

David D'Agostini

La tutela dei dati personali

(aggiornamento: 15 marzo 2005)

1. Introduzione.

Nel 1890 a Boston i due giuristi Samuel D. Warren e Louis D. Brandeis, considerati i padri della privacy, pubblicarono nella Rivista di diritto di Harvard un celebre articolo che diede il via al processo di riconoscimento della riservatezza quale diritto della personalità e alla descrizione di privacy come “*diritto a essere lasciati soli*”¹.

La nozione di privacy nell'ultimo secolo si è evoluta acquistando significati maggiormente corrispondenti all'attualità, secondo un percorso normativo che ha preso le mosse dai principi fondamentali della Costituzione repubblicana e della Convenzione Europea del 4 novembre 1950 “*per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*”. Quest'ultima, realizzando un sistema di tutela sovranazionale, ha riconosciuto esplicitamente al cittadino il diritto individuale al “*rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza*”.

In tale cammino, oltre alla importante Convenzione di Strasburgo “*per la protezione delle persone in relazione all'elaborazione automatizzata dei dati a carattere personale*” n.108 del 1981, una tappa decisiva è rappresentata dall'accordo firmato a Schengen il 14 giugno 1985, che prevedeva l'abolizione dei controlli di frontiera tra paesi firmatari e il contemporaneo rafforzamento delle frontiere esterne della comunità europea. Per poter onorare tale accordo, l'Italia ha dovuto dotarsi di una legge sulle banche dati e, recependo la direttiva comunitaria 95/46/CE, ha approvato la legge 31 dicembre 1996 n.675.

Nel predisporre la prima normativa in tema di privacy, il Parlamento ha cercato di contemperare i diritti individuali e collettivi, approntando un sistema di adempimenti che non fosse eccessivamente oneroso per gli obbligati, ma che tutelasse in maniera effettiva il soggetto cui si riferiscono i dati, al quale vengono riconosciuti i diritti a:

- non fare circolare i propri dati personali;
- controllarne l'utilizzazione;
- far cessare il trattamento illecito.

Nel breve periodo di 5 anni, la legge 675/96 è stata modificata ben 10 volte, fino alla sua definitiva abrogazione a opera del menzionato Codice per la protezione dei dati personali che l'ha integralmente sostituita.

Seguendo il percorso di armonizzazione tracciato dalle istituzioni comunitarie, l'evoluzione legislativa è, da ultimo, approdata al “*Codice in materia di protezione dei dati personali*”, in vigore dal 1° gennaio 2004.

2. Il Codice.

Il decreto legislativo 30 giugno 2003 n.196, intitolato “*Codice in*

¹ Warren e Brandeis, *Right to Privacy*, 4 Harv. L. Rev. 1890.

materia di protezione dei dati personali”, garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà personali, nonché della dignità dell’interessato con particolare riferimento alla riservatezza, all’identità personale e al diritto alla protezione dei dati personali.

Il Codice si compone di 186 articoli suddivisi in tre parti:

- 1) disposizioni generali;
- 2) disposizioni relative a specifici settori;
- 3) tutela dell’interessato e sanzioni.

Inoltre ne sono parte integrante 3 allegati:

- A) codici di deontologia;
- B) disciplinare tecnico in materia di misure minime di sicurezza;
- C) trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia.

Secondo quanto stabilito all’art.4, si deve intendere per:

- “*trattamento*”, qualunque operazione compiuta sui dati dalla raccolta fino alla cancellazione o distruzione compresa;
- “*dato personale*”, qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione;
- “*dati identificativi*”, i dati personali che permettono l’identificazione diretta dell’interessato;
- “*dati anonimi*”, i dati che non possono essere associati a un interessato identificato o identificabile;
- “*dati sensibili*”, i dati personali idonei a rivelare l’origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l’adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
- “*dati giudiziari*”, i dati personali idonei a rivelare determinati provvedimenti in materia di casellario giudiziale o la qualità di imputato o di indagato in un procedimento penale;
- “*comunicazione*”, il dare conoscenza dei dati personali a uno o più soggetti determinati;
- “*diffusione*”, il dare conoscenza dei dati personali a soggetti indeterminati.

Queste distinzioni si riverberano sulla disciplina applicabile in concreto ai singoli trattamenti.²

Il *titolare* del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione o qualsiasi altro ente o associazione, a cui spettano le decisioni in ordine alle finalità e alle modalità del trattamento

² Appare opportuno chiarire che non tutti i dati personali sono anche identificativi (si pensi a uno *username* di fantasia privo di riferimenti all’interessato); inoltre che i dati considerati “riservati” non sono necessariamente “sensibili” secondo la definizione di legge (per es. le coordinate bancarie sono dati comuni).

di dati personali, nonché agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Il titolare ha la facoltà di designare secondo le esigenze organizzative uno o più *responsabili*, ai quali possono anche essere suddivisi i compiti, scegliendoli tra i soggetti dotati di maggiore esperienza in materia di trattamento di dati personali e di sicurezza;³ nell'atto di nomina vengono specificati analiticamente i compiti affidati al responsabile che nell'esercizio della propria funzione deve, comunque, attenersi alle istruzioni impartite dal titolare.

Tutte le persone fisiche autorizzate a compiere operazioni di trattamento, secondo le istruzioni impartite dal titolare o dal responsabile, vengono definite *incaricati* al trattamento.

Solitamente sono lavoratori dipendenti del titolare, ma può anche trattarsi di collaboratori occasionali (per es. stagisti) ovvero esterni, non essendo importante tanto la sussistenza di un rapporto di lavoro, quanto l'effettivo trattamento di dati da parte del soggetto incaricato. Anche in questo caso la nomina deve avvenire per iscritto e individuare puntualmente l'ambito del trattamento consentito.

Infine l'*interessato* è il soggetto al quale si riferiscono i dati personali, cui viene riconosciuto e garantito che il trattamento si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della sua dignità, con particolare riferimento alla riservatezza.

3. I diritti dell'interessato.

Gli artt.7 e segg. del Codice disciplinano i diritti dell'interessato, tra i quali spicca il *diritto di accesso*, cioè di ottenere la conferma dell'esistenza o meno dei propri dati personali e la loro comunicazione in forma intelligibile.

L'interessato ha diritto di conoscere:

- a) l'origine dei dati -il cd. flusso a monte-;
- b) le finalità e le modalità del trattamento;
- c) la logica applicata in caso di trattamento automatizzato;
- d) gli estremi identificativi del titolare e degli eventuali responsabili;
- e) i soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati -il cd. flusso a valle-.

All'interessato vengono riconosciuti i *diritti di interdizione, inibizione e di opposizione*.

Si rientra nella prima ipotesi qualora venga richiesto l'aggiornamento, ovvero la rettificazione o l'integrazione dei dati⁴; la seconda si sostanzia nell'istanza di cancellazione, di trasformazione in

³ Nella prassi aziendale è possibile verificare come tale ruolo venga spesso ricoperto dal responsabile dei sistemi informativi.

⁴ Salvo che si tratti di dati personali di tipo valutativo, come nel caso di giudizi soggettivi espressi dal datore di lavoro.

forma anonima o di blocco dei dati trattati in violazione di legge. Il diritto di opposizione è consentito in due ipotesi:

- 1) in presenza di motivi legittimi;
- 2) nel caso di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale (secondo il cd. principio del ripensamento).

L'interessato non può godere dei diritti menzionati in alcune particolari fattispecie, laddove prevalgono forti esigenze di segretezza;⁵ il loro esercizio non richiede motivazione, nè l'osservanza di particolari formalità.⁶

4. Il riscontro del titolare.

L'art.10 del Codice regola il riscontro all'interessato da parte del titolare del trattamento il quale non può esimersi dal fornire le informazioni richieste e/o dall'ottemperare alle legittime istanze.

Il titolare è obbligato a garantire all'interessato un effettivo esercizio dei suoi diritti, agevolandogli l'accesso ai propri dati personali, eventualmente pure mediante l'impiego di strumenti informatici e telematici.⁷ Le informazioni possono essere comunicate per iscritto o anche oralmente, ovvero mediante strumenti elettronici, assicurandone sempre l'intelleggibilità.⁸ Qualora non risulti confermata l'esistenza di dati che riguardano il richiedente, quest'ultimo dovrà pagare un contributo per le spese sostenute dal titolare.

Il titolare è tenuto a dare riscontro a tutte le richieste entro *15 giorni* dal ricevimento (ovvero 30 giorni nei casi di particolare complessità, previo avviso all'interessato).

Qualora la domanda venga respinta o non sia esaudita nei termini, l'interessato può presentare *ricorso* all'Autorità Garante, che invita il titolare ad aderire spontaneamente oppure a giustificare il proprio diniego.

In caso di accoglimento del ricorso, il Garante adotta i provvedimenti più opportuni per tutelare i diritti dell'interessato, per esempio ordinando al titolare di esibire il documento richiesto oppure disponendo il blocco di un trattamento illecito e così via (è solo il caso di accennare che l'inosservanza di tali provvedimenti è sanzionata penalmente con la reclusione da 3 mesi a 2 anni).

⁵ Per es. nel corso di indagini penali o di inchieste parlamentari, ovvero qualora i trattamenti di dati personali siano effettuati da forze di polizia per motivi di ordine pubblico.

⁶ Nella prassi si utilizza solitamente la lettera raccomandata con avviso di ricevimento, allo scopo di preconstituirsì una prova documentale da utilizzare in sede di ricorso al Garante. La richiesta viene rivolta al titolare, o all'eventuale responsabile, e potrà anche essere inoltrata tramite un incaricato.

⁷ Si pensi ai siti web che erogano servizi a mezzo internet permettono all'utente di verificare e modificare il profilo personale *on line*.

⁸ Quindi, se viene fatto uso di codici o sigle, è necessario fornire i parametri per la comprensione del relativo significato.

5. L' informativa.

Prima di dare inizio al trattamento il titolare è obbligato, ai sensi dell'art.13 del Codice, a informare l'interessato - oralmente o per iscritto - in merito a:

- a) le finalità e le modalità del trattamento;
- b) la natura obbligatoria o facoltativa del conferimento dei dati;⁹
- c) le conseguenze di un eventuale rifiuto di rispondere;
- d) i soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, nonché l'ambito di diffusione dei dati stessi;
- e) i diritti che spettano all'interessato stesso;
- f) gli estremi identificativi del titolare e degli eventuali responsabili.

Il Garante, soprattutto nei primi tempi di applicazione della legge 675/96, si è più volte pronunciato contro le informative generiche e le formule tautologiche, in quanto non idonee a perseguire il principio di trasparenza insito nella norma; pertanto, è necessario che il titolare descriva il trattamento effettuato in concreto, al di là di schemi preimpostati, in modo chiaro e funzionale allo scopo.

L'obbligo generale di informativa sussiste anche nell'ipotesi in cui i dati personali non siano forniti direttamente dall'interessato, bensì raccolti presso terzi, come nel caso di acquisto di banche dati e archivi per scopi economici o di marketing ovvero di reperimento da registri pubblici o da elenchi di dominio pubblico.

Si rammenta, infine, la necessità di rispettare la norma anche nell'ipotesi di trattamento elettronico delle informazioni e di sistemi informativi automatizzati, come nel caso non infrequente in cui i dati siano raccolti mediante la compilazione di un *form* all'interno di un sito internet.

La mancata (o inidonea) informativa all'interessato viene punita dall'art.161 del Codice con una sanzione amministrativa.¹⁰

6. Il consenso.

A eccezione degli enti pubblici nel limite dello svolgimento delle loro funzioni istituzionali, ai sensi dell'art.23 del Codice il trattamento di dati personali richiede il consenso dell'interessato che, affinché sia validamente prestato, dev'essere:

- 1) *informato*
- 2) *libero*
- 3) *esplicito*

⁹ Si distinguono i casi in cui i dati siano forniti per un obbligo di legge, per l'esecuzione di un rapporto contrattuale, per ulteriori ragioni, etc..

¹⁰ Sanzione amministrativa del pagamento di una somma da 3.000 a 18.000 euro, oppure da 5.000 a 30.000 euro se si tratta di dati sensibili o giudiziari; tale predetta sanzione può essere aumentata fino al triplo qualora, viste le condizioni economiche del contravventore, risulti inefficace.

4) *specifico*.

Pertanto l'omissione o l'insufficienza dell'informativa è causa di invalidità del consenso eventualmente ottenuto, inoltre l'interessato non deve subire condizionamenti nella propria scelta; il consenso non può essere desunto per fatti concludenti, tuttavia può essere rilasciato anche oralmente, oppure mediante strumenti informatici o telematici, purchè risulti *documentato per iscritto* dal titolare.

Il trattamento di dati sensibili, invece, necessita dell'autorizzazione del Garante e del consenso *manifestato in forma scritta*.

Il titolare viene esonerato dal richiedere il consenso in alcune specifiche fattispecie previste dall'art.24 del Codice e, in particolare, quando:

- a) il trattamento è obbligatorio per legge;
- b) vengono eseguiti obblighi contrattuali;
- c) i dati provengono da pubblici registri;
- d) si tratta di dati relativi allo svolgimento di attività economiche;
- e) è necessario far valere un diritto in sede giudiziaria.

La mancanza del consenso dell'interessato, al di fuori dei casi di esonero, rende illecito il trattamento dei dati, con conseguente responsabilità a carico del titolare¹¹.

7. Ulteriori adempimenti.

Secondo quanto disposto dagli artt.37 e 38 del Codice, in alcuni casi tassativi il titolare prima di procedere a determinati trattamenti è tenuto a presentare al Garante idonea *notificazione*.

In particolare vanno notificati i trattamenti concernenti i dati:

- a) genetici e biometrici;
- b) indicanti la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
- c) registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti;
- d) sensibili registrati in banche di dati a fini di selezione del personale per conto terzi;
- e) sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
- f) trattati con strumenti elettronici per definire il profilo o la personalità dell'interessato o per analizzare le abitudini o le scelte di consumo.

L'omessa (o incompleta) notificazione viene punita dall'art.163 del Codice con una sanzione amministrativa.

La notificazione viene trasmessa *una tantum*, prima dell'inizio del trattamento, tramite il sito internet del Garante e dev'essere sottoscritta con firma digitale; è richiesto un nuovo invio solo nel caso di cessazione del trattamento oppure di variazione degli elementi.

L'art.39 del Codice obbliga il titolare a *comunicare* previamente al

¹¹ P. Manes, *Il consenso al trattamento dei dati personali*, CEDAM, 2001.

Garante ulteriori ipotesi.

La trasmissione di dati tra soggetti pubblici non prevista dalla legge e il trattamento di dati sanitari nell'ambito della ricerca biomedica possono avere inizio solamente dopo 45 giorni dal ricevimento della comunicazione da inviarsi per via telematica oppure mediante fax o lettera raccomandata con avviso di ricevimento.

Infine, il titolare è tenuto a *richiedere l'autorizzazione* del Garante per il trattamento dei dati sensibili e giudiziari, salvo il rilascio da parte della stessa Autorità di autorizzazioni concernenti intere categorie di titolari o di trattamenti.

Il Garante ha emesso (e ogni anno rinnova) 7 autorizzazioni generali che riguardano le fattispecie di trattamenti più diffusi:

- 1) trattamento dei dati sensibili nei rapporti di lavoro;
- 2) trattamento dei dati idonei a rilevare lo stato di salute e la vita sessuale;
- 3) trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni;
- 4) trattamento dei dati sensibili da parte dei liberi professionisti;
- 5) trattamento dei dati sensibili da parte di diverse categorie di titolari;
- 6) trattamento di alcuni dati sensibili da parte degli investigatori privati;
- 7) trattamento di dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

In presenza di dati sensibili, pertanto, appare essenziale che il titolare verifichi che il trattamento operato rientro nelle ipotesi di autorizzazione generale indicate, dovendo provvedere -in caso contrario- a un apposita istanza al Garante.

7. La cessazione del trattamento.

In caso di cessazione del trattamento, a prescindere dalla causa, l'art.16 del Codice prescrive che i dati siano:

- a) distrutti;
- b) ceduti ad altro titolare per scopi compatibili con quelli precedenti;
- c) conservati per fini esclusivamente personali;
- d) trattati per scopi storici, statistici o scientifici.

8. Il Garante.

L'Autorità garante per la protezione dei dati personali è stata istituita dalla legge 675/96, come organo collegiale dotato di piena autonomia e indipendenza di giudizio e di valutazione¹².

Il Garante è costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica.

I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità,

¹² G. Rasi, *Società e privacy: un anno da Garante*, Roma, 2002.

nonchè un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

Il presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

Al Garante è assegnato il compito istituzionale di:

- a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione;
- b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
- c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti;
- d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporre il blocco;
- e) promuovere la sottoscrizione di codici deontologici;
- f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi;
- g) esprimere pareri nei casi previsti;
- h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;
- i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
- j) tenere il registro dei trattamenti formato sulla base delle notificazioni;
- k) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del Codice.¹³

L'art.154 del Codice impone al Presidente del Consiglio dei ministri e a ciascun ministro di consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulla materia del trattamento dei dati personali.

In tal caso il Garante deve rendere un parere nel termine di quarantacinque giorni dal ricevimento della richiesta, decorso il quale l'amministrazione può procedere.

Infine la medesima norma dispone che copia dei provvedimenti emessi dall'autorità giudiziaria in materia protezione dei dati personali ovvero di criminalità informatica venga trasmessa al Garante.

¹³ La relazione viene trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

9. Le sanzioni.

Le sanzioni previste in caso di violazione delle norme contenute nel Codice sono disciplinate nella sua terza e ultima parte e si dividono in

a) sanzioni amministrative:

- omessa o inidonea informativa all'interessato
- mancata o incompleta notificazione
- omessa informazione o esibizione al Garante
- cessione illecita di dati

L'organo competente a provvedere è il Garante, secondo la procedura delineata nel Codice e integrata dalla legge 24 novembre 1981 n.689 (legge sulle sanzioni amministrative).

Il titolare, entro 60 giorni dalla contestazione, può far pervenire le proprie difese, allegando eventuali documenti e richiedendo di essere sentito personalmente.

Esaurita la fase istruttoria, l'Autorità, qualora ritenga accertata la violazione, commina la sanzione e ne ingiunge il pagamento con ordinanza motivata, che costituisce titolo esecutivo nei confronti del titolare.

Quest'ultimo, nel termine di 30 giorni dalla notifica del provvedimento, può pagare quanto dovuto oppure presentare opposizione all'ordinanza-ingiunzione davanti al giudice.

b) sanzioni penali:

- trattamento illecito di dati
- falsità nelle dichiarazioni e notificazioni al Garante
- omissione delle misure minime di sicurezza
- inosservanza di provvedimenti del Garante

L'ipotesi delittuosa principale è quella di trattamento illecito di dati personali che prevede la violazione di precetti molto eterogenei che spaziano dalle norme sul consenso al trattamento alle regole in tema di comunicazioni indesiderate, con particolare inasprimento delle pene previste per la comunicazione e la diffusione dei dati sensibili.

Per essere condannato, il reo deve avere agito al fine di trarre un profitto o per recare un danno a terzi, indipendentemente dall'aver raggiunto il proprio scopo (il reato ha *dolo specifico*); inoltre, dal trattamento illecito dev'essere derivato un nocumento all'interessato (*condizione di punibilità*).

10. La responsabilità civile.

A norma del Codice della privacy, chiunque subisce un danno per effetto del trattamento di dati personali ha diritto al risarcimento, salvo che il titolare dimostri di aver adottato tutte le misure idonee a evitarlo (secondo la regola generale stabilita per l'esercizio di attività pericolose dall'art. 2050 c.c.).

In virtù di questa inversione dell'onere probatorio, il danneggiato può limitarsi a provare di aver subito un danno a causa del trattamento del danneggiante (secondo un rapporto eziologico di

causa-effetto); mentre il titolare del trattamento per sottrarsi alla condanna deve convincere il giudice di aver osservato tutte le norme previste dalla legge, dettate dal Garante e suggerite dalla diligenza.

Tale prova (chiamata non a caso *probatio diabolica*) si rivela estremamente difficile da fornire in giudizio, per la semplice considerazione che l'illecito che causa il danno è sempre frutto di una lacuna del titolare, salvi rari casi fortuiti o di forza maggiore¹⁴.

Peraltro in una recente pronuncia la Corte di Cassazione per la prima volta ha affermato espressamente che tale responsabilità si qualifica come "oggettiva" e, pertanto, prescinde dalla colpa di chi ha posto in essere l'attività¹⁵.

Ciò si traduce in un'ulteriore estensione della tutela per il danneggiato in quanto il giudice non è tenuto a valutare la colpevolezza del titolare del trattamento, ma solo il nesso causale tra fatto illecito e danno provocato.

Per quanto concerne il *quantum* oggetto di risarcimento, l'art.15 del Codice dispone che venga liquidato non solo il danno patrimoniale (composto da danno emergente e lucro cessante), ma anche quello non patrimoniale (es. danno morale e biologico), potendo utilizzare anche criteri di valutazione equitativa, qualora non risulti comprovato l'ammontare preciso del danno patito.

Si tenga, infine, presente che molto spesso la tutela predisposta dal Codice della privacy si affianca a quella garantita da altre norme: per es. in relazione alla foto di una persona, oltre alle norme sulla riservatezza si può richiamare la tutela della fotografia (e i diritti di sfruttamento) stabilita dalla legge sul diritto d'autore; oppure la pubblicazione di certe informazioni, al di là della privacy, può sostanziarsi in una lesione della dignità o dell'immagine professionale di un soggetto (ovvero commerciale se trattasi di un'impresa).

¹⁴ S. Sica, *Articolo 18 (Danni cagionati per effetto del trattamento di dati personali)* in *La tutela dei dati personali: commentario alla L.675/96*.

¹⁵ Cass. Civ., III sez., sent. 4 maggio 2004, n.8457 in *Foro it.*, 2004, I, 2378 con nota di Bitetto.