un trattamento diverso da quello iniziale, sia esso successivo o contestuale ad esso – purché la diversa finalità (che sorregge l'ulteriore trattamento) sia compatibile con quella iniziale. La regola è ulteriormente specificata all'art. 6, par. 4 GDPR, là dove è stabilito che qualora il trattamento per una finalità diversa da quella per la quale i dati personali sono stati (inizialmente) raccolti non sia basato (*i*) sul consenso dell'interessato (naturalmente prestato in relazione alla nuova finalità, non potendosi basare il trattamento effettuato per la diversa finalità sul consenso prestato in relazione alla originaria finalità, né essendo ammissibile, per carenza del requisito della specificità, prestare un consenso anche per una finalità diversa, non ancora determinata) o (*ii*) su un atto legislativo che preveda il trattamento dei dati personali, quale misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'articolo 23, par. 1 – ipotesi, queste, nelle quali è possibile trattare ulteriormente i dati personali anche se le finalità sono tra loro incompatibili [cfr. CGUE, 2 marzo 2023, C-268/21 per la possibilità, da parte di una società committente, di utilizzare il registro del personale tenuto dall'appaltatore e contenente i dati dei lavoratori per finalità di controllo fiscale, per (il diverso fine) di dimostrare in giudizio l'infondatezza della domanda dell'appaltatore volta ad ottenere il pagamento del corrispettivo ancora dovuto] –; fuori da queste ipotesi è necessario accertare se la (diversa e ulteriore) finalità sia compatibile con quella originaria.

Di là dalle ipotesi del trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità a quanto previsto dall'art. 89 GDPR, trattamento considerato di per sé non incompatibile, al fine di verificare la compatibilità della ulteriore finalità (c.d. *test di compatibilità*) l'art. 6, par. 4 GDPR, unitamente al considerando 30 GDPR, invitano a tenere in considerazione: a) ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulte-

riore trattamento previsto; b) il contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) la natura dei dati personali (categorie particolari di dati personali, dati relativi a condanne penali e a reati); d) le possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) l'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione dei dati. Si tratta di criteri che, come ha precisato la Corte di Giustizia «riflettono la necessità di un nesso concreto, logico e sufficientemente stretto, tra le finalità della raccolta iniziale dei dati personali e l'ulteriore trattamento di tali dati, e consentono di assicurarsi che tale ulteriore trattamento non si discosti dalle legittime aspettative degli interessati quanto all'ulteriore utilizzo dei loro dati» [così CGUE, 20 ottobre 2022, C-77/21, secondo cui «il principio della "limitazione della finalità" non osta alla registrazione e alla conservazione da parte del titolare del trattamento, in una banca dati creata al fine di effettuare test e di correggere errori, di dati personali precedentemente raccolti per la diversa (ma compatibile) finalità consistente nella conclusione e nell'esecuzione di contratti di abbonamento»]. Laddove vi sia un trattamento ulteriore dei dati personali compatibile con le finalità originarie troveranno applicazione gli artt. 13, par. 3 e 14, par. 4 GDPR a mente dei quali il titolare «prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente». In particolare, secondo le *Linee guida WP29 sulla trasparenza ai sensi del regolamento 2016/679* i titolari del trattamento dovrebbero fornire «informazioni sull'analisi di compatibilità svolta ai sensi dell'articolo 6, paragrafo 4, qualora la nuova finalità del trattamento si fondi su una base giuridica diversa dal consenso o da un atto legislativo dell'Unione o degli Stati membri (in altre parole, una spiegazione del modo in cui il trattamento per una finalità diversa sia compatibile con la finalità iniziale)», in modo da consentire agli interessati «di valutare la compatibilità dell'ulteriore trattamento e delle garanzie fornite e di decidere se esercitare o no i loro diritti, ad esempio, tra gli altri, il diritto di limitazione di trattamento o il diritto di opporsi al trattamento».

12. Il principio di minimizzazione

Una volta fissata la finalità, il titolare deve trattare i dati personali nel rispetto del principio di necessità (o di minimizzazione) tra mezzi e fini: i dati personali devono essere pertanto adeguati e pertinenti (profilo qualitativo) e limitati (profilo quantitativo) a quanto necessario per il perseguimento della finalità per le quali sono trattati. I primi requisiti obbligano a verificare se la finalità perseguita (e es. la prova di un fatto in un giudizio instaurato per far valere un diritto o l'esecuzione di un servizio di trasporto ferroviario) «non possa essere realizzata ricorrendo a mezzi di prova meno invasivi» (CGUE, 2 marzo 2023, C-268/21) che non implichino i il trattamento dei dati personali. Il canone della limitazione, invece, impone di circoscrivere il trattamento ai soli dati indispensabili per la realizzazione dello scopo perseguito; così, a esempio, qualora sono una parte dei dati sia necessaria per far valere un proprio diritto in giudizio, «il giudice nazionale deve prendere in considerazione l'adozione di misure appropriate in materia di protezione dei dati, quali

la pseudonimizzazione […] dei nomi degli interessati o qualsiasi altra misura destinata a ridurre al minimo l'ostacolo al diritto alla protezione dei dati personali costituito dalla produzione di tale documento. Siffatte misure possono comprendere, in particolare, la limitazione dell'accesso del pubblico al fascicolo o l'ordine alle parti a cui i documenti contenenti dati personali sono stati comunicati di non utilizzare tali dati per finalità della prova durante il procedimento giurisdizionale di cui trattasi» (in tal senso CGUE, 2 marzo 2023, C-268/21). E, ancora, risponde al principio di minimizzazione, sotto il profilo quantitativo, la limitazione di una comunicazione commerciale ai soli «nomi e cognomi dei clienti, atteso che il loro appellativo e/o la loro identità di genere sono un'informazione che non pare essere strettamente necessaria in tale contesto» (CGUE, 9 gennaio 2025, C-394/23).

13. Il principio di esattezza e di limitazione della conservazione

I dati personali, prosegue l'art. 5, co. 1, lett. d) GDPR, devono essere esatti e aggiornati: la norma, che istituisce un obbligo per il titolare di fedeltà contenutistica del contenuto dei dati alla realtà da essi rappresentati, attribuisce, al contempo, all'interessato una serie di prerogative. Il primo, infatti, deve adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati; il secondo, se del caso anche esercitando il diritto di accesso, ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo nonché l'integrazione di quelli incompleti. Il principio di limitazione della finalità trova completamento sotto il profilo temporale nella previsione dell'art. 5, co. 1, lett. e) GDPR, il quale limita la possibilità di identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono stati trattati (*principio di limitazione della conservazione*): pertanto, una volta conseguita la finalità originariamente stabilita, un ulteriore trattamento che consenta l'identificazione dell'interessato (con esclusione dei trattamenti per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica) deve ritenersi non più consentito (cfr. CGUE, 20 ottobre 2022, C-77/21, secondo cui «il "principio della limitazione della conservazione" osta alla conservazione, da parte del titolare del trattamento, in una banca dati creata al fine di effettuare test e di correggere errori, di dati personali precedentemente raccolti per altre finalità, per un arco di tempo superiore a quello necessario alla realizzazione di tali test e alla correzione di tali errori»). All'obbligo del responsabile del trattamento di impedire l'ulteriore identificazione dell'interessato corrisponde il diritto di quest'ultimo di ottenere la cancellazione o la trasformazione in forma anonima dei dati personali.

14. Il principio di sicurezza e riservatezza

L'art. 5, co. 1, lett. f) GDPR richiede, infine, che i dati personali siano trattati in modo da garantirne un'adeguata sicurezza e riservatezza contro il rischio di trattamenti non autorizzati o illeciti, di perdita, distruzione o danni accidentali ai dati. A tal fine, l'art. 32 GDPR, prescrive al titolare e al responsabile di adottare – tenuto conto

dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto, delle finalità del trattamento, delle esigenze di protezione dei dati specificamente coinvolti e, dunque, dei rischi che presenta il trattamento (cfr., altresì, i considerando 75, 76 e 83 GDPR) – ogni misura tecnica e organizzativa idonea ad evitare una violazione dei dati personali e indica, a titolo esemplificativo, tra le misure da adottare: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

15. Il principio di accountability

L'art. 32 GDPR rappresenta una specificazione, in materia di sicurezza, della più generale disciplina dettata all'art. 24 GDPR, il quale obbliga il titolare e il responsabile del trattamento, tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, ad adottare ogni altra misura tecnica e organizzativa adeguata per garantire che il trattamento sia effettuato in conformità al regolamento (cfr., altresì, il considerando 74 GDPR). La norma dà espresso riconoscimento al c.d. principio di accountability (da tradurre come responsabilizzazione e non responsabilità) il quale si concretizza in un mutamento di approccio da parte del legislatore europeo: in luogo di prescrizione dirette e precise, alla cui mancata applicazione consegue una sanzione, il regolamento prevede un obiettivo generale (la conformità ai principi del regolamento), affidando al titolare la scelta delle modalità concrete più adeguate per conseguirlo e rimettendo all'autorità di controllo o al giudice la successiva valutazione in merito alla loro adeguatezza.

Oltre all'art. 24 GDPR e al già richiamato art. 32 GDPR in materia di sicurezza fa diretto riferimento al principio di *accountability* anche l'art. 5, co. 2 GDPR, il quale dispone che «il titolare del trattamento è competente per il rispetto del paragrafo 1 [che menziona i principi applicabili al trattamento] e in grado di comprovarlo», così evidenziando il duplice profilo prescrittivo e probatorio che dà contenuto al principio: all'obbligo di conformarsi alle prescrizioni del regolamento si affianca infatti l'obbligo di dimostrare la correttezza e l'adeguatezza della misura adottata e, più in generale, la conformità al regolamento. A tal fine particolare importanza riveste il registro delle attività di trattamento che il titolare e il responsabile devono tenere ai sensi dell'art. 30 GDPR: la sua omissione, tuttavia, sebbene renda meno agevole dimostrare la conformità del trattamento ai principi del regolamento, non dimostra di per sé che i diritti e le libertà degli interessati siano stati violati (così CGUE, 4 maggio 2023, C-60/22). Sono espressione del principio di *accountability* anche l'art. 12 GDPR, là dove rimette al titolare la scelta delle «misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22»; l'art. 7 GDPR, il quale rimette al titolare del trattamento la scelta della modalità di acquisizione del consenso e del conseguente

onere probatorio; l'art. 6, co. 1, lett. f) GDPR, il quale impone al titolare del trattamento di compiere la valutazione comparativa tra il proprio legittimo interesse e gli interessi e i diritti dell'interessato.

Nella scelta della misura più appropriata, il titolare del trattamento, nell'esercizio della discrezionalità di cui dispone, deve tenere conto tra gli altri, e specie in materia di sicurezza, del livello di *rischio* che il trattamento presenta per i diritti e le libertà dell'interessato (art. 32, par. 1, GDPR). A tal fine il titolare, prima di avviare il trattamento, deve svolgere una valutazione di impatto qualora prevede di utilizzare una nuova tecnologia o, indipendentemente dal mezzo utilizzato, allorquando, considerati la natura, l'oggetto, il contesto e le finalità del trattamento valuti l'esistenza di un rischio elevato per i diritti e le libertà delle persone fisiche (art. 35, par. 1 GDPR; v., altresì, provvedimento del Garante per la protezione dei dati personali n. n. 467 dell'11 ottobre 2018), come accade, a esempio, nelle ipotesi: a) di trattamento che implica una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) di trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, par. 1, o di dati relativi a condanne penali e a reati di cui all'art. 10; c) di trattamento che implica la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. La valutazione di impatto che il titolare del trattamento deve svolgere, consultando il responsabile del trattamento e, se del caso, gli interessati o i loro rappresentanti, e che, dovrà essere periodicamente riesaminata (art. 35, par. 11 GDPR), include gli adempimenti di cui all'art. 35, par. 7 GDPR, tra i quali spicca la individuazione e la valutazione dei rischi per i diritti e le libertà degli interessati nonché la successiva illustrazione delle misure predisposte per affrontare tali rischi e rendere il trattamento conforme al Regolamento.

Qualora a seguito della valutazione di impatto dovesse emergere che, tenuto conto della tecnologia disponibili e dei costi di attuazione (considerando 84 GDPR) le misure adottate dal titolare non sono in grado di ridurre il rischio (il quale, dunque, persiste elevato) quest'ultimo sarà obbligato a consultare l'autorità di controllo, la quale – anche esercitando i poteri di indagine previsti dall'art. 58 – là dove dovesse accertare che il trattamento violi il Regolamento entro il termine di otto settimane (prorogabile di ulteriori sei settimane) dovrà emanare un parere scritto.

Strettamente connessi con il principio di responsabilizzazione e con la valutazione d'impatto, sono i c.d. principi della *privacy by design* e *privacy by default*, sanciti all'art. 25 (cfr., altresì, EDPB Linee guida 4/2019 sull'articolo 25, Protezione dei dati fin dalla progettazione e per impostazione predefinita), i quali – tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione del contesto e delle finalità del trattamento così come dei rischi del trattamento – impongono, sin dalla progettazione del trattamento (dunque prima che il trattamento sia avviato), nonché per impostazione predefinita, l'adozione di soluzioni tecniche e organizzative (la cui individuazione in concreto spetta al titolare di determinare) adeguate per rendere conforme il trattamento ai principi del Regolamento.

Ciò comporta, a esempio, che il titolare che intenda trattare dati personali per finalità di vendita *online* di beni dovrà configurare il *layout* del sito internet in mo-

do da fornire le informazioni in conformità a quanto prescritto dall'art. 12 GDPR: dovrà, perciò, adottare un approccio multilivello, evidenziando immediatamente i punti più importanti e, mediante la creazione di menu a discesa e collegamenti ad altre pagine, mettere a disposizione dell'interessato le ulteriori informazioni di dettaglio; dovrà, ancora, rendere visibile l'informativa privacy su tutte le pagine del sito di modo che l'interessato acceda sempre alle informazioni con un semplice *clic*; dovrà, infine, mettere a disposizione le informazioni nel giusto contesto e al momento adeguato, utilizzando ad esempio *snippet* informativi o *pop-up*. Il medesimo titolare dovrà, poi, predisporre il modulo d'ordine per la raccolta dei dati personali dei clienti in conformità al principio di minimizzazione: dopo aver individuato i dati personali strettamente necessari per l'acquisto dei beni, dovrà, ad esempio, rendere opzionale la compilazione di quei campi del modulo d'ordine che richiedono dati ulteriori rispetto a quelli necessari per l'esecuzione del contratto. Sempre avuto riguardo al principio di minimizzazione, il titolare del trattamento – in un altro esempio: un ospedale che gestisce le informazioni sullo stato di salute dei pazienti – dovrà, per impostazione predefinita, consentire l'accesso a tali informazioni solo ai membri del personale medico ai quali sia affidata la cura del paziente nel reparto specifico cui questi è assegnato. Con riferimento, invece, al principio di limitazione della conservazione, il titolare del trattamento dovrà anzitutto definire e adottare una procedura interna per la conservazione e la cancellazione dei dati, in base alla quale i dipendenti cancelleranno manualmente i dati personali dopo la fine del periodo della loro conservazione e, poi, per rendere più efficace la cancellazione, predisporre un meccanismo di cancellazione dei dati automatico. In attuazione del principio di integrità e sicurezza, il titolare del trattamento dovrà, infine, a titolo esemplificativo, predisporre un sistema di gestione della sicurezza delle informazioni, limitare l'accesso soltanto a taluni dipendenti, dotati di chiavi di accesso, predisporre una segregazione della rete in modo tale che l'eventuale *malware* che abbia superato il perimetro di *security* non sia in grado di paralizzare tutti i dispositivi aziendali connessi; prevedere la pesudonimizzazione dei dati.

Sez. III. La violazione dei dati personali

16. Introduzione. La nozione

La violazione dei dati personali, spesso nota con l'espressione inglese di *data breach*, è definita dal legislatore europeo come «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4, n. 12) GDPR). A tale nozione fanno riferimento alcune regole (artt. 33-34 GDPR), che al ricorrere, per l'appunto, di una violazione dei dati personali, gravano il titolare del trattamento e, in parte, il responsabile del trattamento di una serie di obblighi.

Prima di esaminare nel dettaglio i vari elementi che compongono la nozione e la disciplina, è utile soffermarsi su alcuni aspetti preliminari per ricostruire la storia e la finalità dell'istituto in esame.

Le norme sulla violazione dei dati personali rappresentano una novità introdotta dal GDPR. La direttiva 95/46/CE, infatti, non disciplinava le conseguenze di un'eventuale violazione dei dati personali, né tanto meno ne forniva una definizione. In realtà, già si prevedevano obblighi di sicurezza in capo al titolare del trattamento «al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, […] o da qualsiasi altra forma illecita di trattamento di dati personali» (art. 17, par. 1, direttiva 95/46); tuttavia, mancavano specifiche disposizioni per l'ipotesi in cui tali circostanze, oggi qualificabili come violazioni di dati personali, si verificassero.

Prima dell'adozione del GDPR, il legislatore europeo si era comunque già occupato della violazione dei dati personali in un intervento di modifica della direttiva e-privacy, contenuto nella direttiva 2009/136/CE. A livello di diritto interno, l'art. 4, co. 3, lett. g-*bis*) del codice privacy, introdotto in attuazione di quest'ultima direttiva dal d.lgs. n. 69/2012, definiva la violazione dei dati personali come la «violazione della sicurezza che comporta anche accidentalmente la distruzione, la perdita, la modifica, la rivelazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque elaborati nel contesto della fornitura di un servizio di comunicazione accessibile al pubblico». Tale fattispecie, in armonia con il disposto della direttiva comunitaria, veniva presa in considerazione, dall'abrogato art. 32-*bis*, cod. privacy, solo nell'ambito dei servizi di comunicazione elettronica accessibili al pubblico (ad esempio, servizi telefonici, servizi di accesso a Internet), il cui fornitore veniva obbligato, al verificarsi di una siffatta violazione, di informare il Garante per la protezione dei dati personali e, qualora la violazione rischiasse di arrecare pregiudizio ai dati personali o alla riservatezza dell'utente contraente del servizio o di altra persona, di compiere una comunicazione a questi ultimi. Simili obblighi informativi, in caso di violazioni dei dati, venivano imposti anche alle banche (v. provvedimento del Garante per la protezione dei dati personali n. 192 del 12 maggio 2011), ai titolari dei trattamenti di dati biometrici (v. provvedimento del Garante per la protezione dei dati personali n. 513 del 12 novembre 2014), alle strutture sanitarie (v. provvedimento del Garante per la protezione dei dati personali n. 331 del 4 giugno 2015) e alle amministrazioni pubbliche (v. provvedimento del Garante per la protezione dei dati personali n. 393 del 2 luglio 2015).

Sono diverse le analogie con le norme adesso previste dal GDPR. Tuttavia, la differenza più significativa risiede nell'ambito applicativo soggettivo: mentre, in passato, gli obblighi da osservare in caso di *data breach* incombevano soltanto su alcuni soggetti, adesso gravano su qualunque titolare del trattamento di dati personali.

Come risulta ormai chiaro, le norme sulla violazione dei dati personali devono essere lette in stretta connessione agli obblighi di sicurezza del titolare del trattamento (art. 32 GDPR), i quali rappresentano un'espressa concretizzazione del principio sancito dall'art. 5, par. 1, lett. f) GDPR (v. *supra* in questo cap., sez. II, § 14). La stessa nozione sopra richiamata (art. 4, n. 12 GDPR), infatti, definisce la violazione dei dati personali come una «violazione di sicurezza».

Non bisogna, però, intendere che quest'ultima consista necessariamente in una violazione degli obblighi previsti dall'art. 32, relativi all'adozione di misure

tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio connesso al trattamento dei dati. La sicurezza, infatti, può risultare violata anche in assenza di condotte censurabili del titolare o del responsabile del trattamento (CGUE, 14 dicembre 2023, C-340/21, § 31). La violazione dei dati personali va intesa, dunque, come un incidente di sicurezza informatica da cui discende una situazione pregiudizievole per i dati personali trattati – quale la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzati – che può comportare un rischio per i diritti e le libertà delle persone fisiche cui i dati si riferiscono (art. 33, par. 1 GDPR).

La causa dell'incidente potenzialmente rischioso può essere di natura accidentale o illecita. In quest'ultimo caso, l'illecito (ad esempio, una frode informatica) è solitamente imputabile a terzi diversi dal titolare e dall'eventuale responsabile del trattamento, i quali, tuttavia, possono essere comunque ritenuti (in parte) responsabili della violazione di sicurezza, laddove non abbiano preventivamente adottato le misure volte a proteggere i dati personali dall'esterno. In ogni caso, al di là del concorso nella causa della violazione, il titolare e il responsabile del trattamento possono essere ritenuti responsabili del rischio generato dalla violazione stessa, laddove non abbiano eseguito in modo adeguato e tempestivo gli adempimenti necessari dopo il *data breach*. Il rischio, che deriva dalla violazione di sicurezza, dev'essere affrontato secondo tali modalità per evitare che lo stesso si traduca in danni per gli interessati.

La disciplina predisposta dal legislatore europeo mira, quindi, ad anticipare la tutela delle persone fisiche coinvolte a uno stadio precedente rispetto al concretizzarsi dei danni, peraltro non sempre facilmente riparabili (cfr. *infra* cap. *Il risarcimento del danno da illecito trattamento dei dati personali*).

Tra i pregiudizi che gli interessati al trattamento possono subire in ragione di una violazione dei dati personali, si possono citare, a titolo esemplificativo: la perdita del controllo sui dati personali che li riguardano, la limitazione dei loro diritti, la decifratura non autorizzata della pseudonimizzazione, la discriminazione, il furto o l'usurpazione d'identità, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale, perdite finanziarie (v. considerando 85 GDPR).

Per definire in modo completo il significato della nozione di violazione di sicurezza, occorre altresì precisare cosa si intende per «distruzione», «perdita» e «modifica» dei dati personali, oltre che per «divulgazione» e «accesso» non autorizzati. A tal fine, preziose indicazioni provengono dalle *Linee guida n. 9/2022 sulla notifica delle violazioni dei dati personali*, adottate il 28 marzo 2023 dal Comitato europeo per la protezione dei dati (European Data Protection Board)[2].

[2] Le Linee guida 9/2022 hanno aggiornato le precedenti Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017 ed emendate il 6 febbraio 2018. Ancora prima, il medesimo Gruppo di lavoro aveva adottato il Parere 03/2014 sulla notifica delle violazioni, riferito, tuttavia, all'obbligo dei fornitori di servizi di comunicazione elettronica ai sensi della direttiva 2002/58/CE.

In tale documento, si chiarisce che: la «distruzione» dei dati personali si verifica quando i dati non esistono i più, o comunque non esistono più in una forma che possa permetterne un qualsiasi uso da parte del titolare del trattamento; la «perdita» dei dati personali sottende una situazione in cui i dati possono ancora essere presenti, ma il titolare del trattamento ne ha perso il controllo o l'accesso, o non ne è più in possesso; la «modifica» dei dati personali ha luogo quando i dati perdono la loro integrità; la «divulgazione» e l'«accesso» non autorizzati sono, infine, due ipotesi nelle quali i dati personali sono, rispettivamente, oggetto di una comunicazione a destinatari non autorizzati al trattamento o, in assenza di comunicazione, di un accesso da parte di terzi che non avrebbero dovuto trattare i medesimi dati.

Le fattispecie appena descritte sono classificabili, in base ai principi di sicurezza informatica, all'interno di tre diverse tipologie di violazioni: la violazione della riservatezza; la violazione dell'integrità; la violazione della disponibilità. Mentre la divulgazione e l'accesso non autorizzati realizzano un *vulnus* alla riservatezza dei dati, la modifica ne intacca l'integrità, e la perdita, al pari della distruzione, fa sì che i dati non siano più nella disponibilità del titolare. In base alle circostanze, la gravità della violazione può variare: il grado massimo si raggiunge quando essa presenta una combinazione delle tre tipologie menzionate.

Si pensi, a esempio, a un attacco informatico che riesca, da un lato, a cifrare i dati personali in possesso del titolare (c.d. attacco *ransomware*), con conseguente perdita di disponibilità dei dati in mancanza di un *backup*, cioè di una copia di sicurezza, e che riesca, d'altro lato, anche ad esportarli (c.d. esfiltrazione) e a modificarli, con conseguente violazione di riservatezza e integrità. All'estremo opposto, come incidente meno grave, si pone il caso di una semplice perdita temporanea di disponibilità dei dati, che talvolta, come evidenziano le *Linee guida 9/2022*, potrebbe anche non trattarsi di una violazione di sicurezza, come quando la perdita temporanea è dovuta a un intervento programmato di manutenzione del sistema informatico su cui i dati sono conservati. Tuttavia, ciò non vale per altre ipotesi in cui si verifica una mancanza temporanea di controllo dei dati: ad esempio, se questa è imputabile a un'interruzione prolungata di corrente elettrica, pur non presentando solitamente rischi per i diritti e le libertà degli interessati, dovrebbe essere comunque considerata una violazione, con le conseguenze che ne derivano per il titolare del trattamento.

17. L'obbligo di documentazione

La violazione dei dati personali è fonte di una serie di obblighi per il titolare e il responsabile del trattamento. Alcuni di tali obblighi sorgono qualora la violazione abbia determinate caratteristiche; altri, invece, rappresentano una costante di qualsiasi violazione dei dati personali. Nel primo gruppo, come vedremo, rientrano la notifica all'autorità di controllo e la comunicazione agli interessati, da parte del titolare del trattamento; nel secondo, occorre annoverare l'obbligo di informazione del responsabile del trattamento nei confronti del titolare e l'obbligo di documentazione dell'incidente gravante su quest'ultimo.

In particolare, a tal riguardo, l'art. 33, par. 5 GDPR prevede che il titolare del trattamento documenti qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione dev'essere conservata in quanto la stessa potrà essere esaminata dall'autorità di controllo per verificare che il titolare abbia agito in conformità agli (altri) obblighi previsti dal GDPR, in caso di violazione dei dati personali. L'obbligo di documentazione risulta, dunque, strumentale all'attività di vigilanza sull'applicazione del GDPR, svolta dall'autorità di controllo (v. *infra* cap. *La regolamentazione e la tutela amministrativa*, § 1).

Al contempo, la documentazione serve allo stesso titolare del trattamento per (mettersi in grado di) dimostrare di aver operato nel rispetto della disciplina in materia di protezione dei dati personali. Da quest'angolo di visuale, l'obbligo in esame costituisce una chiara concretizzazione del principio di responsabilizzazione (*accountability*), sancito dall'art. 5, par. 2 GDPR e attuato, in termini generali, dagli obblighi del titolare del trattamento di cui all'art. 24, par. 1 GDPR (v. *supra* in questo cap., sez. II, § 15). Per il rispetto del suddetto principio, oltre alla documentazione raccolta, assume rilevanza anche la conoscenza, da parte dei dipendenti del titolare, delle procedure da adottare in caso di *data breach*: a tal fine, può risultare utile, a livello interno, la redazione preventiva di un manuale per la gestione delle violazioni dei dati.

Per conservare la documentazione relativa alle violazioni di sicurezza, è implicito, come specificano le *Linee guida 9/2022*, che il titolare del trattamento tenga un registro delle violazioni in questione. Non deve necessariamente trattarsi di un registro separato da quello relativo alle attività di trattamento di cui all'art. 30, par. 1 GDPR, potendo costituire semplicemente parte di quest'ultimo.

Il titolare del trattamento è, quindi, abbastanza autonomo nella scelta del metodo con cui registrare le informazioni relative a una violazione dei dati personali; è, invece, vincolato rispetto al contenuto, che deve includere tanto le cause dell'incidente di sicurezza, quanto gli effetti, con speciale riferimento alle azioni intraprese dal titolare per porvi rimedio. A quest'ultimo riguardo, pur nel silenzio dell'art. 33, par. 5 GDPR, il Comitato europeo per la protezione dei dati raccomanda di documentare anche le ragioni che hanno condotto alle azioni in questione. Se, ad esempio, il titolare del trattamento non notifica la violazione dei dati personali all'autorità di controllo, è bene che nel registro siano riportati i motivi in base ai quali il titolare ritiene che la violazione non presenti un rischio per i diritti e le libertà delle persone fisiche, cui i dati violati si riferiscono.

L'obbligo di documentazione implica la conservazione delle informazioni relative alla violazione di sicurezza; pertanto, laddove tali informazioni facciano esplicito riferimento a dati personali, si pone il problema di definire il periodo di conservazione di tali dati. Occorre rifarsi al principio generale secondo cui i dati possono essere conservati, 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 (art. 5, par. 1, lett. e) GDPR). Nel caso in questione, la conservazione è ammessa finché il titolare del trattamento può essere chiamato a fornire prova, dinanzi all'autorità di controllo, del rispetto della procedura relativa al *data breach* e, più in generale, del rispetto del principio di *accountability*.

18. La notifica all'autorità di controllo

Se la documentazione è un'attività sempre necessaria nel caso in cui si verifichi una violazione di dati personali, non può dirsi altrettanto per la notifica all'autorità di controllo, cioè il Garante per la protezione dei dati personali. Il titolare del trattamento, infatti, può esimersi dalla notifica quando ritiene improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche (art. 33, par. 1 GDPR).

Nella valutazione di tale rischio, il titolare può avvalersi del responsabile della protezione dei dati (meglio noto come *Data Protection Officer*: *DPO*), che, quando presente (v. art. 37, parr. 1 e 4 GDPR), deve fornire consulenza in merito agli obblighi derivanti dalla disciplina europea e nazionale sulla protezione dei dati personali (art. 39, par. 1, lett. a)). Il *DPO* (sulla cui figura, v. *supra* cap. *Le definizioni fondamentali*, § 7), inoltre, è indicato come il punto di contatto presso cui l'autorità di controllo può ottenere informazioni aggiuntive, circa la violazione dei dati personali, rispetto a quelle inserite nella notifica effettuata dal titolare. Per tale ragione, si devono almeno comunicare il nome e i dati di contatto (ad esempio, l'indirizzo e-mail) del responsabile della protezione dei dati (art. 33, par. 3, lett. b)).

Prima di esaminare i fattori da considerare per la valutazione dei rischi della violazione, propedeutica all'eventuale notifica al Garante, è bene evidenziare che il titolare deve preliminarmente venire a conoscenza del *data breach*. Ciò deve avvenire il prima possibile: infatti, solo se si prende consapevolezza dell'incidente di sicurezza in tempi rapidi, è possibile effettuare la notifica all'autorità di controllo «senza ingiustificato ritardo», come richiede l'art. 33, par. 1. Inoltre, la stessa norma impone al titolare del trattamento, una volta appresa la violazione, di procedere con la notifica, ove possibile, entro 72 ore; altrimenti, il titolare deve specificare all'autorità di controllo i motivi del ritardo.

La *ratio* alla base di tali prescrizioni è che prima si interviene, informando il Garante per la protezione dei dati personali, meglio si riesce a mitigare i rischi discendenti dal *data breach*. Coerentemente con tale disegno, occorre che il titolare del trattamento, al fine di agire in modo tempestivo, si doti di tutte le misure tecnologiche e organizzative adeguate per stabilire immediatamente se c'è stata violazione dei dati personali (v. considerando 87 GDPR). Talvolta, il titolare potrebbe semplicemente sospettare che una violazione di dati personali abbia avuto luogo; in casi del genere, svolgerà celermente una verifica interna per accertarne il reale avvenimento e, in tale frangente temporale, non potrà considerarsi ancora consapevole della violazione per il decorso del termine delle 72 ore entro cui effettuare la notifica (v. le *Linee guida 9/2022*).

Da non trascurare, inoltre, il ruolo del responsabile del trattamento, il quale, con l'obbligo di informare tempestivamente il titolare di eventuali incidenti di sicurezza (art. 33, par. 2 GDPR), contribuisce a mettere quest'ultimo nelle condizioni di notificare la violazione al Garante senza ingiustificato ritardo.

Da quando il titolare del trattamento viene a conoscenza del *data breach*, egli deve procedere senza indugio alla valutazione del rischio per i diritti e le libertà delle persone fisiche, vale a dire il rischio che la violazione dei dati personali comporti discriminazioni, furti o usurpazioni di identità, perdite finanziarie, pregiudizi alla

reputazione, perdita di riservatezza dei dati personali protetti da segreti professionali, decifratura non autorizzata di dati pseudonimizzati, perdita del controllo dei dati personali da parte degli interessati, o qualsiasi altro danno economico o sociale significativo (v. considerando 75 e 85 GDPR).

La valutazione di tali rischi, come si è visto (v. *supra* in questo cap., sez. II, § 15), ricorre anche nell'ambito della valutazione di impatto sulla protezione dei dati (v. art. 35, par. 7, lett. c) GDPR). Non bisogna, tuttavia, pensare che la valutazione dei rischi susseguente a una violazione di dati personali coincida con quella oggetto di una *data protection impact assessment* (*DPIA*). Invero, sebbene nella *DPIA* si faccia riferimento anche ai rischi connessi a un eventuale *data breach*, non può trascurarsi che i rischi in essa valutati riguardano un evento del tutto ipotetico, con la conseguenza che la probabilità del loro verificarsi può essere ben diversa rispetto a quella inerente a un incidente di sicurezza che si è concretamente verificato. D'altronde, in una *DPIA* si prendono in considerazione i dati personali genericamente coinvolti in un determinato trattamento, mentre nella valutazione dei rischi successiva a un *data breach* si tiene conto soltanto dei dati personali violati.

I rischi possono variare in base a diversi fattori. Tra questi, le *Linee guida 9/2022* suggeriscono di valorizzare: il tipo di violazione; la natura, la sensibilità e il volume dei dati violati; la facilità di identificazione degli interessati, così come il numero e le caratteristiche degli stessi, oltre alla gravità di conseguenze che la violazione può causare nei loro confronti. Invero, la perdita di disponibilità, dovuta a un attacco informatico, di dati particolarmente sensibili (ad esempio, i dati delle cartelle cliniche dei pazienti di un ospedale) presenta rischi maggiori dell'accesso non autorizzato, da parte di un ex dipendente del titolare, a dati comuni di un gruppo, pur numeroso, di interessati (ad esempio, il nome, il cognome e la data di nascita dei clienti possessori della carta fedeltà di un supermercato). A sua volta, quest'ultima violazione risulta più rischiosa dell'invio involontario, al destinatario sbagliato, di un'e-mail contenente informazioni di non particolare rilievo, relative ad un solo interessato (ad esempio, un'e-mail di conferma dell'ordine di acquisto di una t-shirt, effettuato da un singolo cliente).

Al contempo, l'adozione preventiva di tecniche di protezione dei dati può ridurre sensibilmente i rischi, anche a fronte di violazioni che colpiscano dati rilevanti (ad esempio, l'esfiltrazione da un sito web delle password degli utenti è poco probabile che comporti rischi per gli interessati nella misura in cui le password siano crittografate e l'autore dell'attacco informatico non abbia accesso alla chiave crittografica). Quest'ultimo esempio è tratto dall'accurata casistica delle violazioni di dati personali più frequenti, stilata dal Comitato europeo per la protezione dei dati, che fornisce altresì le istruzioni necessarie sulle azioni da intraprendere da parte del titolare del trattamento (v. *EDPB, Linee guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali*).

Se dalla valutazione, che il titolare del trattamento è chiamato a compiere, risulta un rischio per i diritti e le libertà degli interessati, la notifica al Garante per la protezione dei dati personali è obbligatoria.

Le informazioni da fornire devono comprendere almeno: la descrizione della natura della violazione dei dati personali, compresi, ove possibile, le categorie e il

numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; la comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere informazioni; la descrizione delle probabili conseguenze della violazione dei dati personali; la descrizione delle misure adottate, o di cui si propone l'adozione, da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e, se del caso, per attenuarne i possibili effetti negativi (art. 33, par. 3 GDPR).

È possibile che il titolare non riesca a raccogliere tutte le informazioni da notificare all'autorità di controllo entro il breve termine di 72 ore dalla scoperta della violazione dei dati personali. Per tale ragione, l'art. 33, par. 4 permette di fornire le informazioni mancanti dopo la notifica, purché ciò avvenga «senza ulteriore ingiustificato ritardo». A fronte di attacchi informatici particolarmente sofisticati, può darsi, ad esempio, che solo un'indagine di polizia riesca a ricostruire la natura e la portata dell'incidente di sicurezza; in tal caso, una volta ottenute le ulteriori informazioni sulla violazione dei dati personali, il titolare può integrare la notifica in una fase successiva.

19. La comunicazione agli interessati

La notifica all'autorità di controllo e l'adozione di misure idonee ad attenuare i rischi del *data breach*, da documentare, a livello interno, insieme alle caratteristiche della violazione, non esauriscono gli adempimenti del titolare del trattamento. Come si è anticipato, infatti, la violazione di sicurezza richiede anche la comunicazione agli interessati, i cui dati sono stati violati, laddove il rischio per i loro diritti e le loro libertà risulti elevato. Nell'esempio sopra citato di un attacco informatico che renda indisponibili i dati delle cartelle cliniche dei pazienti di un ospedale, non vi è dubbio che si ricada in tale fattispecie. Ma, volendo cambiare tipologia di violazione, lo stesso varrebbe anche in caso di furto di un supporto materiale su cui sono memorizzati dati personali non cifrati di un numero molto significativo di soggetti (ad esempio, il furto del computer portatile del dipendente di una società di servizi contenente una lista di oltre 100.000 clienti, comprendente, oltre che il nome e il cognome, il sesso, la data di nascita e l'indirizzo di residenza: l'esempio è tratto dalle *Linee guida 01/2021*).

Valutata la gravità del rischio derivante dal *data breach*, il titolare del trattamento, senza ingiustificato ritardo, deve comunicare agli interessati la violazione, descrivendone la natura e le probabili conseguenze e informandoli delle misure adottate o di cui si propone l'adozione per porvi rimedio, facendo altresì riferimento ai dati di contatto del responsabile della protezione dei dati (art. 34, parr. 1-2 GDPR). Ove opportuno, la comunicazione dovrebbe anche fornire raccomandazioni agli interessati sulle misure da impiegare per proteggere sé stessi dai possibili effetti negativi della violazione (v. considerando 86 GDPR): ad esempio, a seguito di un attacco informatico a un sito web, potrebbe suggerire il cambio di password, nel caso in cui vi sia il dubbio che l'autore dell'attacco abbia avuto accesso alle credenziali degli utenti. D'altronde, l'obbligo di comu-

nicazione mira proprio a mettere gli interessati nelle condizioni di prendere consapevolezza dei rischi e di agire, ove possibile, con misure di autoprotezione.

La scelta del mezzo comunicativo è rimessa al titolare del trattamento, che, su raccomandazione del Comitato europeo per la protezione dei dati (v. le *Linee guida 9/2022*), dovrebbe comunque preferire il canale più idoneo a far pervenire correttamente la comunicazione a tutti gli interessati. In quest'ottica, il titolare potrebbe anche ricorrere contemporaneamente a diversi canali, come l'invio di messaggi telematici (ad esempio, e-mail, SMS), o cartacei tramite i servizi postali, oppure la pubblicazione di banner su siti web di primo piano. Non è, invece, sufficiente la pubblicazione di un comunicato stampa.

In ogni caso, la comunicazione dev'essere trasparente: il titolare deve utilizzare un linguaggio semplice e chiaro per gli interessati (art. 34, par. 2 GDPR) e deve evitare di inviare le informazioni sul *data breach* insieme ad altre informazioni che, non riguardando la violazione, potrebbero sviare l'attenzione dei destinatari. Sul piano della comprensibilità del messaggio, inoltre, è di particolare rilievo la lingua in cui la comunicazione viene scritta. Il titolare dovrebbe impiegare la lingua già utilizzata in altre occasioni di contatto con gli interessati; tuttavia, se non vi sono state precedenti interazioni, può essere accettata, stando alle indicazioni del Comitato europeo per la protezione dei dati, la lingua del Paese in cui il titolare del trattamento ha sede.

In casi particolari, nonostante la violazione possa astrattamente comportare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, il titolare del trattamento è esonerato dalla comunicazione. Ciò avviene quando: a) il titolare ha adottato, prima della violazione, misure adeguate di protezione dei dati, quali la cifratura; b) il titolare adotta, dopo la violazione, misure atte a scongiurare il sopraggiungere del rischio elevato, come, ad esempio nel caso in cui riesca a identificare l'autore del *data breach*, impedendogli di fare alcunché coi dati violati (art. 34, par. 3 GDPR). Una terza fattispecie in cui il titolare può legittimamente astenersi dal comunicare agli interessati la violazione, sebbene quest'ultima presenti realmente un rischio elevato per i diritti e le libertà degli interessati, si ha quando tale comunicazione richiederebbe sforzi sproporzionati. È il caso in cui i dati di contatto degli interessati sono stati persi a causa della violazione o, già da prima, non erano nella disponibilità del titolare del trattamento. Questi deve, comunque, procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia (art. 34, par. 3, lett. c) GDPR).

Se il titolare ritiene che ricorra una delle condizioni appena descritte, può evitare di comunicare la violazione dei dati personali agli interessati. Nel rispetto del principio di responsabilizzazione (*accountability*), deve essere in grado di dimostrare al Garante per la protezione dei dati che la condizione di esonero sia soddisfatta. L'autorità di controllo può, da par suo, decidere che effettivamente si ricada in una delle ipotesi sopra menzionate, confermando la legittimità della scelta del titolare; tuttavia, può anche richiedere a quest'ultimo di provvedere alla comunicazione non ancora effettuata (art. 34, par. 4 GDPR), esercitando, se del caso, i propri poteri per sanzionare l'omissione.

Riferimenti bibliografici

Barba Angelo, Pagliantini Stefano (a cura di). 2019. *Delle persone. Leggi collegate*, II. Torino: Utet.

Bolognini, Luca. 2016. "I principi del trattamento." In Bistolfi C., Bolognini L., Pelino E., *Il Regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*. Milano: Giuffrè.

Caggia, Fausto. 2019. "Libertà ed espressione del consenso." In Vincenzo Cuffaro, Roberto D'Orazio e Vincenzo Ricciuto, *I dati personali nel diritto europeo*. Torino: Giappichelli, pp. 249-73.

Dell'Utri, Marco. 2019. "Principi generali e condizioni di liceità del trattamento dei dati personali." In Cuffaro Vincenzo, D'Orazio Roberto, Ricciuto Vincenzo (a cura di), *I dati personali nel diritto europeo*. Torino: Giappichelli.

Finocchiaro, Giusella. 2017. "Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali." In Finocchiaro Giusella (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*. Bologna: Zanichelli.

Garofalo, Andrea M. 2022. "Il campo di applicazione del GDPR e i principi del trattamento." In Magri Geo, Martinelli Silvia, Thobani Shaira (a cura di), *Manuale di diritto privato delle nuove tecnologie*. Torino: Giappichelli.

Iamiceli, Paola, Cafaggi, Fabrizio, Angiolini Chiara (a cura di). 2022. *Casebook Effective Data Protection and Fundamental Rights*. Scuola Superiore della Magistratura.

Irti, Claudia. 2021. *Consenso "negoziato" e circolazione dei dati personali*. Torino: Giappichelli.

Kamara, Irene, De Hert, Paul. 2018. "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach." *Bruxelles Privacy Hub Working Paper* n. 12.

Lucchini Guastalla, Emanuele. 2019. "Privacy e Data Protection: principi generali." In Tosi Emilio (a cura di), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*. Milano: Giuffrè.

Malgieri, Gianclaudio. 2021. "Art. 5." In D'Orazio Roberto, Finocchiaro Giusella, Pollicino Oreste, Resta Giorgio, *Codice della privacy e data protection*. Milano: Giuffrè.

Messinetti, Davide. 1998. "Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali." *Riv. crit. dir. privato* 3.

Panetta, Rocco (a cura di). 2019. *Circolazione e protezione dei dati personali tra libertà e regole di mercato. Commentario al regolamento UE n. 2016/679 e al novellato d.lgs. n. 196/2003*. Milano: Giuffrè.

Renna, Mario. 2020. "Violazione dei dati personali, sicurezza del trattamento e protezione dai rischi". *Rivista del mercato assicurativo e finanziario* 2: 197-221.

Resta, Giorgio. 2000. "Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali." *Rivista critica del diritto privato* 2: 299-333.

Resta, Giorgio, Zeno-Zencovich, Vincenzo. 2018. "Volontà e consenso nella fruizione dei servizi in rete." *Riv. trim. dir. proc. civ* 2.