CAPITOLO IV
IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI E IL REGOLAMENTO (UE) 2016/679

di *Juri Monducci*

SOMMARIO: 1. Introduzione. – 2. L'ambito di applicazione. – 3. I principi e le definizioni. – 4. I soggetti. – 5. Il trattamento dei dati personali e le condizioni di legittimità. – 5.1. Le modalità del trattamento dei dati personali. – 5.2. La notificazione. – 5.3. L'informativa. – 5.4. Il consenso dell'interessato. – 5.5. Il trattamento dei dati sensibili e giudiziari. – 5.6. Il trattamento dei dati per finalità giornalistiche. – 5.7. Il trasferimento dei dati all'estero. – 6. I diritti dell'interessato. – 7. Il trattamento da parte di soggetti pubblici. – 7.1. Il trattamento dei dati comuni. – 7.2. Il trattamento dei dati sensibili. – 8. Il Garante per la protezione dei dati personali. – 9. La tutela giurisdizionale e amministrativa. – 10. La responsabilità nel trattamento dei dati. – 10.1. La responsabilità civile. – 10.2. La responsabilità penale. – 10.3. La responsabilità amministrativa. – 11. Le misure di sicurezza. – Riferimenti bibliografici.

1. Introduzione

Il D.Lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali [1] (*G.U.* 29 luglio 2003, n. 174, di seguito "Codice"), anche sulla scia dei principi affermati nella c.d. Carta di Nizza, aveva codificato nell'ordinamento italiano il diritto alla protezione dei dati personali, di fatto già in precedenza disciplinato dalla L. 31 dicembre 1996, n. 675 [2].

[1] L'epigrafe per esteso, in esito alle modifiche introdotte dal D.Lgs. 8 agosto 2018, n. 101, è ora "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE".

[2] Detta L. 675/1996 fu adottata anche per attuare in Italia la direttiva 95/46/CE e numerosi altri

Recentemente, poi, è stato approvato il Regolamento (UE) 2016/279 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*» (Regolamento Generale sulla Protezione dei dati) [3], in esito al quale la Repubblica Italiana ha approvato il D.Lgs. 8 agosto 2018, n. 101, con il quale sono state introdotte le disposizioni nazionali per il completo adeguamento, al predetto Regolamento, del già menzionato D.Lgs. 196/2003.

In precedenza "diritto alla riservatezza" e "diritto alla privacy" venivano spesso utilizzati come sinonimi.

L'art. 1 del Codice, invece, ne aveva codificato la differenza, ora accennata solo dall'art. 1 del Regolamento UE che, oltre a richiamare il diritto alla protezione dei dati, precisa come la finalità propria della normativa europea sia anche quella di regolamentare la «*libera circolazione dei dati personali*» che, nell'Unione, «*non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*» (cfr. art. 1, par. 3, del Regolamento).

Il diritto alla riservatezza è stato ampiamente definito dalla giurisprudenza, consistendo nel diritto di ciascuno «*alla tutela di quelle situazioni personali o familiari svoltesi anche al di fuori del domicilio domestico che non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze non giustificate da interessi pubblici prevalenti, anche se lecite e tali da non offendere l'onore e il decoro. Questo diritto non può essere negato ad alcuna categoria di persone, solo in considerazione della loro notorietà, salvo che un reale interesse sociale all'informazione o altre esigenze pubbliche lo esigano*» [4].

Il diritto alla protezione dei dati personali, invece, consiste nel diritto di ciascuno di controllare la circolazione delle informazioni riguardanti la propria persona [5].

---

provvedimenti internazionali e sovranazionali, quali l'Accordo di Schengen (Ratificato dall'Italia con L. 30 settembre 1993, n. 388 che si proponeva di abbattere gradualmente le frontiere tra i Paesi aderenti, prevedendo che gli Stati firmatari fossero tutti collegati al «Sistema Informativo Schengen»), la Convenzione del Consiglio d'Europa n. 108/81, sulla protezione delle persone rispetto al trattamento automatizzato di dati personali, adottata a Strasburgo il 28 gennaio 1981 (ratificata dall'Italia con L. 21 febbraio 1989, n. 98 cui, tuttavia, non avrebbe potuto seguire la ratifica vera e propria ad opera del Capo dello Stato, causa la mancanza di una normativa interna sulla protezione dei dati) e le diverse Raccomandazioni del Consiglio d'Europa finalizzate a tutelare il diritto alla riservatezza e gli altri diritti della personalità rispetto ai trattamenti di dati personali.

[3] *G.U.C.E.* 4 maggio 2016, n. L119, quindi, in relazione all'art. 99 del Regolamento stesso, entrato in vigore il 24 maggio 2016, se pur con applicazione differita al 25 maggio 2018.

[4] Cass., 27 maggio 1975, n. 2129, in *Foro it.*, 1976, I, c. 2895.

[5] S. RODOTÀ, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir.*, dicembre 1991, in questo senso, già identificava il diritto alla riservatezza nel trinomio «persona –

2. L'ambito di applicazione

Nell'attuale contesto normativo il diritto alla protezione dei dati personali è normato esclusivamente dal Regolamento, mentre il Codice in materia di protezione dei dati personali, in esito alle modifiche apportate dal D.Lgs. 101/2018, reca semplicemente le disposizioni finalizzate ad adeguare il Regolamento all'ordinamento nazionale (cfr. art. 2 del Codice).

Diversamente da come avveniva in passato, sino al 2011, il Regolamento tutela esclusivamente le persone fisiche e non, invece, le persone giuridiche [6] (oltre che nella rubrica, infatti, l'art. 1, par. 1, del Regolamento, evidenzia che esso «*stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*»).

Sotto il profilo oggettivo, il Codice, che estende il suo ambito applicativo, oltre che ai trattamenti elettronici di dati, anche a quelli cartacei o manuali (art. 2, par. 1, Regolamento), si applica anche ai trattamenti di dati effettuati da chiunque abbia sede nel territorio dell'Unione Europea, indipendentemente dal luogo in cui avviene il trattamento [7]. Il Regolamento introduce un importante elemento di novità: esso si applica, infatti, anche ai trattamenti svolti all'estero da soggetti (titolari o responsabili) stabiliti all'estero, se quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi a interessati «*che si trovano*» nell'Unione europea [8] oppure il monitoraggio del comporta-

---

informazione – segretezza» e il diritto alla privacy nel quadrinomio «persona – informazione – circolazione – segretezza».

[6] Il testo originario della L. 675/1996 e, quindi, del D.Lgs. 196/2003, invece, tutelavano sia le persone fisiche sia le persone giuridiche, ponendosi peraltro all'avanguardia rispetto alle altre normative europee e comunitarie; ciò, tuttavia, solo sino al 2011 quando, con l'art. 40 del D.L. 6 dicembre 2011, n. 201 (convertito, con modificazioni, dalla L. 22 dicembre 2011, n. 214), è stato rimosso dall'impianto normativo ogni riferimento alla tutela, appunto, della persona giuridica. Il testo originale della norma, infatti, qualificava «*dato personale* […] *qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*» (cfr. con l'attuale art. 4, num. 1) che, invece, qualifica come dato personale «*qualunque informazione relativa a una persona fisica identificata o identificabile* »). Nella stessa direzione, inoltre, si è collocata la modifica normativa al concetto di "interessato" che, mentre in precedenza, era qualificabile come «*la persona fisica, la persona giuridica, l'ente o l'associazione, cui si riferiscono i dati personali*», ora è la sola «*persona fisica*».

[7] V. art. 3, par. 1, del Regolamento che sancisce l'applicabilità del Regolamento al trattamento di dati effettuato nell'ambito delle attività di uno stabilimento nell'Unione «indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione».

[8] Indipendentemente, quindi, dalla cittadinanza o dal titolo della permanenza nell'Unione, che potrebbe essere anche solo temporanea.

mento degli stessi interessati che avvenga all'interno dell'Unione europea.

In sostanza, e a parte le ipotesi specifiche escluse dall'applicazione di talune norme, il Regolamento esclude dalla sua applicazione il trattamento dei dati svolti in materie che non sono oggetto del diritto dell'Unione europea, svolti per finalità di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali (che sono invece oggetto di una normativa specifica) e da persone fisiche per l'esercizio di attività a carattere esclusivamente personale o domestico (art. 2, par. 2, del Regolamento).

3. I principi e le definizioni

Il complesso articolato legislativo può essere agevolmente compreso solo grazie all'art. 4 del Regolamento, finalizzato a raccogliere e definire la terminologia utilizzata dal legislatore.

La norma in analisi definisce preliminarmente il «*trattamento*» come «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*» (art 4, par. 1, n. b). In sostanza, qualsiasi operazione che abbia ad oggetto un dato personale può costituire trattamento e, quindi, qualsiasi attività venga svolta con uno o più dati personali rientra nell'applicazione della normativa in analisi.

Tra le operazioni del trattamento occorre altresì distinguere, per esaustività di trattazione, la «*comunicazione*» e la «*diffusione*». La prima consiste nel «*dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione*», mentre per diffusione il legislatore sottende «*il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*» (cfr. art. 2 *ter*, D.Lgs. 196/2003). Da un lato, quindi, con la comunicazione è possibile de-

terminare quali sono i soggetti che sono venuti a conoscenza del dato personale; con la diffusione, invece, non è possibile [9].

Come si è già avuto modo di accennare, laddove il Regolamento si riferisce al «*dato personale*», esso intende «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*» (art. 4, par. 1, n. 1, del Regolamento).

La definizione di dato personale è evidentemente molto ampia. La norma individua nel dato personale qualsiasi informazione che sia in grado di essere riferita ad una determinata persona fisica, anche se tale riferibilità derivi da elementi esterni al dato stesso, o da elementi di contorno che consentano, anche ad una ristretta cerchia di persone, di individuare il soggetto al quale l'informazione è riferibile [10].

4. I soggetti

Nell'ambito del trattamento dei dati personali intervengono, tra gli altri, diversi soggetti: il titolare, l'interessato, il responsabile e il soggetto autorizzato.

Il «*titolare*» del trattamento è definita dalla legge come «*la persona fisica o*

---

[9] Si pensi, ad esempio, al dato personale pubblicato su un quotidiano (diffusione) e al dato personale pubblicato in una Intranet (comunicazione).

[10] A fini dell'inquadramento del concetto di "identificabile" può farsi riferimento ai principi già espressi in più occasione dalla Corte di legittimità che, come noto, in materia di diffamazione ha già più volte evidenziato che «*ai fini dell'individuabilità dell'offeso non occorre che l'offensore ne indichi espressamente il nome, ma è sufficiente che l'offeso possa venire individuato per esclusione in via deduttiva, tra una categoria di persone, a nulla rilevando che in concreto l'offeso venga individuato da un ristretto gruppo di persone*» (cfr. Cass., 24 luglio 2012, n. 30369 che, a sua volta, richiama anche Cass., 17 gennaio 1978, n. 6507). Sul punto specifico, inoltre, si è espressa anche la Corte di Giustizia dell'Unione europea, che ha evidenziato come «*fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un «trattamento di dati personali [...] ai sensi dell'art. [...] della direttiva 95/46/CE*» (Corte di giustizia delle Comunità europee C-101/2001 del 6.11.2003, punto 27).

giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali» (art. 4, par. 1, n. 7, del Regolamento).

Alla luce della definizione normativa, il titolare del trattamento non è necessariamente una persona fisica, bensì un qualsiasi soggetto giuridico che svolge sui dati personali quelle operazioni che, sole o unitamente ad altre, costituiscono, appunto, il trattamento dei dati. In merito, già nella vigenza della precedente normativa, era anche intervenuto il Garante per la protezione dei dati personali il quale, alla luce delle difficoltà interpretative, aveva chiarito che nel caso di trattamento effettuato da una persona giuridica, da una Pubblica Amministrazione o, comunque, da una organizzazione o da un ente di ampie dimensioni, il titolare è l'entità nel suo complesso e non le persone fisiche che concorrono ad esprimerne la volontà [11]. E non v'è dubbio che tale interpretazione sia stata confermata dal Regolamento UE, soprattutto laddove individua il «*titolare*», appunto, anche nel «*servizio*» o «*altro organismo*».

Il medesimo principio deve ritenersi applicabile anche al concetto di «*responsabile*» del trattamento, che è «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*» (art. 4, comma 1, n. 8, ma anche art. 28 del Regolamento). Il titolare, pertanto, nel trattare i dati personali, ha la facoltà di preporvi uno o più responsabili, i quali dovranno poi procedere al trattamento rispettando le istruzioni impartite dal titolare (che, comunque, ha l'onere di verificare periodicamente) e di vigilare sull'osservanza di tali istruzioni e, in genere, sul suo operato (cfr. art. 28, par. 3) [12].

Il Regolamento prevede poi che chiunque agisca sotto l'autorità del titolare e/o del responsabile deve essere «*istruito in tal senso*» (art. 29, Regolamento). La norma, senza dubbio finalizzata ad identificare il soggetto che materialmente compie le operazioni del trattamento e che, evidentemente, può essere soltanto una persona fisica, è stata in effetti completata dall'art. 2 *quaterdecies* del D.Lgs. 196/2003 che prevede espressamente come il titolare e/o il responsabile debbano prevede «*nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano*

[11] Garante, 9 dicembre 1997, in *Bollettino*, 2, pp. 44 e 46.

[12] Si badi che, ai sensi dell'art. 28 del Regolamento, il trattamento demandato ad un responsabile deve essere disciplinato «*da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri*».

attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità».

La figura del c.d. "soggetto autorizzato" e/o "soggetto designato", che dir si voglia, è quindi la figura della persona fisica che il titolare o il responsabile individuano, all'interno della loro organizzazione, per il trattamento dei dati, il quale deve essere preposto ad uno specifico ambito del trattamento e deve essere senza dubbio istruito e formato sulle modalità per lo svolgimento della sua attività. È infatti vero che, nell'esercitare le sue funzioni, tale soggetto deve attenersi alle istruzioni impartite, e deve operare sotto la diretta autorità del delegante.

Contrapposto alle figure del titolare, del responsabile e del soggetto autorizzato si trova l'interessato che è la persona fisica alla quale si riferiscono i dati personali che, come si è già visto, può essere «*identificata o identificabile*» (art. 4, comma 1, lett. a) [13].

L'art. 37 del Regolamento UE prevede una ulteriore figura, quella del «*responsabile della protezione dei dati*», generalmente chiamato *Data Privacy Officer* (DPO), la cui designazione è imposta dalla normativa europea nel caso in cui il trattamento sia effettuato da una pubblica amministrazione, dai titolari e/o dai responsabili i cui trattamenti richiedano un monitoraggio «*regolare e sistematico degli interessati su larga scala*» nonché dai titolari e/o responsabili che procedano al trattamento «*su larga scala*» dei dati sensibili (compresi i dati genetici e biometrici) e dei dati giudiziari.

La finalità dell'imposizione della nomina di un DPO, che deve avere una posizione di indipendenza rispetto al titolare, è quella di inserire nell'organizzazione di quest'ultimo un soggetto che gli fornisca consulenza in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, che sorvegli l'osservanza di tale normativa, ivi compresa la «*sensibilizzazione e la formazione del personale*», di fornire un parere sulla valutazione d'impatto sulla protezione dei dati, di cooperare, e fungere da punto di contatto, con il Garante per la protezione dei dati personali.

---

[13] In proposito occorre rimarcare che, diversamente dal passato, in esito alle modifiche apportate al Codice dalla legislazione d'urgenza del 2011, la normativa, ora, tutela esclusivamente le persone fisiche e non più le persone giuridiche, gli enti e gli organismi collettivi così come, in precedenza, il testo originario del Codice in materia di protezione dei dati personali.

5. Il trattamento dei dati personali e le condizioni di legittimità

5.1. Le modalità del trattamento dei dati personali

L'art. 5 del Regolamento disciplina il principio di «liceità, correttezza e trasparenza» che, unitamente al principio di «limitazione della finalità», di «minimizzazione dei dati» e di «limitazione della conservazione», plasmano l'intera normativa in materia di protezione dei dati personali.

Tali connotati sono finalizzati a consentire il trattamento dei dati solo qualora sia necessario per adempiere alle finalità per le quali i dati erano stati raccolti, nei limiti dei dati all'uopo necessari e delle operazioni strettamente indispensabili per gli scopi medesimi, il tutto rispettando quella «correttezza» che deve plasmare il comportamento di colui che tratta i dati, e che funge da principio di chiusura, così come il generale principio codicistico della buona fede.

La «*correttezza*» impone il rispetto di tutte le regole, anche non codificate, che devono porsi quale presupposto del trattamento medesimo e, nell'ambito del Regolamento UE, si affianca alla «*trasparenza*» che, tuttavia, altro non è che il principio che impone a chiunque di rendere ostensibile il trattamento dei dati al suo interessato.

Ai fini di cui sopra l'art. 5 del Regolamento, che è considerata una norma cardine del trattamento dei dati personali, determina le modalità della raccolta e del successivo trattamento dei dati, così come i requisiti dei dati personali oggetto di trattamento.

L'art. 5 regola i diversi momenti del trattamento e, in particolare, quelli relativi alla raccolta dei dati, ai requisiti dei dati, alle modalità di elaborazione e di conservazione [14], ed è completata da una norma interna che prevede espressamente che «[i] *dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*» (art. 2 *decies* del Codice).

Alla luce di tale norma, la liceità del trattamento deve essere valutata attraverso l'analisi di tutte le norme dell'ordinamento giuridico, non solo di quelle in materia di protezione dei dati personali (cfr., a titolo esemplificativo, gli artt. 615 *bis*, 614, 616 c.p.) anche se, da più parti, si evidenzia come la valutazione del rispetto del principio di «*liceità*» deve essere fatta tenendo in considerazione, preliminarmente, la sussistenza di una delle «*basi giuridiche*» previste dagli artt. 6, 9 e 10 del Regolamento.

---

[14] M. LOSANO, *Commento all'art. 9*, in E. GIANNANTONIO-M. LOSANO-V. ZENO-ZENCOVICH, *Trattamento dei dati e tutela della persona*, Giuffrè, Milano, 1998.

I dati oggetto del trattamento devono essere «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*». La norma distingue la raccolta dal successivo trattamento, dato che, in realtà, la raccolta potrebbe non essere successivamente seguita da ulteriori operazioni del trattamento. Il punto è che il titolare che procede ad un trattamento di dati, per valutarne la legittimità, deve sempre tenere in considerazione le finalità per i quali i dati erano stati in precedenza raccolti, e li deve trattare conformemente agli scopi originari, fatto salvo l'eventuale trattamento «a *fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*» che il Regolamento considera comunque compatibile con gli scopi originari (cfr. art. 5, par. 1, lett. a), del Regolamento).

Il trattamento deve quindi essere effettuato solo per scopi determinati ed espliciti, ossia per finalità comunicate chiaramente agli interessati, affinché questi ultimi siano posti in grado di conoscere le specifiche finalità, chiare ed univoche, per cui il titolare ha proceduto al trattamento.

Il trattamento deve inoltre essere effettuato per scopi legittimi, trattandosi quindi di un rinvio ai principi generali dell'ordinamento del rispetto della normativa, dell'ordine pubblico e del buon costume.

Secondo l'art. 5, par. 1, lett. d), i dati trattati devono essere «*esatti e, se necessario, aggiornati*» nonché «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*». Tali requisiti devono essere garantiti anche al fine di perseguire il diritto all'identità personale dell'interessato che, evidentemente, verrebbe inutilmente leso nel caso di trattamento di dati errati, incompleti, eccedenti le finalità della raccolta [15].

Agli stessi fini, e comunque per la più completa garanzia del diritto alla protezione dei dati personali, questi ultimi non devono essere eccedenti rispetto alle finalità per cui sono stati raccolti o successivamente trattati e «*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*».

Questa rappresenta un'altra clausola di compatibilità atta a determinare il principio secondo il quale nel momento in cui lo scopo per cui i dati sono stati raccolti o trattati è stato raggiunto, i medesimi devono essere resi anonimi o, comunque, cancellati, e ciò, salvo che il trattamento successivo non concerna il trattamento dei dati «*a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici*», nel quale caso possono essere trattati anche per i dati personali possono essere conservati «per periodi più lunghi». In sostanza la normativa eurounitaria prevede espressamente che le finalità archi-

[15] G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Giuffrè, Milano, 1997.

vistiche, storiche e di ricerca, se perseguite nel rispetto delle altre disposizioni del Regolamento e del Codice, non sono mai considerate incompatibili con gli scopi originari del trattamento.

5.2. Il principio di «responsabilizzazione» e il Registro delle attività di trattamento

V'è da precisare che il Regolamento UE non prevede l'istituzione di alcuna banca dati pubblica che raccolga l'elenco dei trattamenti di dati personali, e ciò anche in virtù del principio di «responsabilizzazione» che, codificato dall'art. 24, impone al titolare del trattamento di mettere in atto «*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento*».

Il punto è che, diversamente dalla normativa precedente, il Regolamento UE è strutturato sulla base dell'attribuzione di una vera e propria responsabilità nei confronti del titolare, che non è (più) soggetto a specifici obblighi e analitiche misure di sicurezza, ma è consegnatario del rispetto del diritto alla protezione dei dati personali dell'interessato, e deve dimostrare di aver adottato tutte le misure necessarie finalizzate a garantire la conformità del trattamento alle previsioni normative.

In sostanza il Regolamento attribuisce ai titolari il compito di determinare autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, fermo restando che i titolari medesimi devono comunque essere in grado di dimostrare tali modalità, garanzie e limiti, soprattutto laddove vi sia un controllo dell'autorità competente e/o laddove vi sia stata una violazione dei dati.

Uno degli adempimenti imposti al titolare (e, sotto certi profili, anche al responsabile) per fornire tale dimostrazione, è anche l'istituzione di un Registro delle attività di trattamento (art. 30 del Regolamento), che è senza dubbio uno strumento indispensabile per disporre di un quadro aggiornato dei trattamenti svolti presso il titolare, anche per valutare e analizzare il rischio insito nel trattamento stesso

Il Registro delle Attività di Trattamento può essere conservato in formato elettronico e deve contenere i seguenti requisiti:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) gli eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, nel caso, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

Il Registro dei trattamenti deve essere istituito e tenuto solo dai titolari che abbiano alle proprie dipendenze oltre 250 dipendenti oppure dai titolari che, pur avendo meno dipendenti, procedono al trattamento che possa presentare un rischio per i diritti e le libertà dell'interessato, che non sia occasionale o che includa dati di natura particolare.

5.3. L'informativa

Prima della raccolta dei dati personali il titolare o il responsabile (o, per essi, il soggetto designato al trattamento), devono fornire all'interessato (anzi, dapprima alla persona che fornisce i dati) la c.d. *informativa* finalizzata, da un lato, a garantirgli la conoscenza della tipologia di trattamento cui i propri dati sono destinati e, dall'altro, a consentirgli di esprimere un consenso effettivamente informato. In realtà, ad un'attenta lettura dell'art. 13, par. 1, del Regolamento, l'informativa deve essere resa una volta «ottenuti» i dati personali per cui, evidentemente, può (ora) considerarsi legittima la prassi di fornire l'informativa stessa al momento stesso della raccolta e/o immediatamente dopo [16].

L'informativa, disciplinata dagli artt. 13 e 14 del Regolamento UE, può essere fornita per iscritto, oralmente o con «altri mezzi» anche se, con l'entrata in vigore del Regolamento, può essere fornita oralmente soltanto se richiesto dall'interessato (cfr. art. 12, par. 1, del Regolamento). L'informativa deve contene-

[16] A mero titolo esemplificativo si consideri la prassi commerciale di registrare i dati, procedendo successivamente alla registrazione alla stampa della modulistica contrattuale, contenente l'informativa, che viene sottoposta alla firma del cliente pochi minuti dopo che lo stesso ha fornito i dati.

re le informazioni necessarie ad identificare il trattamento e deve essere fornita in forma concisa, trasparente, intellegibile, con un linguaggio semplice e chiaro.

La persona che fornisce i dati deve quindi essere resa edotta delle finalità, delle modalità, della «*base giuridica*» del trattamento stesso [17], della durata del trattamento e, soprattutto deve essere avvertita della natura (facoltativa o obbligatoria) del conferimento dei dati (art. 13, par. 2, lett. e, del Regolamento).

Nell'ottica di ottenere, poi, il consenso informato, l'interessato deve anche avere la possibilità di sapere quali sono le conseguenze nel caso rifiuti il conferimento dei dati (art. 13, par. 2, lett. e, del Regolamento). La finalità della norma è quella di porre l'individuo nella condizione di optare per la soluzione migliore e, pertanto, di bilanciare i diversi interessi in questione. Lo stesso interessato, allo stesso fine, deve essere informato dei soggetti (o categorie di soggetti) ai quali i dati possono essere comunicati nonché l'eventuale trasferimento all'estero dei dati medesimi (art. 13, par. 1, lett. e, lett. f, del Regolamento).

L'informativa deve contenere il riferimento alla possibilità di esercitare alcuni dei diritti previsti dal Regolamento (accesso, rettifica, cancellazione, portabilità, limitazione, opposizione), della possibilità di revocare il consenso nonché della possibilità di proporre reclamo all'autorità di controllo, così come deve contenere nonché dei dati identificativi (e di «*contatto*») del titolare e dell'eventuale Responsabile della Protezione dei Dati.

In molte circostanze i dati vengano raccolti presso soggetti diversi dall'interessato. In tali casi, non potendosi fornire l'informativa all'interessato stesso, quantomeno non prima della raccolta, l'art. 14 del Regolamento impone di fornirla, in prima battuta, alla persona che fornisce i dati e, successivamente, «*entro un mese dall'ottenimento dei dati*» o «*al momento della prima comunicazione all'interessato*», all'interessato stesso (c.d. informativa *postuma*).

Da un lato, al fine di semplificare l'attività del titolare, l'art. 14, par. 5, lett. a, del Regolamento che l'informativa postuma può non essere fornita laddove l'interessato sia già a conoscenza delle informazioni che dovrebbero essergli date, dall'altro, nel caso di dati raccolti presso terzi, l'informativa all'interessato non è obbligatoria qualora (i) l'ottenimento e la comunicazione dei dati sia prevista da un obbligo normativo, (ii) qualora i dati debbano rimanere riservati conformemente a un obbligo di segreto legale o professionale oppure (iii) quando tale obbligo risulti impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato (la norma fa espresso riferimento al

[17] Il Regolamento UE prevede anche la necessità di informare l'interessato di qual è il «*legittimo interesse*» del titolare che consente di procedere al trattamento anche senza il consenso dell'interessato stesso.

caso dell'archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici), oppure nella misura in cui l'obbligo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità del trattamento.

All'evidente scopo di agevolare i contatti tra lavoratori e datori di lavoro, inoltre, l'art. 111 *bis* del Codice prevede espressamente che l'informativa «*nei casi di ricezione dei curricula spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del curriculum medesimo*» con la conseguenza che l'informativa postuma potrebbe anche non essere resa, soprattutto nei casi in cui, appunto, non vi sia un successivo «*primo contatto utile*".

5.4. La liceità del trattamento: le c.d. basi giuridiche

L'art. 6 del Regolamento prevede che il trattamento dei dati è lecito solo se viene svolto in presenza di una c.d. base giuridica, ovvero di una condizione legittimante il trattamento stesso.

La prima base giuridica che consente il trattamento è, senza dubbio, il consenso dell'interessato. Il trattamento è infatti considerato lecito se prestato liberamente e, se prestato nel contesto di una dichiarazione scritta che riguarda altre questioni «*la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro*».

Il consenso può quindi riguardare l'intero trattamento oppure una o più operazioni del medesimo ed è valido solo se è espresso liberamente. Il Regolamento UE pone particolare attenzione al principio di libertà del consenso, tanto che si è spinto sino a "codificare" alcuni principi manifestati in precedenza da diverse autorità di controllo europee, dato che precisa come per valutare l'effettiva libertà deve tenersi «*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*».

La «*libertà*» del consenso richiesta dalla norma in analisi, in sostanza, esclude che la volontà dell'interessato possa essere viziata, ovvero manifestata in presenza di errore, violenza, dolo o incapacità naturale di intendere e di volere, anche solo temporanea [18], con precisazione che l'art. 8, par. 1, del Regolamento

[18] Il Garante ha precisato che «*il consenso può essere ritenuto effettivamente libero solo se si presenta come manifestazione del diritto all'autodeterminazione informativa, e dunque al riparo*

UE "abbassa" l'età alla quale può essere prestato il consenso al trattamento dei dati nel contesto dei servizi della società dell'informazione a 16 anni, con facoltà degli Stati di stabilire un'età inferiore, fino a 13 anni (tant'è vero che l'Italia ha abbassato il limite a 14 anni con l'art. 2-*quinques* del Codice).

Laddove la condizione di liceità del trattamento sia il consenso, lo stesso deve essere prestato prima dell'inizio del trattamento e comunque dopo aver avuto conoscenza dell'informativa e, comunque, può liberamente essere revocato fermo restando, in tal caso, la legittimità del trattamento svolto prima della revoca.

La precedente normativa italiana prevedeva espressamente che il consenso dovesse essere "espresso", inciso non riprodotto nella formulazione regolamentare. In realtà si ritiene che detto requisito permanga, dato che la formulazione complessiva dell'art. 8 del Regolamento pare escludere, di fatti, che il consenso possa "presumersi" anche solo da un comportamento concludente da parte dell'interessato.

Sull'istituto del consenso vige in linea di principio il principio della libertà delle forme, fermo restando che ai sensi dell'art. 8, par. 1, del Regolamento prevede espressamente che «*il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali*».

Il medesimo art. 6, ai fini del corretto bilanciamento degli interessi sottesi alle esigenze dei diversi soggetti che si contrappongono nell'ambito del trattamento di dati (in linea di principio titolare e interessato), prevede poi ulteriori ipotesi di liceità, che sono sottratte al principio del consenso.

Si tratta, in particolare, del caso in cui il trattamento riguarda dati raccolti e detenuti in base ad obblighi legali, del caso in cui il trattamento sia necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato e del caso in cui riguardi dati contenuti nei curricula spontaneamente inviati dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro [19].

Gli altri casi di esclusione dell'obbligo del consenso sono quelli relativi trattamenti effettuati per perseguire un diritto costituzionale considerato prevalente sul diritto alla protezione dei dati, quale il perseguimento di un interesse vitale dell'interessato o di un terzo nonché l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

---

da qualsiasi pressione, e se non viene condizionato all'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto» (Garante, 28 maggio 1997, in *Bollettino*, 1, p. 17).

[19] V. sul punto, l'art. 111 *bis* del Codice, che esclude l'obbligo del consenso nel caso dei curricula.

L'ultima, ma non per importanza, condizione di liceità del trattamento, peraltro elemento di grande novità, è il perseguimento di un «*legittimo interesse del titolare del trattamento o di terzi*» sul quale la dottrina, dato l'elemento di grande novità introdotto anche nell'ordinamento giuridico italiano, è intervenuta diffusamente.

Affinché il «*legittimo interesse*» possa costituire idonea base giuridica del trattamento è essenziale che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto in particolare conto le ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare.

Secondo il considerando n. 47 del Regolamento, potrebbero sussistere il «*legittimo interesse*» quando esiste una relazione pertinente e appropriata tra l'interessato e il titolare del trattamento, ad esempio nel caso in cui l'interessato sia un cliente o alle dipendenze del titolare del trattamento (un esempio di «*legittimo interesse*» in realtà previsto per legge è l'art. 130, comma 3 *bis*, del Codice che, come noto, consente l'invio di comunicazioni commerciali a coloro che, ineriti negli elenchi telefonici, non abbiano chiesto l'iscrizione nel registro delle opposizioni o, addirittura, il medesimo art. 130, comma 4, laddove consente l'invio di comunicazioni elettroniche con finalità di marketing ai clienti che, all'atto della conclusione dell'originario contratto, non si siano opposti al relativo trattamento, se pur solo con riferimento a prodotti e servizi "analoghi").

In ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero prevalere sugli interessi del titolare qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali.

5.5. Il trattamento dei dati particolari

Gli artt. 9 e 10 del Regolamento UE, sulla base della particolare pericolosità dell'uso indiscriminato di determinate informazioni, ha disciplinato *ad hoc* i dati «*particolari*» che, a loro volta, si distinguono in due categorie che, in questa sede, possiamo definire dati sensibili (disciplinati dall'art. 9 del Regolamento) e dati giudiziari (disciplinati dall'art. 10 del Regolamento) [20].

[20] In realtà la ripartizione tra dati sensibili e dati giudiziari deriva dalla precedente normativa nazionale che, appunto, all'art. 4 lett. d) ed e), D.Lgs. 196/2003 definiva separatamente le due ti-

L'art. 9, in particolare, vieta, se pur in linea di principio, il trattamento dei 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*».

A fronte di questo generale divieto, la stessa norma prevede poi delle deroghe (che, in realtà ricalcano quasi le basi giuridiche previste per il trattamento dei dati comuni dall'art. 6 del Regolamento). I dati sensibili possono infatti essere trattati se «*l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche*», con la precisazione che gli Stati membri dell'UE possono prevedere limitazioni al principio del libero consenso come, appunto, ha fatto l'Italia.

L'art. 2 *septies* del Codice, sul punto, non esclude la possibilità di acconsentire al trattamento di taluni dati particolari (la norma, infatti, pone una deroga al solo trattamento di dati genetici, biometrici e sanitari), ma prevede che il consenso dell'interessato legittima il trattamento purché quest'ultimo avvenga «*in conformità alle misure di garanzia disposte dal Garante*» le quali "possono individuare […] ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito".

Come è possibile constatare dalla lettura delle due norme, quella eurounitaria e quella italiana, i due legislatori partono dal presupposto che il trattamento dei dati particolari possa essere particolarmente lesivo dei diritti e delle libertà fondamentali, in quanto potenzialmente discriminatorio. Per tale ragione, a fronte del fondamentale divieto di trattamento, l'eventuale consenso dell'interessato viene circondato dal rispetto di un provvedimento sostanzialmente autorizzatorio dall'autorità Garante alla quale, evidentemente, il legislatore attribuisce i potere di verificare *ex ante* se, per uno o più specifici trattamenti, possono ritenersi prevalenti altri interessi costituzionalmente rilevanti per i quali l'interessato possa acconsentire.

In realtà, come si è visto, l'art. 9 consente il trattamento anche in presenza di

---

pologie di informazioni. La distinzione parrebbe scomparsa con l'efficacia del Regolamento UE ma, in realtà, proprio alla luce della distinzione che svolgono gli artt. 9 e 10 del predetto Regolamento può essere ancora utilizzata, quantomeno nel linguaggio comune e/o dottrinale, e ciò anche considerando che l'art. 22, comma 2, del D.Lgs. 101/2018 prevede espressamente che «[a] *decorrere dal 25 maggio 2018 le espressioni «dati sensibili» e «dati giudiziari» utilizzate ai sensi dell'articolo 4, comma 1, lettere d) ed e), del codice in materia di protezione dei dati personali, di cui al decreto legislativo n. 196 del 2003, ovunque ricorrano, si intendono riferite, rispettivamente, alle categorie particolari di dati di cui all'articolo 9 del Regolamento (UE) 2016/679 e ai dati di cui all'articolo 10 del medesimo regolamento».*

altre condizioni legittimanti, che prescindono dal consenso dell'interessato e che, evidentemente, sono finalizzate a bilanciare i vari interessi coinvolti.

In sostanza la norma deroga al divieto di trattamento dei dati sensibili quando «*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*» nonché «*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*». In tali casi, evidentemente, il legislatore sovranazionale ha considerato prevalente, rispetto al consenso dell'interessato, l'esigenza di procedere al trattamento per finalità legate alla gestione del rapporto di lavoro e per tutelare la salute dei terzi che, si badi, è considerato prevalente, a giudizio di chi scrive, anche dall'art. 32 della Costituzione italiana.

L'art. 9 disciplina poi altri casi in cui il titolare di trattamento dei dati sensibili può procedere al trattamento senza il consenso dell'interessato. Si riferisce (i) 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, (ii) al trattamento necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali, (iii) al trattamento 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, (iv) al trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

L'art. 9 del Regolamento UE consente poi il trattamento dei dati sensibili nel caso in cui gli stessi siano stati resi manifestamente pubblici dall'interessato perché, in tale eventualità, evidentemente, non v'è alcun interesse alla loro secretazione.

Per quanto invece concerne i dati giudiziari, ovvero quelle informazioni relativi alle condanne penali e ai reati o a connesse misure di sicurezza, la disciplina regolamentare, di fatto, fa rinvio alle basi giuridiche previste dall'art. 6, par. 1, ma lo subordina al «*controllo dell'autorità pubblica*» o lo consente, al di fuori di tale controllo, solo se «*autorizzato dal diritto dell'Unione o degli Stati membri*».

Su tale particolare tipologia di dati, peraltro, l'art. 2-*octies* del Codice pre-

vede che, al di fuori delle ipotesi dei trattamenti di dati giudiziari svolti dall'autorità pubblica, gli stessi sono consentiti solo se autorizzati «*da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati*» ovvero, in mancanza, da un apposito provvedimento autorizzatorio del Ministro della Giustizia (cfr. art. 2-*octies*, comma 2, del Codice).

5.6. Il trattamento dei dati per finalità giornalistiche

Nella normativa italiana la «diffusione» dei dati personali è una specifica operazione del trattamento consistente nel rendere noti i dati personali a persone indeterminate ed indeterminabili e, come tale, si distingue dalla «*comunicazione*» (cfr. art. 2 *ter*, comma 4, del Codice).

Il giornalismo è quindi un settore di attività nell'ambito del quale si trattano una moltitudine di dati personali, anche particolari, che vengono principalmente sottoposti a diffusione, essendo pubblicati in ambito locale, nazionale (es., sui quotidiani) o, addirittura, internazionale (es., Internet).

La rilevanza costituzionale, da un lato, della libertà di stampa, di pensiero, di critica (art. 21 Cost.) e, dall'altro, del diritto alla protezione dei dati personali, alla riservatezza e all'identità personale, comportano la necessità di bilanciare con particolare rigore ed attenzione i diritti stessi, valutando caso per caso quale deve prevalere.

Sul punto il Regolamento UE lascia la competenza alla normativa degli Stati membri i quali hanno la possibilità di derogare gran parte delle norme dell'Unione sui principi generali, fermo restando l'obbligo di notificare alla Commissione le disposizioni adottate.

A ciò ha provveduto l'art. 137 del Codice che, in nome della libertà di manifestazione del pensiero, esclude l'obbligo del consenso per i trattamenti effettuati nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità, purché il trattamento venga svolto nel rispetto dei limiti del diritto di cronaca posti a tutela della riservatezza, così riprendendo e codificando i principi espressi dalla Corte Suprema di Cassazione, riassumibili nel concetto di essenzialità dell'informazione riguardo a fatti di interesse pubblico [21].

[21] I principi espressi dalla giurisprudenza di legittimità sono rappresentati (i) dall'utilità o interesse sociale a fruire delle informazioni oggetto di cronaca, (ii) dalla verità dei fatti esposti, (iii) dalla continenza, intesa quale obbligo per il giornalista di utilizzare una forma civile nell'esposizione dei fatti e nella loro valutazione (cfr. fra le altre, Cass., 22 giugno 1995, n. 982).

Al fine di meglio contemperare il principio costituzionale della libertà di informazione con il diritto alla protezione dei dati, l'art. 137 del Codice impone poi che il trattamento avvenga nel rispetto delle regole deontologiche relative al trattamento dei dati nell'ambito dell'attività giornalistica che devono essere approvate dal Consiglio nazionale dell'Ordine dei giornalisti, di fatto, nel rispetto di eventuali indicazioni del Garante [22].

Le regole deontologiche richieste dall'art. 137 del Codice, in particolare, sono state effettivamente approvate dal Consiglio dell'Ordine [23] e hanno individuato specifiche misure e accorgimenti a garanzia degli interessati, peraltro rapportate alla natura dei dati.

L'art. 2 *quater* del D.Lgs. 196/2003 prevede infatti che Il rispetto delle disposizioni contenute nelle regole deontologiche costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali, con ciò attribuendo alle stesse un vero e proprio rango secondario, alla cui inosservanza possono essere ricollegate le sanzioni civili, penali ed amministrative previste dalla normativa in analisi [24].

5.7. Il trasferimento dei dati all'estero

Il «trasferimento all'estero» dei dati personali consiste nello spostamento dei dati dal territorio nazionale a quello di Paesi stranieri (intendendosi come tali i paesi terzi, non appartenenti all'UE e/o allo Spazio Economico Europeo o organizzazioni internazionali).

Sul punto, preliminarmente, l'art. 1, par. 3, del Regolamento UE prevede che «*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*». In sostanza la circolazione dei dati

---

[22] L'art. 139, comma 5, del Codice prevede infatti che «[i]*l Garante, in cooperazione con il Consiglio nazionale dell'ordine dei giornalisti, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire*».

[23] In realtà erano già state approvate nella vigenza del testo originario del d.lgs. 196/03 nella forma del «*Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica*» e sono poi state «tramutate» nelle odierne «Regole deontologiche», in forza dell'art. 20 del D.Lgs. 101/2018 e del provvedimento del Garante del 29 novembre 2018.

[24] Ma, sul punto, e sul concetto di codificazione delle norme deontologiche si veda più ampiamente F. BRAVO, *Le condizioni di liceità del trattamento dei dati*, in J. MONDUCCI-G. SARTOR (a cura di), *Il Codice in materia di protezione dei dati personali*, Cedam, Padova, 2004, nonché J. MONDUCCI, *Diritti della persona e trattamento dei dati particolari*, Giuffrè, Milano, 2003.

tra i Paesi dell'Unione può avvenire alle stesse condizioni in virtù delle quali la circolazione avviene all'interno di ciascuno stato. È quindi evidente la finalità di perseguire i principi fondamentali del diritto dell'Unione Europea, come noto finalizzato al perseguimento della libera circolazione di persone, beni e servizi.

Al fine di evitare che il trasferimento dei dati venga attuato al fine di eludere la normativa eurounitaria, gli artt. dal 45 al 49 del Regolamento prevedono che il trasferimento dei dati al di fuori dell'Unione possa avvenire, nel rispetto delle altre norme previste dal Regolamento, solo laddove, alternativamente (1) vi sia stata una decisione di adeguatezza da parte della Commissione Europea, (2) il trasferimento sia soggetto a particolari garanzie, (3) il trasferimento sia effettuato nell'ambito delle norme vincolanti d'impresa, (4) il trasferimento sia disposto da un provvedimento dell'autorità giurisdizionale in presenza di un accordo internazionale tra il paese terzo e l'Unione Europea o il singolo Stato dell'Unione e, in ultimo, (5) in presenza delle specifiche deroghe previste dall'art. 49 del Regolamento.

Il presupposto fondamentale sotteso all'art. 45 è che il trasferimento al di fuori del territorio UE è di base vietato qualora la legislazione del Paese di destinazione non assicuri un livello di tutela adeguato. La norma, tuttavia, attribuisce alla Commissione Europea il potere di «decidere» che il Paese o l'organizzazione internazionale di destinazione garantiscono un livello di protezione adeguato e, nel caso, il trasferimento potrà avvenire senza autorizzazione, così come può avvenire tra gli Stati dell'Unione.

In mancanza di tale decisione di adeguatezza, il trasferimento all'estero potrà avvenire solo in presenza delle garanzie adeguate perviste dagli artt. 46 e 47 del Regolamento (tra le tante si evidenzia come costituiscano garanzia adeguata la stipulazione tra le parti del flusso dei dati di particolari clausole contrattuali approvate dalla Commissione Europea) oppure in presenza di una delle condizioni previste dall'art. 49 che, tra la altre condizioni, consente il trasferimento in presenza dello specifico consenso dell'interessato che, tuttavia, deve essere stato «*informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate*».

6. I diritti dell'interessato

Il Capo III del Regolamento, al fine di garantire a pieno il diritto alla protezione dei dati personali (inteso, in particolare, quale potestà di controllo da parte dell'interessato), disciplina specifici diritti, che possono essere esercitati dal-

l'interessato [25] o, in caso di suo decesso, da chiunque vi abbia interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione (cfr. 2 *terdecies* del Codice).

Ai sensi dell'art. 15 del Regolamento l'interessato ha diritto di ottenere la conferma dell'esistenza di un trattamento di dati che lo riguardano, ha diritto di accedere «ai dati» e ha diritto di accedere alle informazioni concernenti le finalità del trattamento, le categorie di dati personali trattati, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, il periodo di conservazione dei dati personali previsto o i criteri utilizzati per determinarlo, l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, il diritto di proporre reclamo all'autorità di controllo, l'origine dei dati [26] e l'esistenza di un processo decisionale automatizzato.

La norma appena analizzata conferisce quindi all'interessato il diritto di ottenere «*copia*» dei dati personali, così che, in realtà, è assolutamente conforme alla disposizione precedentemente contenuta nell'art. 7 del Codice la cui formulazione letterale consentiva all'interessato di ottenere la comunicazione «*in forma intellegibile*» dei dati personali.

In aggiunta al generale «diritto di accesso» ai dati personali, la normativa regolamentare europea aggiunge un'ulteriore serie di diritti che gli consentono di intervenire sul dato trattato che lo riguarda: il «diritto di rettifica» e il «diritto all'oblìo» (che, in precedenza, era conosciuto come «diritto alla cancellazione»).

Il primo di questi diritti di "intervento" sui dati, in particolare, attribuisce il diritto di ottenere dal titolare la «*rettifica*» dei dati inesatti e, «*tenuto conto delle finalità del trattamento*», la «*integrazione degli stessi*» (art. 16 del Regolamento). In ordine alla «*integrazione*» v'è da dire che la norma chiarisce molto il suo ambito di efficacia rispetto a quella precedente [27], dato che evidenzia come la valutazione dell'interesse in presenza del quale l'interessato può "aggiungere" informazioni ai dati trattati deve essere fatta tenendo in considerazione le finalità del trattamento, così che vi sarà interesse solo nel caso in cui l'integrazione

[25] L'interessato, per l'esercizio dei suoi diritti, può delegare persone fisiche o associazioni, conferendo delega scritta. Per ovvie ragioni, qualora l'interessato sia una persona giuridica, l'istanza deve essere avanzata dalla persona fisica a ciò legittimata in base ai rispettivi ordinamenti o statuti.

[26] L'art. 138 fa comunque salve le norme sul segreto professionale dei giornalisti, non essendo questi ultimi tenuti a comunicare la fonte dei dati trattati.

[27] Il previgente art. 7 del Codice attribuiva all'interessato il diritto di chiedere l'integrazione dei dati qualora aveva «interesse».

dell'informazione sia necessaria per il miglior perseguimento degli scopi per i quali i dati sono, appunto, oggetto di trattamento da parte del titolare.

L'interessato, dopo aver avuto notizia, o avendo già notizia, del trattamento, può inoltre domandare al titolare o al responsabile la cancellazione (alla quale è senza dubbio equiparata la previgente «trasformazione in forma anonima»), ma solo in alcune ipotesi tipiche, ovverosia nel caso in cui i dati non siano più necessari rispetto alle finalità, l'interessato abbia revocato il consenso su cui si basa il trattamento o si sia opposto al trattamento automatizzato o per finalità di marketing, i dati personali sono stati trattati illecitamente, gli stessi debbano essere cancellati per adempiere un obbligo legale o gli stessi siano stati raccolti relativamente all'offerta di servizi della società dell'informazione.

Sul diritto alla cancellazione giova evidenziare come la normativa si sia allineata a quanto previsto dalla sentenza «Google Spain»[28], tanto che consente all'interessato il diritto di ottenere la cancellazione di «*qualsiasi link, copia o riproduzione dei suoi dati personali*». Sul punto giova tuttavia osservare come il diritto alla cancellazione soffra dei limiti, determinati dalla necessità di bilanciare il diritto alla protezione dei dati con altri diritti (per la gran parte costituzionalmente rilevanti) del titolare o di terzi, dato che non può essere esercitato laddove il trattamento è svolto nell'ambito dell'esercizio del diritto alla libertà di espressione e di informazione, per l'adempimento di un obbligo legale, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

L'art. 18 del Regolamento attribuisce poi all'interessato il diritto di chiedere la «*limitazione*» del trattamento che consiste nel «*contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*» (cfr. art. 4, par. 1, n. 3, del Regolamento) che, di fatto, comporta la conseguenza che i dati possono essere oggetto solo di conservazione, con impossibilità di svolgere qualunque altra operazione, salvo che non sia necessaria per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante (cfr. art. 18, par. 2, del Regolamento).

---

[28] CGUE, 13 maggio 2014 nella causa C-131/12 che ha nella sostanza, riconosciuto il c.d. diritto all'oblìo, in virtù del quale, nel caso in cui, a seguito di una ricerca effettuata a partire dal nome di una persona, l'elenco di risultati mostra un link verso una pagina web che contiene informazioni sulla persona in questione, questa può rivolgersi direttamente al gestore oppure, qualora questi non dia seguito alla sua domanda, adire le autorità competenti per ottenere, in presenza di determinate condizioni, la soppressione di tale link dall'elenco di risultati (*http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT*).

La limitazione, che, di fatto, deve avere una durata temporanea, può essere chiesta laddove l'interessato contesta l'esattezza dei dati personali (per il periodo necessario al titolare del trattamento per verificare l'esattezza), quando il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali, chiedendo semplicemente che ne sia limitato l'utilizzo, quando il titolare del trattamento non ne abbia più bisogno ai fini del trattamento ma i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, e quando l'interessato si è opposto al trattamento (in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato).

Si osserva come, nel solo caso in cui siano stati esercitati i diritti di «intervento» sui dati (rettifica, cancellazione, limitazione), il titolare è tenuto, «*salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato*», a comunicare a ciascun destinatario a cui erano stati comunicati i dati l'esecuzione di tali operazioni.

L'art. 20 del Regolamento ha poi codificato il diritto alla «*portabilità*» dei dati, a fronte del quale l'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano, anche se tale diritto è limitato al caso in cui i suoi dati siano oggetto di trattamento automatizzato e solo nel caso il trattamento si basi sul consenso o su un contratto.

Speculare al diritto alla limitazione del trattamento è rimasto, se pur limitato solo ad alcuni trattamenti (*recte*, ai trattamenti svolti per talune basi giuridiche) il diritto di «opposizione» che, disciplinato dall'art. 19, può essere esercitato *ad nutum* nel caso in cui il trattamento sia svolto per finalità di marketing (nel quale caso i dati non possono più essere oggetto di trattamento «per tali finalità», mentre, si ritiene, laddove la finalità fosse l'unica finalità per la quale i dati erano oggetto di trattamento, allora devono essere cancellati), oppure può essere esercitato per motivi connessi alla situazione particolare dell'interessato allo scopo di impedire la prosecuzione del trattamento dei dati per finalità di interesse pubblico e/o sulla base del legittimo interesse del titolare o di terzi.

L'opposizione si distingue nettamente dalla cancellazione dei dati; con quest'ultima, infatti, l'interessato opta per l'eliminazione definitiva dei suoi dati personali; con l'opposizione, invece, l'interessato si limita ad impedire l'esecuzione anche solo di alcune operazioni del trattamento che, pertanto, sussistendo i requisiti di legge, non possono più essere effettuate.

Si badi che, non meno importante, l'art. 21 del Regolamento attribuisce agli interessati il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla

sua persona, salvo che tale trattamento non sia stato acconsentito dall'interessato stesso (anche se, sul punto, si consideri che il consenso è sempre revocabile), che non sia previsto da un contratto del quale è parte l'interessato e che non sia consentito dalla normativa (art. 22, par. 2, del Regolamento).

La normativa nazionale, sulla scorta di quanto consentito dall'art. 23 del Regolamento, ha poi previsto talune ipotesi che escludono la possibilità di esercitare tali diritti (art. 2-*undecies* del Codice). Si tratta, in particolare, dei casi in cui dall'esercizio di tali diritti possa deriva un pregiudizio (i) agli interessi tutelati dalle disposizioni antiriciclaggio, (ii) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di estorsioni, (iii) all'attività di Commissioni parlamentari d'inchiesta, (iv) all'attività svolta da un soggetto pubblico per finalità inerenti la politica monetaria e valutaria, al sistema dei pagamenti al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità nonché (v) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria e (vi) alla riservatezza dell'identità del dipendente pubblico che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio (c.d. whistleblowing).

7. Il trattamento da parte di soggetti pubblici

In linea di principio il Regolamento, che non si sofferma in modo particolare sul trattamento dei dati da parte della pubblica amministrazione, si limita ad individuare l'interesse pubblico come base giuridica del trattamento [29].

Il soggetto pubblico può quindi procedere al trattamento dei dati solo qualora quest'ultimo sia finalizzato all'adempimento dei suoi fini istituzionali, purché rispetti i limiti stabiliti dalla normativa.

---

[29] L'art. 6, par. 1, lett. e) del Regolamento, in particolare, consente il trattamento dei dati quando «*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*» e precisa che detta finalità può essere stabilità dal diritto dell'Unione e/o di uno Stato membro, e che «*potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per altre specifiche situazioni di trattamento di cui al capo IX. Il diritto dell'Unione o degli Stati membri persegue un obiettivo di interesse pubblico ed è proporzionato all'obiettivo legittimo perseguito*» (art. 6, par. 3, del Regolamento).

Sul punto, a fronte della individuazione della specifica base giuridica da parte del legislatore eurounitario, è intervenuto l'adeguamento nazionale che ha espressamente disciplinato la predetta base giuridica, distinguendo i requisiti di liceità del trattamento dei dati comuni dai requisiti previsti per il trattamento dei dati particolari.

Il Codice detta speciali disposizioni per la disciplina del trattamento dei dati personali del quale è titolare una Pubblica Amministrazione.

In ambito pubblico, infatti, per procedere al trattamento e, quindi, per interferire con il diritto alla protezione dei dati personali dell'interessato, è necessario bilanciare con particolare rigore i contrapposti interessi pubblici e costituzionalmente rilevanti, con la precisazione che, evidentemente, la nuova normativa non distingue più, nettamente, i soggetti pubblici dai soggetti privati, bensì la sola "finalità" pubblicistica del trattamento, che come tale prescinde dalla natura del soggetto che vi procede.

Sulla base di tale precisazione è evidente come, se pur solo in astratto, potrebbero esserci trattamenti di dati svolti da soggetti pubblici non aventi scopi legati al pubblico interesse, così come potrebbero esserci trattamenti svolti sulla base dell'interesse pubblico ma da parte di soggetti privati.

7.1. Il trattamento dei dati comuni

In tale contesto il trattamento dei dati personali comuni necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri deve essere disciplinato da una norma dell'Unione europea oppure da una norma dello Stato membro al quale è soggetto il titolare del trattamento.

Ovviamente, sul punto, la normativa interna poteva intervenire solo rispetto alla normativa nazione, tanto che l'art. 2-*ter* del Codice prevede che tale norma interna può essere costituita solo dalla legge o, sulla base di questa, da un regolamento.

È quindi evidente che i trattamenti dati da parte di soggetti pubblico, o da parte di privati che vi procedono per l'esecuzione di un compito di interesse pubblico possono essere svolti solo laddove detto interesse sia previsto dalla legge.

L'art. 2-*ter*, poi, prevede particolari disposizioni per la comunicazione e la diffusione dei dati. La norma, infatti, consente di procedere alla comunicazione dei dati a soggetti che li debbano trattare per le medesime finalità pubblicistiche solo se prevista da norme di legge o di regolamento o, in mancanza, se risulta «*comunque*» necessaria per lo svolgimento delle funzioni istituzionali. Solo in

tal ultimo caso il titolare è tenuto a darne «*previa*» comunicazione al Garante il quale, ovviamente, gode del potere di vietarla (qualora, ovviamente, ravvisi una violazione di legge, anche sotto il profilo del principio di finalità e di necessarietà), di imporre accorgimento o limitazioni.

Lo stesso art. 2-*ter*, dispone poi che la comunicazione dei dati dai predetti titolari a soggetti che li debbano trattare per finalità aliene da quelle pubblicistiche, e la diffusione (che comporterebbe *ex se* il trattamento per finalità diverse) sono ammesse unicamente quando sono previste da norme di legge o di regolamento. In tali casi, quindi, in mancanza della specifica autorizzazione normativa non sarà possibile procedere alle relative operazioni, nemmeno dandone comunicazione al Garante.

7.2. Il trattamento dei dati particolari

Come si è visto, in virtù della particolare invasività, per l'interessato, dei trattamenti di dati particolari, il legislatore europeo ha inteso proteggere con maggior rigore le libertà fondamentali dell'individuo, circondando con norme più rigorose il trattamento degli stessi per finalità di interesse pubblico.

L'art. 9 del Regolamento, in particolare, consente il trattamento dei dati di natura particolare, oltre che negli altri casi specifici già analizzati, quando «*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*».

L'art. 2-*sexies* del Codice, intervenuto in applicazione di quanto consentito dal'art. 9, par. 4 del Regolamento, dispone in ambito nazionale che il trattamento (ivi compresa la comunicazione e la diffusione) dei dati sensibili (quindi dei dati particolari di cui all'art. 9 del Regolamento), se pur limitatamente a quelli diversi dai dati sanitari, biometrici e genetici (il cui trattamento, invece, è disciplinato dal successivo art. 2-*septies*) è consentito solo qualora sia previsto «*dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento 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*».

Non solo, quindi, l'art. 2-*sexies* impone l'esistenza di una norma autorizzatrice di rango legislativo, ma tale disposizione deve specificare i dati trattabili,

le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

In mancanza di una norma che possieda tali requisiti, anche per evitare la paralisi dell'attività della pubblica amministrazione, l'art. 2 *sexies*, comma 2, prevede già una serie di casi in cui si presume la sussistenza del rilevante interesse pubblico perseguito, fermo restando la necessità, comunque, che vi sia una norma di legge che prevede gli altri due requisiti dei dati trattabili e delle operazioni eseguibili. Il Codice individua già, quindi, in via generale, alcune attività perseguenti rilevanti finalità di interesse pubblico, sopperendo così alla carenza normativa.

Nonostante tali previsioni, tuttavia, l'art. 2-*sexies*, diversamente dal previgente art. 20, non prevede (più) che, qualora sia specificata la rilevante finalità di interesse pubblico, ma non i dati trattabili e le operazioni eseguibili, i soggetti pubblici possono procedere al trattamento previa identificazione, con atto regolamentare, dei tipi di dati e di operazioni strettamente pertinenti e necessarie.

Ma, sul punto, v'è da dire che le particolari limitazioni alla possibilità di trattare dati sensibili sono mitigate dal successivo art. 2-*septies* che, invece, prescindendo dalle disposizioni legislativa testé richiamate, consente il trattamento sulla base dell'interesse pubblico dei dati genetici, dei dati biometrici e dei dati sanitari «*in presenza di una delle condizioni di cui al paragrafo 2 del medesimo articolo ed in conformità alle misure di garanzia disposte dal Garante*».

Si badi che tali misure di garanzia dovranno rispettare i principi contenuti nel medesimo art. 2-*septies*, commi 2, 4 e 5, finalizzato ad introdurre vincoli alla potestà decisionale relativa alle modalità di trattamento e, comunque, ai dati trattabili e alle operazioni eseguibili.

Le predette misure, infatti, sono adottate in relazione a ciascuna categoria dei dati personali, avendo riguardo alle specifiche finalità del trattamento e possono individuare ulteriori condizioni sulla base delle quali il trattamento di tali dati è consentito.

8. Il Garante per la protezione dei dati personali

Già in precedenza si è fatto riferimento al Garante per la protezione dei dati personali, che è l'autorità indipendente istituita in Italia e alla quale, in linea generale, l'art. 51 del Regolamento attribuisce il compito di sorvegliare l'applicazione del Regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di agevolare la libera circolazione dei dati personali all'interno dell'Unione.

Il Garante è composto da quattro membri, nominati dalle due Camere del Parlamento (art. 153, comma 1, del Codice), che decidono con autonomia e indipendenza di giudizio (art. 52, par. 1, Regolamento) tant'è vero che, decorso il settennato di carica, non possono essere rieletti, e nel corso dell'incarico non possono svolgere alcuna altra attività, nemmeno a titolo gratuito.

L'Autorità esercita genericamente il controllo sui trattamenti di dati personali e, comunque, i compiti specificamente elencati nell'art. 57 del Regolamento UE. L'Ufficio del Garante controlla che i trattamenti di dati personali siano effettuati nel rispetto delle norme di legge e di regolamento ed ha il potere/dovere di adottare i provvedimenti previsti dalla legge o dai regolamenti e di decidere sui reclami o sulle segnalazioni aventi ad oggetto inosservanze di legge o di Regolamento presentate dagli interessati ai sensi degli artt. 141 e 144 del Codice

Lo scopo principale del Garante è quindi quella di tutelare gli interessati dai danni che potrebbero ricevere dal trattamento illecito di dati personali. Del resto il medesimo art. 154 attribuisce al Garante il potere di «*ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine*» (art. 58, par. 2, lett. d), del Regolamento), di «*imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento*» (art. 58, par. 2, lett. f), del Regolamento) nonché di «*denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni*» (art. 154, comma 1, lett. d), del Codice).

Queste funzioni vanno ad aggiungersi ai compiti attribuiti per diffondere tra il pubblico le norme che regolano la materia e le sue finalità (art. 57, comma 1, par. b, del Regolamento), nonché quelle di promuovere, nell'ambito delle categorie interessate, l'adozione delle regole deontologiche e codici di condotta (art. 154, comma 1, lett. e), del Codice e art. 57, par. 1, lett. m), del Regolamento).

Non meno importante è la funzione consultiva del Garante, avendo quest'ultimo il compito di coadiuvare l'autorità governativa e legislativa nella loro attività. L'art. 154, comma 1, lett. f), del Codice, infatti, attribuisce al Garante il compito di «*predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione della* […] *legge*» e l'art. 57, par. 1, lett. c), del Regolamento gli attribuisce il compito di «*fornire consulenza* […] *al parlamento nazionale, al governo e ad altri organismi e istituzioni in merito alle misure legislative e amministrative relative alla protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento*», tant'è vero che l'art. 36, par. 4, del Regolamento prevede espressamente che «[g]*li Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve*

essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento».

9. La tutela giurisdizionale e amministrativa

In considerazione della particolarità delle libertà fondamentali tutelate dalla normativa in analisi, la normativa eurounitaria ha ritenuto di disciplinare, a fianco dei procedimenti giurisdizionali, necessariamente disciplinati dagli Stati membri, un rimedio celere ed efficacie dinanzi alle singole autorità di controllo,

L'art. 77 del Regolamento, infatti, prevede che l'interessato ha il diritto di proporre reclamo al Garante ogni qual volta che ritenga che il trattamento dei dati che lo riguarda violi il Regolamento e, in tale caso, l'autorità di controllo (che, lo si ribadisce, per l'Italia è il Garante per la protezione dei dati personali) è tenuta ad informare l'interessato dello stato del suo reclamo e della facoltà di rivolgersi all'autorità giudiziaria.

Il reclamo, che deve contenere un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, deve essere deciso entro nove mesi dalla sua presentazione, e consente al Garante, in via cautelare o in via definitiva, di adottare uno dei provvedimenti di cui all'art. 58 del Regolamento (tra i quali, particolarmente rilevanti nell'ambito del reclamo, quello di ingiungere al titolare o al responsabile di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento, di ingiungere al titolare o al responsabile di conformare i trattamenti alle disposizioni del Regolamento, se del caso, in una determinata maniera ed entro un determinato termine, quello di ingiungere al titolare di comunicare all'interessato una violazione dei dati personali, quello di imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento, ecc.).

Il procedimento giurisdizionale, poi, è disciplinato dai successivi artt. 78 e 79 del Regolamento, il primo dei quali attribuisce a chiunque di agire nei confronti dell'autorità di controllo, sia «*avverso una decisione giuridicamente vincolante*» sia «*qualora l'autorità di controllo che sia competente* […] *non tratti un reclamo o non lo informi entro tre mesi dello stato o dell'esito del reclamo proposto*» (ovviamente tale ultima azione è data solo all'interessato, dato che solo quest'ultimo può proporre i reclami ai sensi dell'art. 77 del Regolamento.

Il successivo art. 79, invece, attribuisce a ogni interessato il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a

norma del Regolamento siano stati violati a seguito di un trattamento. Ovviamente il ricorso all'autorità giurisdizionale è alternativo al reclamo dinanzi l'autorità garante (cfr. art. 140-*bis*, commi 2 e 3, del Codice).

In ambito nazionale il Codice ha poi voluto introdurre un procedimento giurisdizionale particolarmente veloce ed efficace.

In tale contesto, infatti, l'art. 152 del Codice prevede che tutte le controversie che riguardano l'applicazione del Codice sono di competenza dell'autorità giudiziaria ordinaria (anche se tese ad impugnare un provvedimento amministrativo), che decide con il rito del lavoro ed in composizione monocratica, peraltro con l'espresso potere di prescrivere le misure necessarie anche in deroga al divieto di cui all'art. 4 della legge 20 marzo 1865, n. 2248, allegato E) ed anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile dei dati.

10. La responsabilità nel trattamento dei dati

10.1. La responsabilità civile

L'art. 82 del Regolamento disciplina l'obbligo di risarcimento del danno provocato per effetto del trattamento dei dati personali, di fatto reiterando le previgenti disposizioni contenute nell'art. 15 del Codice che, sul punto, facevano rinvio espresso all'art. 2050 c.c.

Legittimato passivo dell'azione risarcitoria è colui che detiene il controllo generale dell'attività (il titolare) e, in esito alle integrazioni europee, anche il responsabile, se pur, quest'ultimo, solo se non ha adempiuto agli obblighi del Regolamento specificamente diretti ai responsabili o se ha agito in modo difforme o contrario rispetto alle istruzioni del titolare (art. 82, par. 2, del Regolamento).

In questi termini la giurisprudenza esclude che legittimato passivo possa essere colui che delega altri, senza vincolo di subordinazione; diversamente, nel caso dell'affidamento del trattamento ad un responsabile, quest'ultimo, pur dovendo essere scelto tra soggetti che forniscano idonea garanzia, deve «*procedere al trattamento attenendosi alle istruzioni impartite dal titolare*». Ciò significa che in tale circostanza gli obbligati devono essere identificati, solidalmente, sia nel titolare sia nel responsabile [30] anche se sul punto, alla luce di quanto dispone l'art. 28, par. 10, del Regolamento («*se un responsabile [...] viola il pre-*

[30] S. SICA, *Commento all'art. 18*, in E. GIANNANTONIO-M. LOSANO-V. ZENO ZENCOVICH, *La tutela dei dati personali: commentario alla L. 675/1996*, Cedam, Padova, 1999.

sente regolamento [...] è considerato un titolare del trattamento in questione»), potrebbe anche legittimamente sostenersi che in caso di violazione di istruzioni e compiti l'unico obbligato dovrebbe essere, appunto, il responsabile ritualmente designato [31].

L'art. 82 attribuisce pertanto a «[c]*hiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile*».

L'obbligazione al risarcimento del danno sorge dunque in qualsiasi caso in il danno sia in rapporto di causa-effetto («causato») con la violazione di una disposizione del Regolamento, con la precisazione che per esonerarsi da responsabilità, il convenuto è tenuto a dimostrare che l'evento dannoso non gli è in alcun modo imputabile. Tale prova non verte, quindi, sulle modalità del fatto, bensì sull'organizzazione dell'attività o sui fattori esterni al verificarsi del fatto: il titolare deve infatti dimostrare, a mero titolo esemplificativo, di aver adottato tutti quegli accorgimenti previsti da norme legislative, regolamentari o tecniche che disciplinano la specifica attività [32], e comunque deve dimostrare di aver correttamente adempiuto agli obblighi di responsabilizzazione previsti dall'art. 24 del Regolamento.

Il danno è quindi risarcibile, nel *quantum*, secondo gli ordinari criteri valutativi di cui agli artt. dal 2056 al 2059 c.c.

Sul punto giova precisare che il legislatore ha preso in considerazione la circostanza che, nell'ambito dei trattamenti di dati, l'eventuale danno è prevalentemente di carattere morale. Per questo motivo l'art. 82 consente espressamente la risarcibilità del «*danno immateriale*» oltre, ovviamente, a quello di natura più propriamente «*materiale*».

10.2. La responsabilità amministrativa

Il Regolamento introduce nell'ordinamento sanzioni di natura pecuniaria particolarmente efficaci.

L'art. 83, anche in considerazione della (spesso) maggior incisività delle sanzioni di natura economica, peraltro sulla scorta di come si era già mosso il

---

[31] Così, del resto, se pur in materia di sanzioni, v. anche Garante, provv. 4 aprile 2019, doc. web 9101974.

[32] G. BUTTARELLI, *op. cit.*, che cita la sentenza Cass., 8 ottobre 1970, n. 1895, in *Giur. it.*, 1971, I, 1, c. 216, nonché D. CARUSI, *La responsabilità*, in V. CUFFARO-V. RICCIUTO (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997.

legislatore nazionale, che aveva depenalizzato (*rectius*, decriminalizzato) alcune previgenti figure delittuose e contemporaneamente aumentato l'importo delle sanzioni amministrative già previste, consente alle autorità di controllo di applicare, anche unitamente alle altre misure di loro competenza del Garante, sanzioni amministrative particolarmente incisive.

Esso infatti prevede la possibilità, a seconda del tipo di violazione, di infliggere sanzioni amministrative basate, proporzionalmente, sul fatturato mondiale annuo.

In particolare, l'art. 83 prevede la possibilità di irrogare una sanzione fino al 2% del fatturato (o fino a 10 milioni di euro se non si tratta di imprenditori) per le violazioni inerenti gli obblighi del titolare e del responsabile e/o degli organismi di certificazione, oppure fino al 4% (o fino a 20 milioni) per le violazioni sui principi del trattamento, sui diritti dell'interessato, sul trasferimento all'estero e/o dei provvedimenti delle autorità di controllo.

10.3. La responsabilità penale

L'art. 84 del Regolamento impone agli Stati dell'UE di adottare sanzioni «*effettive, proporzionate e dissuasive*» per garantire il rispetto della normativa sulla tutela dei dati personali.

Alla luce di quanto dispone l'art. 83 del Regolamento, in materia di sanzioni pecuniarie, si ritiene che l'art. 84 sia più altro finalizzato ad invitare gli Stati membri, per le violazioni più gravi, ad introdurre nell'ordinamento sanzioni di natura penale, quindi senz'altro più efficaci di quelle squisitamente economiche.

In proposito la legislazione di adeguamento ha completamente riformulato l'apparato sanzionatorio penalistico, in particolare l'art. 167 del Codice («*Trattamento illecito di dati personali*») che, sulla scorta di quanto già prevedeva in precedenza, resta applicabile al solo caso in cui il fatto non sia previsto dalla legge come reato più grave, al solo caso di sussistenza del dolo specifico (richiedendo che il reo abbia commesso il fatto arrecando «nocumento» e, comunque, al fine di procurare a sé o ad altri un profitto [33] o di arrecare ad altri un danno) e, comunque, solo se un nocumento si sia effettivamente verificato. La norma, per quanto qui interessa, punisce in particolare chiunque proceda al trattamento dei dati particolari in violazione delle norme che ne disciplinano il trattamento, chiunque proceda al trasferimento dei dati all'esterno in assenza dei

[33] Il profitto di cui parla la lettera della legge non deve essere necessariamente patrimoniale, potendo essere intesa come tale, ad es., l'intenzione di procurarsi notorietà.

relativi presupposti, e chiunque proceda a particolare tipologie di trattamenti, in violazione della relativa disciplina, considerati particolarmente "invasivi" (v. dati relativi al traffico telefonico, all'ubicazione e/o al marketing telefonico).

Il D.Lgs. 101/2018 ha inoltre introdotto due nuove disposizioni incriminatrici che, fermo restando la sussistenza del dolo specifico, ma senza che sia richiesto nocumento (che, evidentemente, è presunto) punisce chiunque comunica, diffonde o acquisisce un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala (cfr. artt. 167 *bis* e 167 *ter* del Codice).

Al fine di attribuire maggiore efficacia ai provvedimenti del Garante e alle sue funzioni, l'art. 170 continua a sanzionare chiunque vìoli (anche mediante comportamento meramente omissivo) i provvedimenti adottati dall'Autorità nell'esercizio dei suoi poteri. In proposito la norma punisce con la sanzione penale il comportamento che si pone in contrasto con le statuizioni contenute (i) nei provvedimenti del Garante che impongono una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento, (ii) nelle misure di garanzia per il trattamento dei dati genetici, biometrici e sanitaria, (iii) nei provvedimenti del Garante che individuano le prescrizioni delle autorizzazioni generali ritenute ancora vigenti.

L'ultima figura delittuosa è contenuta nell'art. 168 che punisce la falsità nei documenti esibiti e nelle dichiarazioni rivolte nell'ambito di un procedimento dinanzi al Garante o nel corso di accertamenti nonché chiunque cagioni l'interruzione o il turbamento della regolare attività del Garante.

11. Le misure di sicurezza

Ai fini della più completa garanzia del diritto alla protezione dei dati personali, l'art. 32 del Regolamento, impone al titolare e al responsabile di mettere «*in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*».

Le misure di sicurezza hanno lo scopo di evitare, per quanto possibile, la lesione dei diritti tutelati dalla normativa in analisi all'evidente fine di apprestare una tutela preventiva, e non solo sanzionatoria, dei diritti stessi.

L'individuazione e l'adozione di tali misure di sicurezza deve avvenire «[t]*enendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisi-*

che». La sicurezza, pertanto, non riguarda il sistema informatico in quanto tale, ma i dati trattati. La protezione del sistema informatico ne è solo la conseguenza o, meglio, lo strumento [34].

L'impostazione data dal legislatore all'individuazione delle misure adeguate di sicurezza è basta sullo stesso principio di responsabilizzazione che governa l'intera impalcatura del Regolamento e che pretende che il titolare metta in atto misure tecniche e organizzative adeguate per garantire e dimostrare che il trattamento sia effettuato conformemente al Regolamento (art. 24).

Gli accorgimenti da adottare non si risolvono, quindi, in una serie di misure di sicurezza standard e applicabili alla generalità dei titolari, bensì in una serie di accorgimenti che devono essere individuati dal titolare e che riguardano lo specifico trattamento, le sue finalità, i dati trattati, gli interessai coinvolti.

In ogni caso l'art. 32 del Regolamento prevede dei criteri guida, dato che prevede espressamente che, a seconda del caso, le misure di sicurezza adeguate devono prevedere:

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.

Riferimenti bibliografici

ACCIAI R., *Privacy e banche dati pubbliche: il trattamento dei dati personali nelle pubbliche amministrazioni*, Cedam, Padova, 2001.

ACCIAI R.-ORLANDI S., *Le nuove norme in materia di privacy*, Maggioli, Rimini, 2003.

ALPA G., *La disciplina dei dati personali. Note esegetiche sulla legge 31 dicembre 1996, n. 675/96 e successive modifiche*, Edizioni SEAM, Roma, 1998.

ALPA G., *Diritto della responsabilità civile*, Laterza, Roma-Bari, 2003.

ARCUDI G., *Il diritto alla riservatezza: profili amministrativi, civili, penali, disci-*

[34] G. FINOCCHIARO, *Una prima lettura della legge 31 dicembre 1996, n. 675, «Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali»*, in *Contr. e impr.*, 1997, 1.

plinari, contabili, deontologici della privacy con particolare riguardo al settore sanitario, Ipsoa, Milanofiori, 2000.

ARNÒ G.-LENSI ORLANDI A., *La tutela della privacy nella rete Internet*, Giappichelli, Torino, 2002.

ATELLI M., *Dal diritto di essere lasciati soli al diritto di essere lasciati in pace: la prospettiva del danno da petulanza*, in *Riv. crit. dir. priv.*, 1997, 4.

ATELLI M.-CONDEMI M.-MONTORI L.-PANETTA R., *Le modifiche alla normativa in materia di privacy*, La Tribuna, Piacenza, 2002.

BELLANTONI D., *Lesione dei diritti della persona: tutela penale, tutela civile e risarcimento del danno: ingiuria, diffamazione, calunnia, tutela della privacy, danno patrimoniale, danno non patrimoniale, danno biologico, danno esistenziale*, Cedam, Padova, 2000.

BELLAVISTA A., *I poteri dell'imprenditore e la privacy del lavoratore*, in *Atti del Convegno "I poteri dell'imprenditore e la privacy del lavoratore"*, Venezia, 2002.

BIANCA C.M.-BUSNELLI D. (a cura di), *Tutela della privacy*, in *Nuove leggi civ. comm.*, 2-3, 1999.

BRANDEIS L.-WARREN S., *The Right to Privacy*, in *Harward Law Review*, 4, 1890.

BUTTARELLI G., *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 676 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Giuffrè, Milano, 1997.

CATAUDELLA A., voce *Riservatezza (diritto alla)*, in *Enc. giur.*, vol. XXVII, Roma, 1991.

CLEMENTE A. (a cura di), *"Privacy"*, Cedam, Padova, 1998.

COMANDÈ G., *Privacy informatica: prospettive e problemi*, in *Danno e resp.*, 1997.

CORRIAS LUCENTE G., *La recente riforma delle norme penali a tutela della riservatezza informatica*, in *Dir. informazione e informatica*, 2, 2002.

COSSU C., *Dal caso Soraya alla nuova legge sulla tutela della riservatezza*, in *Contr. e impr.*, 1998.

CUFFARO V.-RICCIUTO V. (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997.

CUFFARO V.-RICCIUTO V.-ZENO-ZENCOVICH V. (a cura di), *Trattamento di dati e tutela della persona*, Giuffrè, Milano, 1997.

FINOCCHIARO G., *Una prima lettura della legge 31 dicembre 1996, n. 675*, in *Contr. e impr.*, 1997, n. 1, p. 306.

FINOCCHIARO G., *Una prima lettura della legge 31 dicembre 1996*, *n. 675, "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali"*, in *Contr. e impr.*, 1997.

FORTE D., *Le regole e la sicurezza su Internet*, Il Sole 24Ore, Milano, 2003.

FRANCESCHELLI V. (a cura di), *La tutela della privacy informatica. Problemi e prospettive*, Giuffrè, Milano, 1998.

FRANZONI M., *Colpa presunta e responsabilità del debitore*, Cedam, Padova, 1988.
FROSINI V., *La carta d'identità informatica: il profilo perfetto di una persona*, in *Telema*, 20, 2000.
GIACOBBE G.-GIUFFRIDA A., *I diritti della personalità*, vol. III, Utet, Torino, 2000.
GIANNANTONIO E.-LOSANO M.G.-ZENO-ZENCOVICH V. (a cura di), *La tutela dei dati personali. Commentario alla L. 675/96*, Cedam, Padova, 1997.
IMPERIARI R.-IMPERIALI R., *La tutela dei dati personali. Vademecum sulla privacy informatica*, Il Sole 24Ore, Milano, 1997.
IMPERIALI R.-IMPERIALI R., *Il trasferimento all'estero dei dati personali: modalità e soluzioni contrattuali per il flusso dei dati nel mondo economico*, Il Sole 24Ore, Milano, 2003.
LEVI A.-ZANICHELLI F., *L'utilizzo delle e-mail a fini pubblicitari: dallo "spamming" al "permission marketing"*, in *Riv. dir. ind.*, 2001.
LOIODICE A.-SANTANIELLO G., *La tutela della riservatezza*, Cedam, Padova, 2000.
LOSANO M.G. (a cura di), *La legge italiana sulla privacy. Un bilancio dei primi cinque*, Laterza, Roma-Bari, 2001.
LUGARESI N., *Internet, privacy e pubblici poteri negli Stati Uniti*, Giuffrè, Milano, 2000.
MANES P., *Il consenso al trattamento dei dati personali*, Cedam, Padova, 2001.
MANTOVANI M., *Le fattispecie incriminatrici della legge sulla privacy: alcuni spunti di riflessione*, in *Crit. dir.*, 1997, p. 4.
MEMMO D., *La privacy informatica: linee di un percorso normativo*, in *Contr. e impr.*, 3, 2000.
MINELLA T., *La privacy: guida all'applicazione della legge 675/1996*, Simone, Napoli, 2001.
MONDUCCI J., *Il trattamento dei dati personali da parte delle imprese assicuratrici*, in *Diritto e pratica delle Società*, Il Sole 24Ore-Pirola, Milano, 2000.
MONDUCCI J., *La circolazione on line dell'individuo*, in *Ciberspazio e diritto*, 2000, 1.
MONDUCCI J., *Diritti della persona e trattamento dei dati particolari*, Giuffrè, Milano, 2003.
MONDUCCI J., *Il trasferimento dei dati nell'Internet*, in *http://www.interlex.it/675/monducc1.htm*, consultato il 15 maggio 2011.
MONDUCCI J., *Il dato genetico. Tra autodeterminazione informativa e discriminazione genotipica*, BUP, 2014.
MONDUCCI J.-SARTOR G. (a cura di), *Il Codice in materia di protezione dei dati personali*, Cedam, Padova, 2004.
MONTORI L.-PANETTA R., *Le modifiche alla normativa in materia di privacy*, La Tribuna, Piacenza, 2002.
ORLANDI S.-SANTI M.R., *Privacy e libere professioni*, Buffetti, Roma, 1999.
ORLANDI S.-TESSARO T., *Tutela della privacy e diritto di accesso ai documenti nell'ente locale*, Maggioli, Rimini, 2000.

PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione europea*, Giuffrè, Milano, 2002.

PARDOLESI R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003.

PATTI S., *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999.

PELLECCHIA E., *Commento all'art. 22 della l. 31 dicembre 1996, n. 675*, in *Nuove leggi civ. comm.*, 1999.

PERCIBALLI L., *Art. 9, Elenco degli abbonati*, in M. ATELLI, *Privacy e telecomunicazioni. Commentario al D.Lgs. n. 171/1998*, Jovene, Napoli, 1999.

PERRI P., *Privacy, diritto e sicurezza informatica*, Giuffrè, Milano 2007.

PERRI P., *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Giuffrè, Milano, 2007.

PRATTICO F., *Burocratica o tecnologica, è la rete che fa esistere l'uomo*, in *Telema*, 19, 2000.

RODOTÀ S., *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir.*, n. 4, 1991.

RODOTÀ S., *Tecnologie e diritti*, il Mulino, Bologna, 1995.

SCALISI A., *Il diritto alla riservatezza: il diritto all'immagine, il diritto al segreto, la tutela dei dati personali, il diritto alle vicende della vita privata, gli strumenti di tutela*, Giuffrè, Milano, 2002.

SICA S., *La riservatezza nelle telecomunicazioni: l'identificazione del chiamante nell'esperienza inglese e nella prospettiva comunitaria e italiana*, in *Dir. informazione e informatica*, 1997.

SICA S., *D.Lgs. 467/01 e "Riforma" della privacy: un vulnus al "sistema" della riservatezza*, in *Dir. informazione e informatica*, 2002.

ZALLONE R., *Codice dell'informatica, di internet e della privacy: con commento e giurisprudenza*, C. Marinotti, Milano, 2001.

ZENO-ZENCOVICH V., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Juris*, 1997.