PRIVACY E PROTEZIONE DATI PERSONALI

Studio Legale Panama Immigration

WWW.PANAMA-IMMIGRATION.NET

Quella che con un termine ormai entrato nell'uso comune viene indicata come **privacy** è il **diritto alla riservatezza delle informazioni personali e della propria vita privata**, cioè uno strumento posto a salvaguardia e a tutela della sfera privata del singolo individuo, da intendere come la facoltà di impedire che le informazioni riguardanti tale sfera personale siano divulgate in assenza dell'autorizzazione dell'interessato, od anche il diritto alla non intromissione nella sfera privata da parte di terzi. Tale diritto assicura all'individuo il controllo su tutte le informazioni e i dati riguardanti la sua vita privata, fornendogli nel contempo gli strumenti per la tutela di queste informazioni.

L'istituto nasce come diritto "*a essere lasciato solo*" (*to be let alone*) negli Stati Uniti nel 1890, e viene elaborato nel nostro paese a partire dagli anni '60-'70 come generico diritto alla libera determinazione nello svolgimento della propria personalità.
Sempre più compresso nella società della comunicazione elettronica, nel tempo si è evoluto ed oggi si parla di privacy non più, e non solo, nel senso di protezione dei dati personali (quindi come diritto negativo volto a impedire la rilevazione di informazioni sul nostro conto), ma in una accezione più ampia anche quale diritto ad esprimere liberamente le proprie aspirazioni più profonde e realizzarle attingendo liberamente alla

proprie potenzialità. In tal senso è intesa come privacy anche l'**autodeterminazione** e la sovranità su se stessi, il riconoscersi parte attiva, e non più passiva, in un rapporto con le istituzioni, nel rispetto reciproco delle libertà.

Legislazione

I primi riferimenti alla privacy si possono far risalire alla Convenzione europea dei diritti dell'uomo che già stabiliva come non può esservi ingerenza di una autorità pubblica nell'esercizio del diritto alla propria libertà individuale, a meno che tale ingerenza sia prevista dalla legge in quanto misura necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui.
Questo fondamentale concetto è stato poi riportato ed espanso in vari accordi internazionali, come ad esempio quello di **Schengen**, ed anche nella Carta dei diritti fondamentali dell'Unione europea che che all'art. 8 così recita: "*1. Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*".

Tra le fonti comunitarie contenenti riferimenti alla privacy ricordiamo direttiva 95/46/CE del Parlamento europeo e del Consiglio, che dal 2018 sarà sostituita dal Regolamento generale

europeo.

Per quanto riguarda la legislazione italiana è inutile cercare norme sulla privacy nella carta Costituzionale, essendo nata in un'epoca nella quale il problema era poco sentito. Però nel tempo si sono ritrovati numerosi riferimenti tra le righe delle varie disposizioni, in particolare negli articoli 14, 15 e 21, rispettivamente riguardanti il domicilio, la libertà e segretezza della corrispondenza, e la libertà di manifestazione del pensiero. In realtà il primo e più importante riferimento è oggi visto nell'articolo 2 della Costituzione, in quanto si incorpora la privacy nei diritti inviolabili dell'uomo, come del resto ha sostenuto la Corte Costituzionale con la sentenza n. 38 del 1973.
La prima elaborazione del diritto alla privacy la abbiamo a livello giurisprudenziale, con la **sentenza della Corte di Cassazione n. 4487 del 1956**, a seguito di un ricorso degli eredi del tenore Enrico Caruso, con la quale si identificava tale diritto nella tutela delle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile. Una tale affermazione è divenuta fondamentale per il bilanciamento tra riservatezza e diritto di cronaca, in quanto la linea di demarcazione tra privacy e diritto all'informazione di terzi è oggi data dalla popolarità del soggetto, pur precisando che anche soggetti famosi conservano tale diritto, però limitatamente a fatti che non hanno niente a che vedere con i motivi della propria popolarità.
Di seguito il concetto di privacy si evolse a mezzo di ulteriori sentenze, come quella della **Cassazione del 20 aprile 1963, n. 990**, con la quale la Suprema Corte riconosceva fondata la pretesa dei familiari di Claretta Petacci a non raccontare in un libro vicende private in assenza di interesse pubblico.
Se nelle predette sentenze la Cassazione formalmente non riconosceva l'esistenza di un diritto alla riservatezza, ma nella

sostanza ammetteva il diritto ad un tutela in tale ambito, solo nel 1975 finalmente si riconobbe che nel nostro ordinamento il diritto alla privacy aveva una cittadinanza, con la sentenza n. 2129 del 27 maggio 1975, con la quale si tutelava il diritto alla riservatezza della moglie dello Scià di Persia.

Inizialmente, quindi, la riservatezza era più che altro un diritto delle persone famose, infatti l'Italia arrivò come penultima in Europa ad approvare una legge di tutela della privacy di applicazione generale, trasfusa prima nella legge 675 del 1996 e poi nel **Codice in materia di protezione dei dati personali** (Codice della privacy) cioè il Decreto legislativo 30 giugno 2003, n. 196, dal quale si evince chiaramente che la privacy non è solo il diritto a non vedere trattati i propri dati senza consenso, ma anche l'adozione di cautele tecniche ed organizzative che tutti, compreso le persone giuridiche, devono rispettare per procedere in maniera corretta al trattamento dei dati altrui.
Detta normativa, considerata la più completa a livello europeo, dedica la prima parte ai principi generali, dettando le definizioni essenziali per la comprensione della normativa, tra le quali quelle di dato personale e di trattamento.

Dati personali

Oggetto della normativa sulla privacy sono i dati personali, cioè "*qualunque informazione relativa a persona fisica, identificata od identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale*". Il dato personale è quindi un bene giuridico di secondo livello, un contenitore vuoto all'interno del quale l'interprete inserisce uno specifico contenuto relativo al

patrimonio informativo dell'interessato.
Costituiscono sempre dati personali quelli che riguardano la famiglia e altre situazioni personali, il lavoro, le attività economiche, commerciali, finanziarie ed assicurative, i beni, le proprietà e i possessi.
Il decreto Salva Italia del governo Monti ha modificato la normativa stabilendo che i dati delle persone giuridiche non sono dati personali, per cui possono essere liberamente trattati, a parte eventuali ipotesi di illecito civile o penale e a parte la regolamentazione relativa al telemarketing.

I dati personali si dividono in quattro categorie:
- **dati sensibili**: quelli idonei a rivelare "*l'origine razziale o etnica, le convinzioni religiose, filosofiche o di altro genere, 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*" di una persona; i dati relativi alla salute e alla vita sessuale sono anche detti "supersensibili" in quanto sono gli unici per i quali non sussiste alcuna esenzione che ne consente l'uso in assenza di un consenso;
- **dati semisensibili**: categoria non ben definita, nella quale rientrano dati personali il cui trattamento può arrecare danni al titolare, come i dati relativi alle liste di sospettati di frode, i nominativi inseriti nelle centrali rischi, i dati relativi alla situazione finanziaria;
- **dati comuni**: sono tutte quelle informazioni, come nome, cognome, partita I.V.A., codice fiscale, indirizzo (compreso quello di posta elettronica), numeri di telefono, numero patente, che consentono di individuare una persona fisica o giuridica, sia essa anche un ente od associazione;
- **dati giudiziari**: sono quelle informazioni idonee a rivelare provvedimenti in materia di casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reati o carichi pendenti.

Elemento essenziale è la identificabilità del soggetto interessato, direttamente od indirettamente, al fine di classificare un dato come personale. Per identificabilità indiretta si intende la possibilità di identificare il soggetto in relazione al contesto, ad esempio dalle caratteristiche fisiche inserendolo in una specifica categoria o classe, oppure attraverso una operazione di riunione di più frammenti di informazione. In tal modo anche informazioni che di per sé non sono sufficienti per l'identificazione possono essere dati personali, come l'indirizzo IP, oppure un cookie archiviato in un computer.

Per i **dati sensibili** esistono doveri particolari in capo al titolare del trattamento, infatti occorre il consenso scritto al trattamento, nonché la notificazione al Garante. I casi di notifica al Garante sono stati ridotti notevolmente, ormai alle sole ipotesi nelle quali il trattamento sia suscettibile di arrecare pregiudizio al titolare dei dati.

Trattamento

Il cardine della disciplina è dato dalla necessità del consenso per il trattamento dei dati personali, che deve essere libero e consapevole.
Il trattamento deve essere inteso come una qualsiasi operazione, anche svolta senza mezzi elettronici, di raccolta, consultazione, elaborazione, conservazione, organizzazione, modificazione, raffronto, utilizzo, comunicazione, diffusione, cessione, cancellazione, distruzione dei dati, anche se non registrati in una banca dati.
Il trattamento deve rispondere al cosiddetto **principio di necessità**, cioè si deve minimizzare l'utilizzazione di dati

personali ed identificativi, così da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi oppure modalità che permettano di identificare l'interessato solo in caso di necessità.

La normativa, quindi, prevede una serie di adempimenti e di misure minime che colui il quale effettua un trattamento per fini non privati, deve necessariamente porre in essere, altrimenti l'inosservanza di queste norme determina un illecito, amministrativo o addirittura penale.
Ogni danno cagionato da un trattamento illecito dà luogo al **risarcimento del danno**, a meno che il responsabile non provi che l'evento dannoso non gli è imputabile.
Il codice (art. 5 comma 3) **non si applica ai trattamenti effettuati da persone fisiche per fini esclusivamente personali** (come potrebbe essere una rubrica telefonica di un privato), **a meno che i dati non siano destinati ad una comunicazione sistematica od alla diffusione**. Si tenga presente che per comunicazione si intende portare a conoscenza una o più persone diverse dall'interessato, mentre diffusione si ha quando i destinatari sono soggetti indeterminati.
Il codice non si applica nemmeno ai **trattamenti effettuati fuori dal territorio italiano**, però sono soggetti alla normativa i trattamenti effettuati da chi si trova al di fuori del territorio italiano ma impiega strumenti situati nel territorio italiano, ed in particolare deve designare un rappresentante nel territorio italiano.

E' sufficiente l'autorizzazione del Garante, e quindi non occorre il consenso dell'interessato, se il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, compresi partiti e movimenti politici, purché il trattamento avvenga per il perseguimento di scopi determinati nell'atto

costitutivo. È sufficiente l'autorizzazione del Garante anche se il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo, oppure se è necessario per lo svolgimento di investigazioni difensive o per far valere un diritto in giudizio, o per adempiere a specifici obblighi previsti dalla legge, da un regolamento e dalla normativa comunitaria per la gestione del rapporto di lavoro.
In molti di questi casi sono state emanate dal Garante delle **autorizzazioni generali** che specificano l'ambito del trattamento. In ogni caso i dati devono essere utilizzati in modo lecito e secondo correttezza, devono essere raccolti per scopi determinati e trattati in modo compatibili con tali scopi, devono essere aggiornati e mai eccedenti rispetto alle finalità per le quali sono trattati, ed infine conservati per il periodo strettamente necessario per tali finalità. Il gestore di tali dati deve fornire agli interessati apposita **informativa**.

Oltre ai casi soggetti ad autorizzazione generale, è altresì escluso l'obbligo di chiedere il consenso qualora i dati siano trattati in ottemperanza ad un accordo contrattuale o precontrattuale del quale è parte l'interessato, per obbligo di legge, e se i dati derivano da pubblici registri (fatte salve le limitazioni in materia di pubblicazioni degli atti, si pensi a quelli anagrafici), elenchi, atti o documenti conoscibili da chiunque.

Soggetti

Nell'ambito del trattamento dei dati si individuano quattro soggetti:

- **titolare**, la persona fisica, giuridica, ente, associazione o amministrazione, cui competono le decisioni in merito alle finalità

e alle modalità del trattamento dei dati personali e agli strumenti utilizzati. È chi da inizio al trattamento, e possono esserci anche più di un titolare. In particolare ha l'obbligo di **notificazione** all'autorità garante per la privacy (obbligo che sussiste nei soli casi in cui il trattamento sia in grado di recare pregiudizio ai diritti e alle libertà dell'interessato), consentendo in tal modo un controllo sul trattamento, e l'obbligo di **informativa** all'interessato (l'informativa è sempre dovuta anche quando il consenso dell'interessato non è richiesto, o quando quest'ultimo sia tenuto a fornire necessariamente i propri dati in base ad un obbligo di legge); il titolare deve, inoltre, predisporre le misure di sicurezza per evitare una perdita o distruzione dei dati, ma anche per evitare il furto dei medesimi, nel caso l'interessato subisca un danno il titolare è responsabile civilmente; il titolare ha l'obbligo di seguire le fasi del trattamento, e non se ne può disinteressare delegandolo in toto;

- **responsabile**, la persona fisica, giuridica, ente, associazione o amministrazione preposta al trattamento dei dati dal titolare del trattamento, il quale titolare fissa anche i limiti dei suoi poteri. La nomina è facoltativa;
- **incaricato**, la persona fisica autorizzata dal titolare o dal responsabile a compiere materialmente il trattamento;
- **interessato**, la persona fisica cui si riferiscono i dati stessi. A seguito delle modifiche introdotte dal Decreto Legge 6/12/2011 n. 201 (decreto Salva Italia del governo Monti), imprese ed enti non possono più essere considerati interessati al trattamento, per cui non potranno esercitare i diritti di cui all'articolo 7 del Codice Privacy.

Informativa

Chi intende trattare dati personali altrui, prima del trattamento deve fornire agli interessati delle specifiche informazioni. Ciò avviene tramite l'informativa, che può anche essere orale, ma è preferibile sia data per iscritto al fine di provarne l'esistenza.
Il Garante ammette la possibilità di pubblicare l'informativa sul sito web anche in caso di comunicazioni postali, inserendo nella corrispondenza l'indirizzo dove si può visualizzare l'informativa. In questi casi è necessario, però, prevedere anche delle forme alternative, come ad esempio l'invio di fax a seguito di apposita richiesta, per coloro che non hanno la possibilità di leggerla online. L'informativa, quindi, è una comunicazione rivolta all'interessato e finalizzata ad informalo. È sempre **dovuta anche quando il consenso dell'interessato non è richiesto, o quando quest'ultimo sia tenuto a fornire necessariamente i propri dati in base ad un obbligo di legge**. Nei casi in cui la legge prevede l'obbligo di informativa, essa deve avere il seguente contenuto minimo (art. 13 Cod. Privacy):

- **finalità e modalità del trattamento**, con specifica indicazione di cosa si farà con i dati trattati;
- la **natura obbligatoria o facoltativa del conferimento dei dati**, cioè se il soggetto interessato possa o meno rifiutarsi di fornire i dati che lo riguardano e la conseguenza in caso di mancata fornitura dei dati;
- i **soggetti e le categorie di soggetti ai quali i dati possono essere comunicati** e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);
- i **diritti dell'interessato** (diritto di chiedere se dati personali sono presenti nella banca dati, diritto di prenderne visione e di chiederne la modifica) di cui all'articolo 7 del Decreto legislativo 30 giugno 2003, n. 196, che offrono al soggetto interessato una tutela alla propria riservatezza;
- i dati identificativi (nome, denominazione o ragione sociale, domicilio o sede) del titolare del trattamento e , se designati, del

responsabile e del rappresentante nel territorio italiano.

L'eventuale **cessione dei dati a terzi** (pensiamo alla vendita di un elenco contatti) è possibile solo se espressamente autorizzata dall'interessato con l'accettazione dell'informativa, nella quale ovviamente si dovrà indicare la finalità di cessione. Se invece si chiede genericamente il consenso all'invio di comunicazioni commerciali anche da parte di terzi, questa dicitura non consente la cessione dei dati a terzi.

Misure di sicurezza

L'informativa e la richiesta di consenso da presentare all'interessato devono essere strutturati in modo da offrirgli una adeguata tutela. Devono essere previsti anche adeguati accorgimenti tecnici per ridurre al minimo il rischio di perdita dei dati trattati per distruzione o per sottrazione, le cosiddette misure di sicurezza.
Esiste un livello di sicurezza minimo imposto dalla legge, la cui mancata adozione comporta sanzioni penali. Le misure di sicurezza minime, però, possono creare non pochi problemi, perché se si verifica una perdita dei dati, l'interessato può chiedere il risarcimento dei danni, e in questa eventualità spetta al titolare del trattamento dimostrare che le misure minime fossero adeguate alla situazione.

Tra le misure di sicurezza da attuare in caso di dati comuni e sensibili trattati con archivi cartacei abbiamo:
- individuazione per iscritto degli incaricati del trattamento;
- selezione dell'accesso ai dati strettamente necessari;
- restituzione di atti e documenti al termine del trattamento;
- utilizzo di armadi con serrature;

- obbligo di identificazione e registrazione degli incaricati che hanno accesso all'archivio dopo l'orario di chiusura.

Tra le misure di sicurezza in caso di dati comuni e sensibili trattati con archivi elettronici (connessi ad internet) abbiamo:
- individuazione per iscritto degli incaricati del trattamento;
- nomina del responsabile delle password di accesso;
- assegnazione di una password di accesso a ciascun incaricato (con possibilità di modificarla);
- assegnazione di un codice univoco per ognun incaricato al fine di identificare gli accessi;
- adozione di software di protezione;
- autorizzazione del singolo incaricato al trattamento e alla modifica dei dati;
- adozione di un documento di programmazione annuale sulle misure di sicurezza e sulla formazione degli incaricati del trattamento.

Diritti dell'interessato

La legge offre all'interessato degli specifici strumenti per la tutela dei suoi diritti. Tali diritti possono essere esercitati personalmente o a mezzo di delegato.

I diritti sono i seguenti:
- diritto di esprimere il consenso al trattamento dei dati;
- diritto ad essere informato sull'identità del titolare del trattamento e del responsabile del trattamento dei dati, nonché sulle modalità e finalità del trattamento;
- diritto ad ottenere informazioni e modifiche sui dati, in particolare: conferma dell'esistenza di dati che lo riguardano,

comunicazione degli stessi, della loro origine e della finalità del loro trattamento, cancellazione o trasformazione n forma anonima o blocco dei dati trattati illegittimamente, aggiornamento, rettifica e integrazione dei dati;
- diritto al risarcimento del danno in caso di trattamento illecito;
- diritto ad opporsi al trattamento anche se conforme alla finalità dichiarate;
- diritto ad opporsi al trattamento dei dati personali effettuato per finalità commerciali, pubblicitarie, di vendita o ricerca di mercato;
- diritto ad opporsi al trattamento dei dati personali volto a delineare il profilo o la personalità dell'interessato, salvo le eccezioni di legge.

Nel caso in cui l'interessato chieda informazioni sull'esistenza di dati che lo riguardano, il titolare del trattamento, o il responsabile per lui, ha il diritto di chiedere all'interessato di identificarsi, esibendo od allegando copia di un documento di riconoscimento. In assenza di identificazione il titolare può legittimamente rifiutare la richiesta avanzata, opponendo la mancata identificazione.
Ma in caso di corretta identificazione il titolare è obbligato a comunicare tutti i dati personali riguardanti il soggetto e contenuti nella banca dati, oppure, l'inesistenza di dati riferibili al richiedente. Solo in quest'ultima ipotesi è possibile chiedere un contributo spese per la ricerca e la comunicazione negativa, non in caso di comunicazioni positive.
Se l'interessato chiede la cancellazione, l'aggiornamento o la rettifica di dati, il titolare è obbligato ad eseguire e comunicare l'avvenuta operazione.

Sono previste alcune **deroghe**, in base alle quali i diritti dell'interessato non sono esercitabili in relazione ad operazioni di trattamento esplicate in ottemperanza alla normativa anti

riciclaggio, trattamenti per ragioni di giustizia, per investigazioni difensive o per far valere un diritto in sede giudiziaria, trattamenti effettuati dalla forze di Polizia.

Garante per la protezione dei dati personali

L'organo preposto al controllo relativo alla corretta applicazione della normativa in materia di privacy, è il Garante per la protezione dei dati personali, autorità amministrativa collegiale ed indipendente, i cui membri sono nominati dal Parlamento e che opera un controllo preventivo e successivo sulle attività di trattamento di dati personali svolte in Italia. Il Garante, che opera autonomamente dal Governo, ha poteri istruttori, consultivi e sanzionatori, e costituisce il primo grado per il ricorso amministrativo contro eventuali violazioni della normativa. Eventuali decisioni del Garante, assunte in contraddittorio con le parti in causa, sono impugnabili dinanzi alla magistratura.
Il Garante istituisce e mantiene il registro dei trattamenti per la pubblica consultazione, controlla se i trattamenti sono effettuati a norma di legge, segnala le modifiche da apportare ai trattamenti, riceve i reclami degli interessati, denuncia i reati perseguibili d'ufficio di cui viene a conoscenza, vieta i trattamenti illeciti o ne dispone il blocco, in via provvisoria, segnala al Parlamento l'opportunità di modifiche normative, esprime pareri in materia di privacy. È importante tenere presente che il compito del Garante non è tanto autorizzare i trattamenti, quanto piuttosto controllarne la liceità.

Il Garante può chiedere al responsabile e al titolare del

trattamento, all'interessato o anche a terzi, informazioni e documentazione, può disporre accessi alle banche dati e ispezioni nei luoghi dove si svolge il trattamento. Per esercitare i suoi poteri si può avvalere della collaborazione di altri organi dello Stato. Ha inoltre il potere di integrare la normativa in materia di riservatezza, quasi avesse una funzione legislativa, come previsto dall'art. 24 lettera G, che da la facoltà al Garante di individuare casi nei quali si esclude la necessità del consenso al trattamento, o le misure a garanzia dell'interessato.
Infine, il Garante irroga direttamente le **sanzioni** previste dal Codice per la privacy, sia amministrative che penali. L'art. 15 del Codice prevede l'obbligo di risarcire i danni derivanti dall'illecito trattamento. Il richiamo all'art. 2050 c.c. fa sì che dovrà essere il titolare a dimostrare, in caso di danno, di aver adottato tutte le misure idonee a evitare il danno stesso, e non solo le misure minime previste dalla legge. In sostanza si considera il trattamento dei dati personali come un'attività pericolosa, elevando così il livello di responsabilità, per cui il risarcimento spetterà per il solo fatto di aver subito un danno, a prescindere dalla volontarietà del comportamento illecito. Per andare esente da responsabilità il titolare del trattamento dovrà, quindi, dimostrare che il danno si è verificato per caso fortuito o forza maggiore.

Gli illeciti amministrativi riguardano l'omessa o inidonea informativa all'interessato, la cessione dei dati in violazione delle norme, l'omessa o incompleta notificazione, l'omessa informazione o esibizione di documenti richiesti al Garante.

Gli illeciti penali sono previsti dagli articoli da 167 a 172 del codice. All'art. 167 abbiamo il trattamento illecito di dati personali, cioè il trattamento effettuato non rispettando le disposizioni del codice (**trattamento illecito**). La consumazione del reato avviene non con il mero trattamento non conforme alle

norme, bensì al verificarsi del danno, per cui il **nocumento** alla persona offesa è elemento costitutivo del fatto.
L'art. 169 prevede l'omessa adozione di misure necessarie alla sicurezza dei dati, contravvenzione che prevede anche la possibilità di regolarizzare il trattamento nel termine di sei mesi, nel qual caso l'ammenda è diminuita.
L'art. 170 punisce l'inosservanza dei provvedimento del Garante, l'articolo 168 punisce la falsità nelle dichiarazioni e nelle notificazioni al Garante.

Privacy e diritto all'informazione

La privacy, intesa nel modo sopra descritto, trova una sua limitazione nel rapporto col **diritto di cronaca** e il diritto all'informazione costituzionalmente garantito, e si è posto il problema di stabilire il corretto compromesso tra i due interessi. Il diritto all'informazione non deve essere inteso soltanto come diritto ad informare, quindi come diritto di cronaca, ma anche come diritto alla manifestazione del pensiero, tutelato dall'articolo 21 della Costituzione, che riguarda non solo i giornalisti ma anche e soprattutto tutti i cittadini.

Il bilanciamento tra i due interessi, come sancisce il Codice in materia di protezione dei dati personali, si realizza attraverso la previsione che il soggetto interessato presti il consenso esplicito al trattamento dei dati che lo riguardano, mantenendo così il controllo su tali informazioni. Tale consenso, in particolare, è anche revocabile.
A chi esercita **attività giornalistica** è, però, permesso il trattamento dei dati personali, la comunicazione e la diffusione anche senza il consenso dell'interessato e, con riferimento ai dati sensibili e giudiziari, senza la preventiva autorizzazione del

Garante, purché ci si attenga ai limiti dettati dal diritto di cronaca, individuati nell'**essenzialità della notizia** e nell'**interesse pubblico**, con l'unica eccezione dei dati relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso i suoi comportamenti pubblici (Cass. sentenza 17408/2012).
Ad esempio, possono essere pubblicate le fotografie di persone purché acquisite in modo lecito, cioè fornite dall'interessato o scattate in luoghi pubblici o aperti al pubblico o nel corso di eventi pubblici o in collegamento con fatti di interesse pubblico. Ovviamente i dati personali di chi è coinvolto in indagini giudiziarie possono essere legittimamente pubblicati.
È da puntualizzare che le disposizioni speciali non si applicano solo alla diffusione effettuata da giornalisti, bensì a quella compiuta da chiunque, purché abbia i caratteri tipici e gli scopi precisati dall'articolo 136 del Codice privacy, cioè la funzione di informare o che comunque concerna l'espressione del pensiero.

In merito all'**essenzialità** della notizia, gli articoli 5 e 6 del codice deontologico dei giornalisti prevedono che tale requisito è rispettato "*quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti*".

La **Carta dei doveri del giornalista**, approvata nel 1993, afferma che i diritti della persona devono essere tutelati, e nel pubblicare notizie sulla vita privata delle persone si deve correttamente bilanciare il diritto del singolo con i diritti della collettività.
Una protezione particolare è affermata per i minori e i soggetti deboli, sottolineando l'obbligo di tutelare l'anonimato dei minori e l'impegno ad evitare la loro in trasmissioni televisive che possano ledere la loro personalità.
Viene poi stabilito il divieto di rendere identificabili tre tipologie di soggetti:

- le vittime di violenze sessuali;
- i membri delle forze di pubblica sicurezza e dell'autorità giudiziaria;
- i congiunti di persone coinvolte in fatti di cronaca.

La normativa attuale vieta il trattamento in ambito giornalistico di dati idonei a rivelare lo stato di salute e la vita sessuale dei cittadini. Esiste inoltre il diritto alla riservatezza sulle origini etniche, il pensiero politico, le convinzioni religiose, il diritto alla dignità degli imputati nei processi e dei malati.

In estrema sintesi una notizia riguardante la sfera personale dei singolo può essere divulgata, anche in maniera dettagliata, se è indispensabile in ragione dell'originalità del fatto, della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

Infine, nel caso dei dati sensibili si prevede che il giornalista possa prescindere dal consenso dell'interessato, rispettando tuttavia il limite dell'essenzialità dell'informazione, oltre a quello della rilevanza del dato per il caso trattato nell'articolo.

Privacy e minori

Il problema si presenta rilevante in merito al trattamento di dati relativi ai minori, minori che, da oggetto di protezione, oggi sono passati ad esse considerati soggetto di diritti. Il Garante per la privacy si è mosso da tempo nel senso della più ampia tutela del minore sia nell'ambito familiare che nelle relazioni sociali. È stata così stabilita la prevalenza del diritto alla privacy rispetto al diritto all'informazione giornalistica, quando si tratta di minori. Il diritto ad informare l'opinione pubblica, infatti, non può mai incidere negativamente sull'immagine del minore mediante la narrazione di fatti e circostanze che lo vedono protagonista, sia quale autore che vittima di illeciti.

Il Garante non manca di osservare che la divulgazione di dati in grado di consentire una identificazione, sia globale che locale, cioè limitata ad un piccolo centro o paese nel quale il minore realmente dimora, è da ritenersi comunque illecita. E questo vale sia nel casi di divulgazione di dati che rendono riconoscibile il minore direttamente, sia indirettamente, come ad esempio il caso delle divulgazione del cognome di un padre abusante nei confronti dei figli, anche quando dei figli non sia indicato il nome. Quindi si deve realizzare una tutela della privacy del minore effettiva, sia sotto il profilo formale (omissione dei dati personali) che sostanziale (divieto di identificazione in maniera indiretta).

Ovviamente è importante rispettare il principio della essenzialità dell'informazione nell'esercizio dell'attività giornalistica, principio stabilito dall'art. 137 del Codice della privacy e dall'art. 6 del Codice di deontologia del giornalista. Anche l'art. 13 della Convenzione sui diritti del fanciullo, ratificata con legge n. 176 del 1991, riconosce al fanciullo il diritto di essere protetto rispetto ad interferenze arbitrarie od illegali nella sua vita privata.
È ovvio che se manca il rischio di un danno alla personalità dei minori, la diffusione delle immagini ritraente il minore è consentita, come ad esempio nel caso in ci il servizio giornalistico dà positivo risalto a qualità del minore, oppure al contesto familiare in cui si sta formando (Garante Privacy, 6 maggio 2004, n. 1007634).

Privacy e Internet

La normativa in materia di protezione dei dati personali non impedisce l'acquisizione e il successivo trattamento dei dati da parte di organi preposti dalla legge alla tutela della sicurezza

pubblica. La legge consente l'acquisizione di tali dati ai fini di prevenzione, accertamento o repressione dei reati.
Ma, a parte ciò, il problema di garantire la privacy si pone in maniera pressante in internet, dove la diffusione dei dati è facile e veloce. Inoltre, tale problema è strettamente legato al tema della sicurezza informatica, visto che spesso si verificano furti di dati attraverso la rete. Una delle piaghe più dannose è appunto lo spyware che, installandosi spesso in maniera fraudolenta nei personal computer delle vittime, provvede a copiare ed inviare dati personali (pagine visitate, account di posta, gusti ecc) a terzi che successivamente li rielaboreranno e rivenderanno per i loro fini economici. Ovviamente la miglior difesa in questo caso è usare il buon senso e programmi adeguati per la sicurezza, come antivirus, firewall, ecc…

Dal punto di vista giuridico si è, infatti, sentita l'esigenza di ampliare il vecchio ordinamento giuridico e, di conseguenza, anche la normativa relativa al concetto di privacy che, fino a non molti anni fa, si occupava esclusivamente della tradizionale corrispondenza e della comunicazione telegrafica e telefonica.

Oggi vi sono vari reati penalmente punibili in questo campo:
- illecita diffusione di dati personali;
- violazione, sottrazione e soppressione di corrispondenza informatica;
- rivelazione del contenuto di corrispondenza telematica;
- rivelazione di comunicazioni informatiche o telematiche;
- installazioni abusive di apparecchiature per le intercettazioni informatiche;
- falsificazione, alterazione e sottrazione di comunicazioni informatiche;
- rilevazione del contenuto di documenti informatici segreti;

- accesso non autorizzato ad un sito;
- spionaggio informatico;
- frode informatica.

L'**illecita diffusione di dati personali** in rete è un reato previsto dal decreto legislativo n. 196 del 2003. Ricorre qualora si pubblichino in rete dati personali (o sensibili o giudiziari) senza espressa autorizzazione del soggetto interessato e fuori dei casi previsti dalla legge. Classico è il caso dell'azienda che pubblichi sul proprio siti i dati dei propri clienti senza autorizzazione e accessibili al pubblico. La pena prevista può arrivare fino a tre anni di reclusione.
Certamente molto importante è stata l'introduzione del reato di **frode informatica**, sancito dall'art. 640 ter c.p. secondo cui: "*chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 516 a euro 1032.*
La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1549 se ricorre una delle circostanze previste dal n.1 del secondo comma dell'art. 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema […]".

Ovviamente, le norme per il trattamento dei dati personali nell'ambito della rete sono date dal Codice per la protezione dei dati personali. Ma in questo campo sorgono problemi anche in relazione alle legislazioni estere, poiché internet è ovviamente un mezzo transnazionale, quindi una violazione commessa in rete produce effetti in molti paesi contemporaneamente. Il processo

di regolamentazione della rete è quindi agli inizi, sicuramente tutt'ora in crescita.

Privacy e diritto di difesa

Il **diritto di difesa**, essendo un diritto di rango costituzionale (art. 24 Cost.), prevale sul diritto alla privacy e non può essere soggetto a limitazioni essendo posto nell'interesse pubblico. Per questo motivo la scelta delle modalità attraverso le quali il diritto di difesa viene esercitato spetta al titolare del diritto, che lo esplica come necessario presupposto della difesa.
L'utilizzo di dati personali è, quindi, sempre ammesso in sede giudiziaria, ovviamente purché il diritto che si intende tutelare sia di rango pari a quello dell'interessato. In tale ottica, il diritto alla privacy risulta sovra ordinato al **diritto d'autore**, essendo quest'ultimo rivolto a tutelare meri interessi economici e non diritti e libertà dell'individuo, per cui una azienda non è mai autorizzata a tracciare dati dei cittadini al fine di verificare una eventuale violazione dalla normativa sul diritto d'autore, tale attività è infatti demandata in via esclusiva allo Stato e in particolare all'autorità giudiziaria.
In sostanza si asserisce che l'art. 156 bis della legge 633 del 1941 determina la prevalenza delle norme a tutela della riservatezza e segretezza delle comunicazioni sulle norme a protezione della proprietà intellettuale e le eccezioni al divieto di trattamento dei dati sono ristrette ad ipotesi ben specifiche e dettagliate. L'art. 24 del codice della privacy, infatti, consente l'uso di dati personali per far valere un diritto in giudizio, ma la norma prevede che il dato sia già in possesso della parte, non che essa sia autorizzata a cercarselo da sé.