# La normativa Sulla Privacy

## Quaderno di aggiornamento professionale n.3

A.P.T.P.L. Associazione Professionale Triestina Polizia Locale

# *La normativa sulla privacy*

La normativa sulla privacy impone una serie di adempimenti anche nello svolgimento dell'attività di polizia locale, ma del resto tutte le attività di polizia sono sottoposte a regole per la tutela dei dati personali.

La natura trasversale della privacy investe ambiti diversificati dell'attività umana, pubblica e privata e quindi finisce per investire anche i processi gestiti istituzionalmente dalla Polizia Locale.

Il presente quaderno operativo si propone di offrire agli operatori di polizia locale gli strumenti necessari per un primo approccio alla complessa e delicata normativa sulla Privacy ed è finalizzato a promuovere un uso consapevole e responsabile dei dati personali senza incorrere in "incidenti" o grossolani errori.

Il contenuto del quaderno è diviso in cinque parti:

- Inquadramento storico/normativo
- Le figure "chiave" della Privacy
- I vari tipi di dato.
- Le misure minime di sicurezza
- Le buone prassi

## 1. INQUADRAMENTO STORICO/NORMATIVO

Fino agli anni '70 la privacy non era considerata, se non con particolarissime eccezioni.

Un primo grande passo verso la tutela della privacy delle persone fu introdotto con l'approvazione delle "*Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento*" il c.d Statuto dei Lavoratori, fra l'altro la pietra miliare delle norme sul lavoro.

In particolare lo Statuto dei lavoratori Legge 20.05.1970 n° 300 all'art. 4 prevede il divieto dell'utilizzo di sistemi audiovisivi per il controllo a distanza dei lavoratori[1], mentre all'art. 8 stabilisce il divieto di indagini sulle opinioni[2].

Si deve attendere più di un quarto di secolo affinché il nostro Legislatore intervenga nuovamente sulla materia in maniera organica, non tanto perché realmente interessato quanto per adempiere ad un obbligo imposto dall'Unione Europea a tutti i Paesi che aderivano al Trattato di Schengen (ovviamente, lo fa all'ultimo secondo, il 31 dicembre 1996…). Va precisato che questa Legge si inserisce in un quadro normativo ricco e variegato: in ambito europeo l'Italia era rimasto l'unico paese, con la Grecia, a non essere dotata di una specifica legislazione relativa al trattamento dei dati personali.

La normativa sulla privacy è obbligatoria per entrare nell'area Schengen.

Viene quindi promulgata la Legge 31 dicembre 1996, n. 675, "*Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali" composta da* "soli" 45 articoli introduce finalmente, nel nostro paese, il principio per il quale la riservatezza delle persone fisiche e giuridiche (comprese le società di capitali, le associazioni riconosciute e gli enti dotati di personalità giuridica) costituisce un diritto assoluto ed inviolabile, meritevole di tutela attraverso la comminazione di sanzioni civili, penali ed amministrative.

---

1 *Art. 4. Impianti audiovisivi. È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori. Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti. Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti. Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale.*

2 *Art. 8. Divieto di indagini sulle opinioni. È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.*

Successivamente con il Decreto Legislativo 30 giugno 2003, n. 196, *"Codice in materia di protezione dei dati personali", c*omposto da ben 186 articoli più tre allegati si riuniscono in unico contesto la legge 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti negli anni. Il D.L. n.196/2003 contiene importanti innovazioni tenendo conto della "giurisprudenza" del Garante per la protezione dei dati personali e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche, ed introduce significative novità, fra cui una più chiara terminologia e una migliore definizione dei concetti di base. Il Codice è ora in vigore.

Il Decreto Legislativo 30 giugno 2003, n. 196, *"Codice in materia di protezione dei dati personali" è* suddiviso in tre parti fondamentali:

• disposizioni generali - attiene a tutti gli adempimenti e regole del trattamento

• parte speciale - dedicata a settori particolari e specifici

• parte in materia delle tutele di natura amministrativa o giudiziale - sanzioni amministrative e penali, disposizioni relative all'Ufficio del Garante delle privacy.

C'è da sottolineare che con l'entrata in vigore del c.d. Decreto "salva Italia" previsto dalla manovra Monti (Decreto Legge 6/12/2011 n. 201, in G.U. 6/12/2011 n. 284, Disposizioni urgenti per la crescita, l'equità e il consolidamento dei conti pubblici) sono state introdotte alcune modifiche sostanziali al Codice della Privacy.

L'unico risultato oggettivo, piuttosto, è che imprese ed enti non avranno più la possibilità di esercitare i diritti di cui all'art. 7 del d.lgs. 196/2003 e di far valere tali diritti in un eventuale contenzioso giudiziario (es. richieste di risarcimento danni) o dinanzi all'Autorità Garante, in quanto non possono più essere considerati "interessati al trattamento". Imprese, enti o associazioni potranno solo essere chiamati in causa quali semplici convenuti[3], in qualità di titolari o responsabili del trattamento, senza poter essere soggetti attivi e poter tutelare le proprie ragioni.

## 2. LE FIGURE "CHIAVE" DELLA PRIVACY

a. Il Garante per la protezione dei dati personali: è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla *privacy (legge 31 dicembre 1996, n.*

[3] *Convenuto, nel processo civile, è il soggetto contro il quale l'attore (soggetto attivo) propone una domanda giudiziale.*

*675)* - che ha attuato nell'ordinamento giuridico italiano la *direttiva comunitaria 95/46/CE* - e oggi disciplinata dal Codice in materia di protezione dei dati personali *(d.lg. 30 giugno 2003 n. 196)*.

L'istituzione di analoghe autorità è prevista in tutti gli altri Paesi membri dell'Unione Europea (*articolo 8 della Carta dei diritti fondamentali dell'Unione europea*).

Fondamentali per il Garante sono i "Diritti e la Prevenzione" e i "Doveri e la Responsabilità", ai quali sono dedicate due sezioni sul sito istituzionale www.garanteprivacy.it, in questi ambiti per gli accertamenti ispettivi il Garante si avvale della collaborazione del Nucleo speciale privacy della Guardia di finanza.

SEDE
Piazza di Montecitorio n. 121 - 00186 Roma
www.gpdp.it-www.garanteprivacy.it
E-mail: garante@gdp.it
Fax:(+39)06.69677.3785
Centralino telefonico: (+39) 06.69677.1

b. L'interessato: è la persona a cui si riferiscono i dati e che può esercitare i suoi diritti

c. Le gerarchie nel trattamento: il titolare del trattamento, il responsabile del trattamento e l'incaricato del trattamento

c.1 Titolare del Trattamento

La persona fisica, l'impresa, l'ente, l'associazione, ecc. cui fa capo effettivamente il trattamento di dati personali e spetta assumere le decisioni fondamentali sugli scopi e sulle modalità del trattamento medesimo (comprese le misure di sicurezza).

Nei casi in cui il trattamento sia svolto da una società o da una pubblica amministrazione per titolare va intesa l'entità nel suo complesso e non l'individuo o l'organo che l'amministra o la rappresenta (presidente, amministratore delegato, sindaco, ministro, direttore generale, ecc.).

I casi in cui il trattamento può essere imputabile ad un individuo riguardano semmai liberi professionisti o imprese individuali.

c.2 Responsabile del Trattamento

La persona, la società, l'ente, l'associazione o l'organismo cui il titolare affida, anche all'esterno, per la particolare esperienza o capacità, compiti di gestione e controllo del trattamento dei dati.

La designazione del responsabile è facoltativa (art. 29 del Codice) e quindi potrebbe anche non esserci.

c.3 Incaricato del trattamento

Il dipendente o il collaboratore che per conto della struttura del titolare elabora o utilizza materialmente i dati personali sulla base delle istruzioni ricevute dal titolare medesimo (e/o dal responsabile, se designato).

## 3. I VARI TIPI DI DATO

All'articolo 4 del Codice in materia di protezione dei dati personali si hanno varie definizioni tra le quali quelle relative ai dati:

- Dato personale
- Dati sensibili
- Dati giudiziari
- Banca di dati
- Dati relativi al traffico
- Dati relativi all'ubicazione

Le categorie di dati che andremmo ad analizzare sono quelle dei dati giudiziari, dei dati sensibili e di dati personali.

Ci sono alcuni concetti fondamentali sui dati sui quali bisogna sgombrare il campo da ogni dubbio, i dati possono essere comunicati e possono essere diffusi.

- Comunicazione dei dati

I dati vengono portati a conoscenza, anche mediante la messa a disposizione o consultazione, di soggetti determinati.

Per effettuare una comunicazione in maniera lecita, deve esserci il consenso dell'interessato (attenzione: la PA[4] segue regole particolari).

- Diffusione dei dati

I dati vengono portati a conoscenza, anche attraverso la loro messa a disposizione o consultazione, di soggetti indeterminati (potenzialmente infiniti).

- Dato personale

Qualsiasi informazione che riguardi persone fisiche identificate o che possono essere identificate anche attraverso altre informazioni, ad esempio, attraverso un numero o un codice identificativo.

Sono, ad esempio, dati personali: il nome e cognome o denominazione; l'indirizzo, il codice fiscale; ma anche un'immagine, la registrazione della voce di una persona,la sua impronta digitale, i dati sanitari, i dati bancari, ecc..

- Dato sensibile

Un dato personale che, per la sua natura, richiede particolari cautele: sono dati sensibili quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose o di altra natura, le opinioni politiche, l'adesione a partiti, sindacati o associazioni, lo stato di salute e la vita sessuale delle persone.

- Dato giudiziario

I dati giudiziari sono quei dati personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti. Inoltre possono essere quei dati personali indicanti la qualità di imputato o di indagato.

- Banca di dati

La banca di dati è un archivio dati, o un insieme di archivi, in cui le informazioni in esso contenute sono strutturate e collegate tra loro secondo un particolare modello logico (relazionale, gerarchico, reticolare o a oggetti) e in modo tale da consentire la

---

[4] n.d.r. P.A. – Pubblica Amministrazione

gestione/organizzazione efficiente dei dati stessi e l'interfacciamento con le richieste dell'utente.

## 4. LE MISURE MINIME DI SICUREZZA

Sono tutti gli accorgimenti tecnici ed organizzativi, i dispositivi elettronici o i programmi informatici utilizzati per garantire che i dati non vadano distrutti o persi anche in modo accidentale, che solo le persone autorizzate possano avere accesso ai dati e che non siano effettuati trattamenti contrari alle norme di legge o diversi da quelli per cui i dati erano stati raccolti.

Nel Codice sono fissati una serie di misure, criteri e procedure (*ad es.*, codice identificativo, *password* per l'accesso ai dati, programmi antivirus, istruzioni per il salvataggio periodico dei dati) che i titolari devono adottare a seconda che il trattamento sia effettuato con elaboratori o manualmente (archivi e documenti cartacei).

L'allegato B al Codice contiene l'elenco delle misure minime di sicurezza che devono essere obbligatoriamente applicate al fine di non incorrere nelle sanzioni previste dall'articolo 169 del Codice in materia di protezione dei dati personali.

I dati possono essere trattati manualmente (archivi e documenti in formato cartaceo) o mediante elaboratori elettronici e possono/devono essere messi in sicurezza in locali/luoghi idonei a seconda dei dati da "proteggere", non accessibili al pubblico (locali con serratura, armadi con chiave e/o casseforti) ovvero mediante elaboratori elettronici (dotati di Username, Password, Idonei Antivirus aggiornati, Autorizzazioni per Gruppi/utente, Politiche di backup e restore, Disaster recovery, Amministratori di Rete (e loro log).

## 5. LE BUONE PRASSI

Esistono svariate tecniche per carpire e quindi rubare informazioni:

- da telefono;
- dalla spazzatura (trashing);
- da email fraudolente (spaming);
- da virus, trojan e malware su pc (phising ed altro).

- Da telefono: non diamo alcuna informazione al telefono, se si devono trasmettere "dati" e non conosciamo l'interlocutore richiamiamo noi, possiamo

sempre essere intercettati (e non solo dalle forze di polizia), man in the middle (persona che si mette in mezzo a noi), centralinisti o similari, colleghi e strumenti di intercettazione ambientale (cimici e vari aggeggi).

- Dalla spazzatura: non gettiamo nella comune spazzatura alcun documento con dati di qualsivoglia natura, agende/elenchi/ecc. con numeri telefonici, email, biglietti da visita utilizziamo se possibile i distruggi documenti. Normalmente i contenitori per la raccolta della carta da riciclare sono i migliori dispensatori di dati da sottrarre (specie quelli vicini alle stampanti): se stampiamo elenchi e dati importanti, NON RICICLIAMOLI con la spazzatura (trashing):

- Da e mail fraudolente (spaming): non apriamo allegati da email di sconosciuti (possono contenere dei software autoinstallanti), utilizziamo programmi anti spam, verifichiamo il dettaglio dell'email e non solo quanto viene scritto come mittente del messaggio e non forniamo dati via email a sconosciuti. Il funzionamento del sistema di posta elettronica, tecnologicamente parlando, NON E' SICURO, in quanto NON LO E' IL PROTOCOLLO DI TRASMISSIONE SMTP! Non fidarsi al 100% delle email

- Da virus, trojan e malware su pc (phising ed altro): non frequentiamo con elaboratori "stategici" siti poco raccomandabili (siti porno, siti di gaming, siti di giochi), utilizziamo programmi antivirus e anti malware, utilizziamo chiavette USB sicure, utilizziamo password idonee di almeno 8-10 caratteri con almeno una maiuscola, un numero e un carattere speciale, utilizziamo per i file "delicati", password di protezione.

Appendice

**GLI ACCERTAMENTI D'UFFICIO DA PARTE DELLE P.A.**

Per quanto la normativa non sia più recentissima, ancora oggi permangono incomprensioni sui suoi contenuti e significati e capita, nel corso delle normali attività di ufficio, di doversi scontrare col rifiuto – spesso proprio da parte di funzionari pubblici – di fornire dati indispensabili per il completamento di pratiche in corso. Ciò va ad incidere particolarmente con le attività proprie degli enti territoriali che, essendo a contatto operativo continuo con la cittadinanza, si trovano a dover gestire quotidianamente una mole enorme di dati. Giova pertanto richiamare l'attenzione sul DPR 445/2000 "T.U. delle disposizioni legislative e regolamentari in materia di documentazione amministrativa".

L'art. 43 ("Accertamenti d'ufficio") al comma 1 dispone che P.A. e gestori di pubblici servizi "sono tenuti ad acquisire d'ufficio le informazioni oggetto delle dichiarazioni sostitutive di cui agli articoli 46 e 47, nonche' tutti i dati e i documenti che siano in possesso delle pubbliche amministrazioni, previa indicazione, da parte dell'interessato, degli elementi indispensabili per il reperimento delle informazioni o dei dati richiesti, ovvero ad accettare la dichiarazione sostitutiva prodotta dall'interessato": sussiste cioè l'obbligo, anche in presenza di autocertificazioni, di verificare contenuto ed esattezza dei dati che l'amministrazione riceve e si comprende bene come tale attività venga rallentata ed ostacolata da immotivati richiami alla privacy da parte di chi detiene dati necessari al suo svolgimento. Proprio per ovviare a questo stato di cose, il successivo comma 2 recita: "Fermo restando il divieto di accesso a dati diversi da quelli di cui e' necessario acquisire la certezza o verificare l'esattezza, si considera operata per finalita' di rilevante interesse pubblico, fini di quanto previsto dal decreto legislativo 11 maggio 1999, n. 135, la consultazione diretta, da parte di una pubblica amministrazione o di un gestore di pubblico servizio, degli archivi dell'amministrazione certificante, finalizzata all'accertamento d'ufficio di stati, qualita' e fatti ovvero al controllo sulle dichiarazioni sostitutive presentate dai cittadini. Per l'accesso diretto ai propri archivi l'amministrazione certificante rilascia all'amministrazione procedente apposita autorizzazione in cui vengono indicati i limiti e le condizioni di accesso volti ad assicurare la riservatezza dei dati personali ai sensi della normativa vigente". Il comma 3 dispone che l'acquisizione dei dati può essere effettuata per via telematica o a mezzo fax mentre il seguente comma 4 dispone la non onerosità di tali acquisizioni. Per concludere questo rapido excursus va infine rammentato che, col comma 6, si dispone che "i documenti trasmessi da chiunque ad una pubblica amministrazione tramite fax, o con altro mezzo telematico o informatico idoneo ad accertarne la fonte di provenienza, soddisfano il requisito della forma scritta e la loro trasmissione non deve essere seguita da quella del documento originale." Non è pertanto più possibile richiedere una successiva copia cartacea di un documento già fatto pervenire all'amministrazione in formato elettronico o a mezzo fax.

Trieste 21 agosto 2013