CONSIGLIO REGIONALE DEL PIEMONTE

Dossier informativo per i Consiglieri regionali

*VIII Legislatura*

# *Privacy e Pubblica Amministrazione*

Venticinque

*Ottobre 2007*

Collana pubblicazioni
*Direzione Segreteria dell'Assemblea regionale*

*Direzione Segreteria dell'Assemblea regionale*
*Direttore: Adriana GARABELLO*

*Settore Affari Istituzionali e Supporto Giuridico Legale e Settore Studi e Documentazione Legislativi*
*Dirigente: Valter BOSSI*

*A cura di;*
*Chiara CASAGRANDE e Francesco PALLANTE*

# Indice

# Introduzione

La disciplina inerente la tutela dei dati personali assume una connotazione particolare nei riguardi dei soggetti pubblici e, in generale, dell'attività amministrativa. Per un verso, infatti, in ambito pubblico il trattamento di tali dati viene ad assumere un rilievo particolare, sia per la quantità dei dati trattati, sia per la qualità delle informazioni di cui, per lo svolgimento delle proprie funzioni, la Pubblica Amministrazione deve venire a conoscenza (e, nella maggior parte dei casi, senza che sia necessario richiedere il consenso degli interessati). Per altro verso, inoltre, l'attività amministrativa si trova a operare come cerniera tra la sfera della vita individuale e la dimensione collettiva della vita associata, nella quale trovano espressione i diritti politici dei cittadini: in quest'ottica, il trattamento dei dati personali, rappresentando un'attività suscettibile di incidere in un ambito nel quale pubblico e privato si intrecciano in maniera oltremodo delicata, si configura come una spia particolarmente importante del regolare funzionamento delle istituzioni democratiche.

Sul piano più strettamente operativo, i profili maggiormente problematici emergono dalla tensione che inevitabilmente viene a crearsi a causa dell'operare, in ambito amministrativo, di due principi fondamentali, entrambi necessari, ma contrapposti: a) il principio della trasparenza amministrativa, da un lato, riscontrabile in numerose fonti normative di rango primario (dalla legge n. 241 del 1990 al decreto legislativo n. 29 del 1993, fino al testo unico degli enti locali, il decreto legislativo n. 267 del 2000) e direttamente correlato ai principi costituzionali dell'imparzialità e del buon andamento dell'azione amministrativa; b) il canone della protezione della riservatezza, dall'altro lato, anch'esso espresso a livello normativo primario (in ultimo dal decreto legislativo n. 196 del 2003) e riconducibile, a livello costituzionale, alla sfera dei diritti attinenti alla persona.

In proposito, benché i problemi in tema di trattamento dei dati personali derivanti dalle possibili interferenze tra i due principi siano potenzialmente molto delicati, occorre sottolineare come, forse anche a causa della ricca casistica pratica riscontrabile in materia, si sia ancora ben lontani dalla compiuta definizione del quadro delle esigenze derivanti, rispettivamente, dalla trasparenza e dalla riservatezza. Certo, non si può affermare che la privacy sia una materia poco o non

sufficientemente studiata. Al contrario, è sufficiente scorrere la bibliografia a corredo di una qualsiasi recente pubblicazione in argomento per rendersi immediatamente conto dell'attenzione che questo campo del diritto ha saputo, fin da subito, conquistarsi presso gli studiosi e gli operatori del diritto. In particolare, l'ambito nel quale al momento sembra si siano maggiormente concentrati gli sforzi interpretativi è quello inerente l'accesso ai documenti amministrativi, campo nel quale, soprattutto la giurisprudenza, continua a intervenire con frequenza, facendo continuamente emergere la necessità di aggiornati interventi riepilogativi da parte degli studiosi della materia.

Avvicinandosi al tema della tutela della riservatezza, bisogna tuttavia sempre tener conto del possibile sovrapporsi di molteplici operatori: oltre all'attività del legislatore (ma forse sarebbe meglio dire dei legislatori, se si tiene conto dell'intreccio tra normativa regionale, normativa nazionale e normativa europea)[1], vengono infatti in rilievo le concrete prassi amministrative (spesso differenziate a seconda dei settori d'intervento), le pronunce giurisprudenziali (anche qui, tutt'altro che univoche e comunque di provenienza differente, ordinaria e amministrativa) e gli interventi dell'Autorità Garante in materia di privacy[2]. Le esigenze che muovono questi diversi soggetti sono differenti: dettare la normativa generale e astratta è il compito del legislatore; occuparsi dell'applicazione concreta delle regole, eventualmente correggendo gli errori posti in essere dai diversi operatori, è il ruolo, rispettivamente, della pubblica amministrazione e della magistratura. A cavallo tra le diverse esigenze, data anche particolare strutturazione delle sue funzione, è invece chiamato ad operare il Garante.

Ne deriva un'inevitabile complessità, ulteriormente complicata dall'attualità dei problemi che spesso la tutela della privacy pone agli operatori nella materia. Si potrebbe dire che la sensazione di avere a che fare con un qualche cosa che sembra sempre sul punto di sfuggire dalle mani è inevitabile per chiunque intenda avvicinarsi alla trattazione di questi argomenti.

---

[1] Si segnala che con sentenza n. 271/2005 la Corte Costituzionale ha affermato che la materia della privacy è essenzialmente riferibile, all'interno delle materie legislative di cui all'art. 117 Cost., alla categoria dell'"ordinamento civile", di cui alla lettera l) del secondo comma.

[2] L'Autorità Garante è stata istituita con la legge 31 dicembre 1996, n. 675 e rinominata con il decreto legislativo 9 maggio 1997, n. 123.

È sulla base di questa consapevolezza che, nel predisporre la presente pubblicazione, si è, fin da subito, deciso di circoscriverne l'orizzonte a pochi e limitati obiettivi, scelti cercando di avere a riferimento le possibili esigenze del contesto in cui il lavoro è stato realizzato. L'idea è stata quella di provare a predisporre una sorta di ricognizione delle circostanze nelle quali la tutela della riservatezza in ambito pubblico assume profili particolarmente interessanti, perché delicati o ricorrenti o direttamente ricollegabili ad attività svolte dall'amministrazione consiliare. Nelle pagine che seguono non si ritroverà, pertanto, una rassegna completa delle problematiche inerenti la tutela della privacy nella Pubblica Amministrazione, ma, appunto, una scelta delle situazioni ritenute di maggiore interesse. Gli stessi concetti-chiave della materia (le nozioni di responsabile, titolare, incaricato, interessato; le categorie di dati personali, dati sensibili, trattamento, ecc.) verranno solo brevemente ricordati per consentire una più agevole lettura del testo: sebbene quella della privacy sia una materia in costante aggiornamento, la sua impostazione di base è infatti oramai risalente (lo stesso codice della privacy risale al 2003) e può quindi, nelle sue linee generali, essere ragionevolmente data per acquisita.

Per avvicinare l'argomento, contestualmente inquadrandolo nel suo contesto generale, verrà innanzitutto proposta una breve ricostruzione storica delle vicende che hanno scandito la preparazione, l'adozione e l'aggiornamento della normativa sulla riservatezza. Successivamente verrà presentato l'atto normativo disciplinante la materia (il decreto legislativo n. 196 del 2003), cui si è da ultimo pervenuti dopo diversi anni di interventi correttivi e integrativi della normativa originaria (la legge n. 675 del 1996); una più attenta trattazione sarà riservata alla disciplina generale dettata nei riguardi delle pubbliche amministrazioni. Così inquadrato l'argomento si procederà approfondendo i temi inerenti la tutela del danneggiato, il rapporto di lavoro pubblico, la propaganda elettorale, la videosorveglianza e le raccolte di dati sensibili. Una raccolta di documentazione in materia e l'indicazione di una serie di riferimenti bibliografici verranno collocati a completamento del lavoro.

Il proposito, come già accennato, è di contribuire a chiarificare dal punto di vista non solo teorico, ma anche tenendo presente, per quanto possibile, i risvolti pratici, alcuni aspetti particolarmente importanti legati alla questione della tutela della

riservatezza in ambito pubblico, in particolare avendo presente le esigenze più direttamente riconducibili alle attività svolte dagli uffici del Consiglio regionale.

# SEZIONE I

# PRIVACY E PUBBLICA AMMINISTRAZIONE

# Capitolo 1
# Breve ricostruzione storica

L'origine della tutela della riservatezza nel nostro ordinamento si colloca a livello internazionale.

È infatti nell'articolo 8 della Convenzione per la protezione dei diritti dell'Uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950, e ratificata con legge 4 agosto 1955, n. 848, che si trova il primo esplicito riferimento normativo alla protezione della privacy delle persone. Sebbene di portata molto generale, tale disposizione - posta a sancire l'inviolabilità della vita privata, del domicilio e della corrispondenza - venne fin da subito interpretata dalla Corte europea per i diritti dell'uomo come una previsione contenente obbligazioni negative e obbligazioni positive, rivolte sia verso i pubblici poteri, sia verso i comportamenti posti in essere dai privati.

Verso la fine degli anni Sessanta furono quindi adottate, in seno al Consiglio d'Europa, alcune raccomandazioni volte a specificare i possibili campi d'intervento, ed è interessante notare che fin da subito a essere individuati come settori particolarmente meritevoli di intervento furono quello relativo alla gestione delle banche dati, pubbliche e private, e quello concernente il riconoscimento agli interessati del diritto di accedere ai propri dati personali.

L'attenzione a tali argomenti trovò presto riscontro in numerosi paesi europei, quali Svezia, Germania, Danimarca, Norvegia, Francia e Austria, che furono i primi a effettuare interventi legislativi in materia. I loro interventi, benché caratterizzati a livello generale dall'adozione di un approccio particolarmente restrittivo, risultarono tuttavia fortemente disomogenei fra loro. A questa disomogeneità andava poi ad aggiungersi la circostanza che molti altri paesi europei non avevano ritenuto di intervenire per regolamentare la materia.

## 1. La Convenzione del Consiglio d'Europa 28 gennaio 1981, n. 108

Questa situazione - insieme favorevole, per l'attenzione che andava concentrandosi intorno al problema della tutela della riservatezza, e sfavorevole, per la confusione del quadro normativo complessivo - indusse il Consiglio d'Europa a intervenire in maniera maggiormente incisiva, promuovendo l'approvazione di una Convenzione sulla protezione dei dati personali, la numero 108, che avvenne a Strasburgo il 28 gennaio 1981.

Caratteristica di tale convenzione è l'enunciare alcuni principi fondamentali per la protezione dei dati, valevoli tanto per il settore pubblico, quanto per il settore privato. Con la loro adesione, i paesi firmatari s'impegnavano all'adozione delle misure necessarie a garantirne l'attuazione nel proprio ordinamento interno. Tra i principi contenuti nella Convenzione meritano di essere, in particolare, ricordati:

a) l'obbligo della liceità e della correttezza (quanto a pertinenza e durata rispetto agli scopi) della raccolta dei dati personali e della loro successiva elaborazione;
b) il divieto, salvo la previsione di specifiche garanzie, di elaborare i dati relativi a origine razziale, convinzioni politiche, credo religioso, vita sessuale, condizioni di salute, condanne penali;
c) l'obbligo di adottare le misure necessarie a garantire la sicurezza dei dati raccolti;
d) il riconoscimento dei diritti dell'interessato all'informazione, alla rettifica e, se illegalmente raccolti, alla cancellazione dei dati.

Tale Convenzione rimase inattuata da parte dell'Italia, ma più in generale non riuscì comunque a produrre quella omogeneizzazione del quadro normativo nel contesto europeo che la sua adozione poteva prefigurare.

## 2. La direttiva n. 95/46/CE

Più efficace si dimostrò la Commissione europea, che, a partire dall'inizio degli anni Novanta, si fece promotrice di alcune iniziative in materia, poi sfociate nell'adozione, il 24 ottobre 1995, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio, relativa alla "Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

La direttiva in questione detta le condizioni generali che rendono lecito il trattamento dei dati, individua le categorie in cui suddividere i dati, precisa il contenuto dell'informazione da fornire all'interessato, stabilisce in che cosa si concreta il diritto di accesso (sempre da parte dell'interessato), prevede la costituzione di autorità di controllo in ogni singolo paese e l'istituzione di un organismo europeo di coordinamento, detta le procedure attraverso le quali comunicare alle autorità di controllo nazionali le notificazioni dei trattamenti, fissa i principi in materia di ricorsi, responsabilità e sanzioni, disciplina il flusso dei dati tra i paesi membri dell'Unione europea, incoraggia l'adozione di codici di condotta da parte delle categorie professionali interessate al trattamento dei dati.

Tale normativa venne poi integrata con la direttiva n. 97/66/CE, relativa alla protezione dei dati personali nel delicato settore delle telecomunicazioni.

## 3. La legge 31 dicembre 1996, n. 675

Anche la direttiva 95/46/CE rimase priva di attuazione da parte del legislatore italiano. Fu l'entrata in vigore, nel gennaio del 1995, dell'Accordo di Schengen a mettere il Parlamento italiano di fronte all'urgenza di provvedere. Tale Accordo, con la relativa Convenzione di applicazione, prevedeva, infatti, la creazione di uno spazio di libera circolazione delle persone, attuato tramite l'abolizione dei controlli alle frontiere interne degli Stati aderenti e l'introduzione di un controllo unico da effettuarsi al momento dell'ingresso nel territorio di uno dei paesi facenti parte dell'Accordo. E tuttavia, affinché potessero venire soddisfatte le necessarie esigenze

di sicurezza, era prevista la creazione di un sistema di scambi di informazioni tra gli Stati aderenti, destinati ad andare a costituire un archivio comune relativo alle persone ricercate o poste sotto sorveglianza, ai veicoli e agli oggetti ricercati. Si trattava, dato il coinvolgimento di quasi tutti i principali paesi europei, di un archivio enorme, la cui costituzione ha fatto sorgere l'esigenza che venissero adottate misure idonee a proteggere adeguatamente la vita privata delle persone, conciliando sicurezza e riservatezza. Tali misure sono state individuate, appunto, nell'adozione, da parte di ogni Stato membro, di una legge sulla protezione dei dati personali, in assenza della quale l'adesione al c.d. "Sistema Schengen" restava congelata.

L'importanza dell'Accordo di Schengen non deve essere sottolineata: consentendo la libera circolazione delle persone (accanto a quella delle merci e dei servizi), contribuiva in maniera forse senza precedenti a far sentire concretamente ai cittadini il realizzarsi dell'unità europea. Adottare la necessaria normativa sulla protezione della riservatezza diventava, per il legislatore italiano, un adempimento imprescindibile. È così che si pervenne all'adozione della legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) e della legge delega 31 dicembre 1996, n. 676 (Delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali), i primi due atti normativi emanati dal legislatore italiano in tema di privacy.

La disciplina della materia si trova nella legge n. 675 del 1996; la legge delega n. 676 del 1996 venne adottata allo scopo di consentire l'integrazione e l'adeguamento della normativa principale man mano che la sua applicazione pratica lo avesse reso necessario, anche alla luce dell'evoluzione della normativa comunitaria e internazionale (ne sono scaturiti nove decreti legislativi e due d.P.R.: l'ultimo intervento normativo, il decreto legislativo n. 196 del 2003, mette ordine in tutta questa complessa e articolata normativa).

Quanto al contenuto, la legge n. 675 del 1996 si ispira direttamente alla direttiva 95/46/CE, ed è quindi rivolta principalmente alla disciplina del trattamento dei dati personali.

Nozioni centrali sono dunque, innanzitutto, quelle di «trattamento» e di «dati personali».

«Trattamento» è definito dalla legge «qualunque operazione o complesso di operazioni svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati». Dal punto di vista pratico, le operazioni che possono dar luogo alla fattispecie del «trattamento» sono la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati., siano svolte tali operazioni con o senza l'ausilio di mezzi elettronici o comunque automatizzati.

«Dato personale» è invece, sempre a norma della legge, «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». All'interno di tali dati vanno distinti, affinché possano ricevere una maggiore tutela, i dati relativi ad alcuni provvedimenti giudiziari e i «dati personali sensibili», vale a dire quelli idonei a rilevare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché quelli idonei a rivelare informazioni inerenti lo stato di salute e la vita sessuale.

Altrettanto rilevanti sono le nozioni di «titolare», «responsabile», «incaricato» e «interessato» del trattamento dei dati, le tre figure di riferimento individuate dalla legge come quelle intorno alle quali ruota l'intera normativa.

«Titolare» del trattamento è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza. Si ricorda che nel caso del Consiglio regionale del Piemonte titolare del trattamento dei dati personali è il Presidente del Consiglio stesso (ciò in seguito alla decisione assunta dall'Ufficio di Presidenza con deliberazione n. 61/2006, con la quale la titolarità del trattamento dei dati personali in ambito consiliare è stata resa autonoma da quella della Giunta).

«Responsabile» è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

«Incaricato» è la persona fisica che esegue le operazioni di trattamento su nomina del titolare o del responsabile, osservando le prescrizioni ricevute.

«Interessato» è la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Infine, un ultimo concetto che è bene ricordare è quello di «banca dati», che indica qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento.

Quanto alle concrete regole cui deve essere ispirato il trattamento dei dati, oltre alla distinzione tra dati personali sensibili e dati di natura giudiziaria, da una parte, e tutti gli altri dati personali, dall'altra, la legge distingue, prevedendo una diversa disciplina, tra dati trattati da soggetti pubblici e dati trattati da soggetti privati o da enti pubblici economici. In tutti i casi, però, vengono fissati dei criteri di carattere generale, valevoli per tutti i tipi di dati e per tutti i soggetti preposti al loro trattamento, in base ai quali i dati personali devono: (a) essere trattati in modo lecito e secondo correttezza; (b) essere raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni di trattamento in maniera non incompatibile con tali scopi; (c) essere esatti e mantenuti aggiornati; (d) essere pertinenti, completi e non eccedenti rispetto alle finalità per le quali vengono raccolti o in ogni modo trattati; (e) essere conservati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario per gli scopi che hanno giustificato la raccolta.

La legge prevede, poi, eccezioni per alcuni trattamenti posti in essere, in ambito pubblico, in particolare a favore di attività inerenti la pubblica sicurezza, la difesa e la giustizia. In tali casi è previsto solo il rispetto di alcune cautele particolari.

Infine, importante novità introdotta dalla legge n. 675 del 1996 è la costituzione del Garante per la protezione dei dati personali, una nuova autorità amministrativa indipendente creata proprio per vigilare sulla corretta applicazione della normativa in materia di protezione della riservatezza. Tra i suoi numerosi compiti si possono ricordare: (a) quelli di vigilanza, controllo e monitoraggio sull'attuazione della legge (in particolare va ricordato che presso l'autorità garante è tenuto un registro dei trattamenti che vengono compiuti sul territorio nazionale, e delle

relative modalità, sulla base delle notificazioni ricevute); (b) quelli di carattere normativo (poi implementati dal decreto legislativo 26 febbraio 1999, n. 51); (c) quelli di carattere consultivo e propulsivo (soprattutto nei confronti del governo); (d) quelli inerenti la risoluzione dei contenziosi, esercitabili su segnalazione o reclamo degli interessati; (e) quelli ispettivi, inibitori e sanzionatori; (f) quelli autorizzatori.

## 4. Gli ulteriori interventi normativi interni

L'approvazione della legge n. 675 del 1996 pose l'Italia all'avanguardia in Europa nella tutela della riservatezza, ma sollevò altresì il problema di come riuscire a calare tale normativa in una realtà culturale sino a quel momento lasciata sostanzialmente all'oscuro delle problematiche inerenti la privacy. Inoltre, la necessità di disciplinare la materia in tempi ristretti, per consentire la tempestiva entrata in vigore anche nel nostro paese dell'Accordo di Schengen, comportò, come conseguenza, la redazione di un testo normativo complesso e non sempre organico in tutte le sue previsioni.

Proprio per poter far fronte a questi limiti strutturali, e a quelli che sarebbero potuti derivare dall'applicazione della legge, il Parlamento decise - come si è già ricordato - di affiancare alla disciplina principale una legge delega (la legge n. 676 del 1996) con la quale il governo venne incaricato di adottare uno o più decreti legislativi a contenuto integrativo o correttivo della normativa principale. Il termine originariamente previsto per l'adozione dei decreti venne prorogato (dalla legge 6 ottobre 1998, n. 344, dalla legge 24 marzo 2001, n. 127, dalla legge 1 marzo 2005, n. 26, dalla legge 23 febbraio 2006, n. 51 e, in ultimo, dalla legge 12 luglio 2006, n. 228) fino a consentire l'adozione dell'attuale decreto legislativo n. 196 del 2003 (sul quale si veda il capitolo successivo).

Modesti interventi correttivi in ordine alle procedure da seguire, all'applicazione della normativa in ambito pubblico, all'organizzazione degli uffici del Garante, ai trattamenti effettuati nell'ambito della ricerca scientifica e al trattamento dei dati sensibili in ambito sanitario furono adottati con il decreto legislativo 9 maggio

1997, n. 123 (Disposizioni correttive ed integrative della legge 31 dicembre 1996, n. 675 in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali), con il decreto legislativo 28 luglio 1997, n. 255 (Disposizioni in materia di notificazione dei trattamenti di dati personali integrative e correttive della legge 31 dicembre 1996, n. 675), con il decreto legislativo 8 maggio 1998, n. 135 (Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici), con il decreto legislativo 6 novembre 1998, n. 389 (Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici), con il decreto legislativo 26 febbraio 1999, n. 51 (Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675, concernenti il personale dell'ufficio del Garante per la protezione dei dati personali), con il decreto legislativo 30 luglio 1999, n. 281 (Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica), con il decreto legislativo 30 luglio 1999, n. 282 (Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario).

Di maggiore rilievo risultò il decreto legislativo 13 maggio 1998, n. 171 (Disposizioni di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica): ad esso si deve infatti l'introduzione di disposizioni sul trattamento dei dati in ambito giornalistico e, soprattutto, della più recente normativa comunitaria in materia di protezione della vita privata nel settore delle telecomunicazioni.

Oltre a questa ricca attività di produzione normativa di livello primario occorre ancora ricordare la normativa di attuazione adottata tramite fonte regolamentare, che ha avuto per protagonisti principali il governo, l'Autorità Garante e la Presidenza del Consiglio dei Ministri. In particolare, merita un cenno il regolamento adottato con decreto del Presidente della Repubblica 31 marzo 1998, n. 501 relativo all'organizzazione e al funzionamento dell'ufficio del Garante.

## 5. Ulteriori elaborazioni normative e giurisprudenziali

Parallelamente alla ricordata attività legislativa svolta dal legislatore italiano, anche in ambito europeo la materia inerente la tutela della riservatezza ha continuato a essere oggetto di costante interesse.

Particolarmente importante, a questo riguardo, è stato il processo di elaborazione della Carta di Nizza sui diritti fondamentali nell'Unione europea, che introduce una rilevante distinzione concettuale tra profilo negativo e profilo positivo della tutela della riservatezza. E infatti, accanto all'articolo 7, che disciplina, secondo la concezione tradizionale, la tutela della privacy dal punto di vista negativo, come diritto a essere protetti dalle molestie altrui, si colloca l'articolo 8, che riconosce il diritto all'autodeterminazione informativa, introducendo il profilo positivo del controllo da parte del cittadino sui dati che lo riguardano.

A favorire l'introduzione dell'art. 8 fu anche l'attività giurisdizionale della Corte europea che, attraverso una serie di pronunce, interpretò il concetto di vita privata in modo estensivo, coprendo non solo l'integrità fisica e morale, ma anche il diritto a stringere e sviluppare (e, di conseguenza, anche a non stringere e non sviluppare) relazioni con i propri simili nel mondo esterno.

Questa stessa impostazione sulla scindibilità del diritto alla riservatezza in un profilo positivo e in uno negativo è, d'altro canto, riscontrabile nell'atteggiamento in materia della Corte costituzionale italiana. In proposito, non essendo il diritto alla privacy previsto nella Costituzione italiana, la Corte ha dovuto individuarne il fondamento costituzionale attraverso la sua attività interpretativa, cosa avvenuta, in particolare attraverso le importanti sentenze n. 13 del 1997 e n. 332 del 2000, che hanno ricondotto il profilo negativo, quello della tutela contro le molestie, agli articoli 14 e 15 della Costituzione e il profilo positivo agli articoli 2, 13 e 23.

## 6. Il Consiglio regionale del Piemonte

Prima di concludere questa breve introduzione storica può essere utile tracciare un panorama schematico degli adempimenti attraverso i quali il Consiglio regionale del Piemonte ha progressivamente adattato la propria normativa e la propria organizzazione interna al quadro giuridico in materia di tutela della riservatezza.

In proposito, la novità maggiormente rilevante riguarda la decisione - assunta dall'Ufficio di Presidenza del Consiglio regionale, con delibera n. 61/2006 del 27 aprile 2006 - di configurare il Consiglio regionale stesso, nella persona del suo Presidente, come «autonomo titolare del trattamento dei dati», in tal modo separando la titolarità consiliare da quella della Giunta (in precedenza, infatti, la titolarità del trattamento dei dati riservati era stata attribuita all'Ente Regione Piemonte nel suo complesso, nella persona del Presidente della Regione). La separazione è stata ritenuta maggiormente rispondente alla previsione normativa di cui all'articolo 29 del nuovo Statuto regionale, laddove è previsto che «il Consiglio regionale, nell'esercizio delle sue funzioni e nell'espletamento delle sue attività, ha autonomia funzionale, finanziaria, contabile, organizzativa, patrimoniale e negoziale».

Sulla base di questa decisione, il Presidente del Consiglio ha quindi provveduto a individuare i Direttori, e questi, a loro volta, i Dirigenti di Settore, quali responsabili del trattamento dei dati. I Dirigenti, dal canto loro, hanno portato a compimento gli adempimenti operando le nomine degli incaricati.

Dal punto di vista operativo, rilievo centrale assume il «Regolamento per il trattamento dei dati sensibili e giudiziari di competenza della Regione, delle Aziende sanitarie, degli Enti e Agenzie regionali, degli Enti vigilati dalla Regione», adottato con delibera del Consiglio regionale n. 65-15263 del 9 maggio 2006. Con questo atto il Consiglio regionale ha provveduto, in attuazione degli articoli 20 e 21 del codice della privacy, a identificare le tipologie di dati trattabili e le operazioni su di essi eseguibili da parte della Regione Piemonte, delle aziende sanitarie e degli altri organismi sanitari pubblici della Regione Piemonte, degli enti e agenzie regionali, e degli altri enti in relazione ai quali la Regione esercita poteri di indirizzo e di controllo, ivi compresi gli enti che fanno riferimento a due o più regioni. In particolare, il regolamento individua e disciplina:

- 33 trattamenti di competenza della Giunta regionale, e di enti strumentali o ausiliari o comunque vigilati dalla Regione Piemonte;
- 41 trattamenti di competenza delle aziende sanitarie e degli altri organismi sanitari pubblici della Regione Piemonte;
- 14 trattamenti di competenza del Consiglio regionale del Piemonte.

Per quanto riguarda questi ultimi, il regolamento indica il Consiglio regionale come titolare in materia di:

1) nomine e designazioni;
2) instaurazione e gestione del rapporto di lavoro del personale;
3) assicurazione rischi di morte, invalidità permanente e temporanea, dipendenti da infortunio o infermità, e assicurazione infortuni dei Consiglieri, ex Consiglieri e Assessori regionali;
4) A) anagrafe patrimoniale dei titolari di cariche elettive e di cariche direttive. B) Gestione economica, fiscale e previdenziale delle indennità, degli assegni vitalizi e delle reversibilità dei Consiglieri, ex Consiglieri e Assessori regionali;
5) attività di tutela amministrativa e giudiziaria;
6) difesa civica regionale;
7) strumenti di democrazia diretta (iniziativa legislativa popolare, petizioni e referendum);
8) attività politica, di indirizzo e di controllo - sindacato ispettivo;
9) verifica elettorato passivo e requisiti per l'esercizio del mandato;
10) riconoscimento inabilità totale e permanente al lavoro degli eletti alla carica di Consigliere regionale;
11) documentazione dell'attività istituzionale del Consiglio (o Assemblea legislativa) regionale e degli Organi consiliari (o assembleari);
12) insindacabilità dei Consiglieri regionali;
13) patrocinio legale - rimborso spese legali amministratori e dipendenti regionali per fatti e atti connessi all'espletamento del servizio o del mandato;
14) attività del Comitato regionale per le comunicazioni.

Per ciascuno dei trattamenti elencati il regolamento prevede la definizione delle fonti normative di riferimento, delle finalità del trattamento, della tipologia dei dati trattati,

delle modalità di trattamento dei dati, della tipologia delle operazioni eseguite, la compiuta descrizione del trattamento stesso e la ricostruzione del flusso informativo *ex ante* ed *ex post*.

Infine, per concludere questa breve panoramica sulla tutela della riservatezza nell'ambito delle attività e delle funzioni del Consiglio regionale, occorre ricordare i due adempimenti principali in tema di sicurezza: da un lato la disciplina in tema di videosorveglianza[3]; dall'altro l'adozione del «Documento programmatico sulla sicurezza»[4], adempimento annuale che costituisce il fondamento degli adempimenti assunti a protezione dell'organo consiliare.

[3] Si vedano, in proposito, le delibere dell'Ufficio di Presidenza n. 90/2005 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Provvedimenti in tema di videosorveglianza), n. 92/2006 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Provvedimenti in tema di videosorveglianza - Integrazione D.U.P. 20/06/2005, n. 90) e n. 35/2007 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Provvedimenti in tema di videosorveglianza).

[4] Si vedano, in argomento, le delibere dell'Ufficio di Presidenza n. 39/2006 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Approvazione del "Documento programmatico sulla sicurezza - Anno 2006") e n. 52/2007 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Approvazione del "Documento programmatico sulla sicurezza - Anno 2007").

# Capitolo 2

# Il decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali)

Il decreto legislativo n. 196/2003, entrato in vigore il 1° gennaio 2004, rappresenta il tentativo di comporre in maniera organica le innumerevoli disposizioni relative, anche in via indiretta, alla privacy, riunisce in unico contesto la legge n. 675/1996 e gli altri decreti legislativi, regolamenti e codici deontologici che si sono succeduti in questi anni e contiene anche importanti innovazioni tenendo conto della "giurisprudenza" del Garante e della direttiva Ue 2000/58 sulla riservatezza nelle comunicazioni elettroniche. Con il Codice si è cercato di assemblare in unico testo di rango primario tutte le disposizioni non solo legislative, ma anche regolamentari in materia di protezione dei dati personali, perseguendo il fine di disciplinare in maniera unitaria una materia, la privacy, che interessa tutti i settori pubblici e privati.

Alcuni autori[5] si sono chiesti se fosse stato preferibile, da parte del legislatore, utilizzare, piuttosto che la denominazione "codice" quella di "testo unico" per indicare una raccolta di tutta la normativa vigente in materia che si è stratificata nel tempo, a partire dal 1996, anno di adozione della legge n. 675. Comunque si preferisca qualificarlo, il d.lgs. n. 196/2003 costituisce un provvedimento di assoluta rilevanza, teso a riordinare un settore interessato da una fortissima evoluzione e da una notevolissima rilevanza sociale.

Finalità del Codice, oltre alla razionalizzazione delle norme esistenti e alla semplificazione degli adempimenti, è stata l'introduzione di nuove garanzie per i cittadini.

Il decreto legislativo n. 196/2003 è suddiviso in tre parti:

- La **parte I**, contenente le **"Disposizioni generali"**.

[5] G. Buttarelli, *Profili generali del trattamento dei dati personali*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 61-92.
L'autore osserva come «*di fronte ad un testo normativo come il decreto legislativo n. 196 del 2003, è innanzitutto legittimo chiedersi se la denominazione stessa di 'Codice' sia giustificata e se l'intervento di razionalizzazione che esso opera sia solo di facciata, oppure anche di sistema*».

- La **parte II**, concernente le **"Disposizioni relative ai singoli settori"**.

- La **parte III**, relativa alla **"Tutela dell'interessato e sanzioni"**.

## 1. Parte I - "Disposizioni generali"

La prima parte è dedicata alle disposizioni generali, riordinate in modo tale da affrontare tutti gli adempimenti e le regole del trattamento con riferimento ai settori pubblico e privato e comprende gli articoli da 1 a 45 raccolti in sette titoli.

Si tratta quindi di disposizioni valide per il trattamento di tutti i dati, da parte di soggetti pubblici e privati, nell'esercizio di qualsiasi attività.

- **Il titolo I**

contiene i **"Principi generali"**.

Si segnalano, in particolare, l'articolo 1 (Diritto alla protezione dei dati personali), che sancisce per chiunque il diritto alla protezione dei dati personali che lo riguardano e l'articolo 4 (Definizioni) che contiene numerosissime definizioni, da quella di trattamento a quella di dato personale, da quella di comunicazione elettronica a quella di scopi storici, statistici e scientifici.

Si riporta il testo dell'art. 4 (Definizioni)[6]:

«1. Ai fini del presente codice si intende per:

a) "**trattamento**", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

[6] Per una breve illustrazione delle definizioni si veda *sopra* il capitolo 1

b) “**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;

c) “**dati identificativi**”, i dati personali che permettono l'identificazione diretta dell'interessato;

d) “**dati sensibili**”, i dati personali idonei a rivelare l'origine razziale ed 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;

e) “**dati giudiziari**”, i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

f) “**titolare**”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) “**responsabile**”, la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) “**incaricati**”, le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) “**interessato**”, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) “**comunicazione**”, il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio

dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) "**diffusione**", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) "**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "**blocco**", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "**banca di dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) "**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

a) "**comunicazione elettronica**", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) "**chiamata**", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "**reti di comunicazione elettronica**", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) “**rete pubblica di comunicazioni**”, una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) “**servizio di comunicazione elettronica**”, i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7marzo 2002;

f) “**abbonato**”, qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) “**utente**”, qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) “**dati relativi al traffico**”, qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) “**dati relativi all'ubicazione**”, ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) “**servizio a valore aggiunto**”, il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) “**posta elettronica**”, messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

a) "**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) "**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) "**profilo di autorizzazione**", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) "**sistema di autorizzazione**", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

a) "**scopi storici**", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "**scopi statistici**", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) "**scopi scientifici**", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore».

- **Il titolo II**

disciplina i **"Diritti dell'interessato"**, soprattutto il diritto dell'interessato ad ottenere la conferma o meno di dati personali che lo riguardano e la loro comunicazione.

- **Il titolo III**

riguarda le **"Regole generali per il trattamento dei dati"** e si articola in tre capi.

- ✓ Il **capo I** è relativo alle **"Regole per tutti i trattamenti"**: si evidenziano le disposizioni sulle modalità del trattamento e sui requisiti dei dati, sui codici di deontologia e buona condotta, sull'informativa e sui danni cagionati per effetto del trattamento.
- ✓ Il **capo II** disciplina le **"Regole ulteriori per i soggetti pubblici"**. Si sottolinea che l'articolo 18, comma 2, prevede che "qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali".
- ✓ Il **capo III** contiene **"Regole ulteriori per privati ed enti pubblici economici"**. L'articolo 23, comma 1, vincola il trattamento di dati personali da parte di privati o di enti pubblici economici al consenso espresso dell'interessato. L'articolo 24 elenca una serie di ipotesi (ulteriori rispetto ai casi previsti nella parte II) per le quali il consenso non è richiesto.

- Il **titolo IV**

è relativo ai **"Soggetti che effettuano il trattamento"**, con disposizioni su titolare, responsabile ed incaricati del trattamento.

- Il **titolo V**

è dedicato alla **"Sicurezza dei dati e dei sistemi"** e si articola nei:

- ✓ **capo I "Misure di sicurezza"**
- ✓ **capo II "Misure minime di sicurezza"**

- Il **titolo VI**

concerne gli **"Adempimenti"**, dettando regole sulla notificazione del trattamento, sugli obblighi di comunicazione e sulle autorizzazioni.

- Il **titolo VII**

disciplina i **"Trasferimenti dei dati all'estero"**

## 2. Parte II - "Disposizioni relative ai singoli settori"

La seconda (articoli da 46 a 140) è la parte speciale dedicata a specifici settori.

In questa parte vengono analizzati specifici settori di attività per i quali il Codice prevede, in ragione della particolarità degli stessi, una disciplina apposita.

Questa sezione, oltre a disciplinare aspetti in parte inediti (informazione giuridica, notificazioni di atti giudiziari, dati sui comportamenti debitori), completa anche la disciplina attesa da tempo per il settore degli organismi sanitari e quella dei controlli sui lavoratori.

Si articola nei seguenti tredici titoli:

- **Titolo I**

è dedicato ai **"Trattamenti in ambito giudiziario[7]"**

  - ✓ **Capo I – "Profili generali"**
  - ✓ **Capo II – "Minori"**
  - ✓ **Capo III – "Informatica giuridica"**

- **Titolo II**

è dedicato ai **"Trattamenti da parte di forze di polizia"**

  - ✓ **Capo I – "Profili generali"**

- **Titolo III**

è dedicato alla **"Difesa e sicurezza dello stato"**

  - ✓ **Capo I – "Profili generali"**

- **Titolo IV**

è dedicato ai **"Trattamenti in ambito pubblico"**

  - ✓ **Capo I – "Accesso a documenti amministrativi"**

[7] Rispetto al passato, con il Codice, vengono meglio garantiti i diritti della personalità delle parti. E' prevista anche la possibilità che l'interessato possa chiedere, nel processo, di apporre sulla sentenza un'annotazione con la quale si avvisa che, in caso di pubblicazione del verdetto su riviste giuridiche o su supporti elettronici o di diffusione telematica, debbano essere omessi i dati dell'interessato. I dati vanno sempre omessi se si tratta di minori.
Con disposizione espressa si attribuisce maggiore tutela ai minori non solo nel processo penale, ma anche nei procedimenti civili e amministrativi.

- ✓ **Capo II – "Registri pubblici e albi professionali"**
- ✓ **Capo III – "Stato civile, anagrafi e liste elettorali"**
- ✓ **Capo IV –" Finalità di rilevante interesse pubblico"**
- ✓ **Capo V – "Particolari contrassegni"**

- **Titolo V**

è dedicato al **"Trattamento di dati personali in ambito sanitario[8]"**

- ✓ **Capo I – "Principi generali"**
- ✓ **Capo II – "Modalità semplificate per informativa e consenso"**
- ✓ **Capo III – "Finalità di rilevante interesse pubblico"**
- ✓ **Capo IV – "Prescrizioni mediche"**
- ✓ **Capo V – "Dati genetici"**
- ✓ **Capo VI – "Disposizioni varie"**

- **Titolo VI**

è dedicato all' **"Istruzione"**

- ✓ **Capo I – "Profili generali"**

- **Titolo VII**

è dedicato al **"Trattamento per scopi storici, statistici o scientifici"**

- ✓ **Capo I – "Profili generali"**

[8] In ambito sanitario il Codice semplifica l'informativa da rilasciare agli interessati e consente di manifestare il necessario consenso al trattamento dei dati con un'unica dichiarazione resa al medico di famiglia o all'organismo sanitario (il consenso vale anche per la pluralità di trattamenti a fini di salute erogati da distinti reparti e unità dello stesso organismo, nonché da più strutture ospedaliere e territoriali).
Per il settore sanitario vengono inoltre codificate misure per il rispetto dei diritti del paziente: distanze di cortesia, modalità per appelli in sale di attesa, certezze e cautele nelle informazioni telefoniche e nelle informazioni sui ricoverati, estensione delle esigenze di riservatezza anche agli operatori sanitari non tenuti al segreto professionali.
Vengono introdotte (a partire dal 1 gennaio 2005) le cosiddette ricette impersonali, la possibilità cioè di non rendere sempre e in ogni caso immediatamente identificabili in farmacia gli intestatari di ricette attraverso un tagliando predisposto su carta copiativa che, oscurando il nome e l'indirizzo dell'assistito, consente comunque la visione di tali dati da parte del farmacista nei casi in cui sia necessario.
Per i dati genetici viene previsto il rilascio di un'apposita autorizzazione da parte del Garante, sentito il Ministro della salute.
Per quanto riguarda le cartelle cliniche sono previste particolari misure per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati (comprese le informazioni relative ai nascituri), ma anche specifiche cautele per il rilascio delle cartelle cliniche a persone diverse dall'interessato.

- ✓ **Capo II – "Trattamento per scopi storici"**
- ✓ **Capo III – "Trattamento per scopi statistici o scientifici"**

- **Titolo VIII**

è dedicato al **"Lavoro e previdenza sociale[9]"**

- ✓ **Capo I – "Profili generali"**
- ✓ **Capo II – "Annunci di lavoro e dati riguardanti prestatori di lavoro"**
- ✓ **Capo III – "Divieto di controllo a distanza e telelavoro"**
- ✓ **Capo IV – "Istituti di patronato e di assistenza sociale"**

- **Titolo IX**

è dedicato al **"Sistema bancario, finanziario ed assicurativo"**

- ✓ **Capo I – "Sistemi informativi"**

- **Titolo X**

è dedicato alle **"Comunicazioni elettroniche[10]"**

---

[9] Viene confermata l'elaborazione di un codice di deontologia e buona condotta che dovrà fissare regole per l'informativa ed il consenso anche degli annunci per finalità di occupazione (selezione del personale) e della ricezione dei curricula.
Il Codice affronta anche la questione dei controlli a distanza con la riaffermazione di quanto sancito dall'articolo 4 dello Statuto dei lavoratori (legge 300/1970). Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

[10] Con il Codice i cittadini possono meglio scegliere se essere inseriti nell'elenco telefonico o le modalità con le quali comparire sull'elenco: possono decidere, in particolare, se far usare i loro numeri telefonici e indirizzi anche per informazioni commerciali o solo per comunicazioni interpersonali.
Vengono previste misure per combattere il fenomeno delle chiamate di disturbo.
Le chiamate di disturbo sono telefonate, spesso effettuate negli orari meno opportuni, con le quali vengono proposte offerte commerciali, con continui disturbi alla vita privata dei cittadini.
Si riporta il testo dell'articolo 127 del Codice.
«Art. 127. Chiamate di disturbo e di emergenza
1. L'abbonato che riceve chiamate di disturbo può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.
2. La richiesta formulata per iscritto dall'abbonato specifica le modalità di ricezione delle chiamate di disturbo e nel caso in cui sia preceduta da una richiesta telefonica è inoltrata entro quarantotto ore.
3. I dati conservati ai sensi del comma 1 possono essere comunicati all'abbonato che dichiari di utilizzarli per esclusive finalità di tutela rispetto a chiamate di disturbo. Per i servizi di cui al comma 1 il fornitore assicura procedure trasparenti nei confronti degli abbonati e può richiedere un contributo spese non superiore ai costi effettivamente sopportati
4. Il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predispone procedure trasparenti per garantire, linea per linea, l'inefficacia della

- ✓ **Capo I – "Servizi di comunicazione elettronica"**
- ✓ **Capo II – "Internet e reti telematiche"**
- ✓ **Capo III – "Videosorveglianza"**

- **Titolo XI**

è dedicato alle **"Libere professioni e investigazione privata"**

- ✓ **Capo I – "Profili generali"**

- **Titolo XII**

è dedicato al **"Giornalismo ed espressione letteraria ed artistica"**

- ✓ **Capo I – "Profili generali"**
- ✓ **Capo II – "Codice di deontologia"**

- **Titolo XIII**

è dedicato al **"Marketing diretto"**

- ✓ **Capo I – "Profili generali"**

## 3. Parte III - "Tutela dell'interessato e sanzioni"

La parte terza (articoli da 141 a 186) affronta la materia delle tutele amministrative e giurisdizionali con il consolidamento delle sanzioni amministrative e penali e con le disposizioni relative all'Ufficio del Garante.

Si articola nei seguenti titoli:

- **Titolo I**

---

soppressione dell'identificazione della linea chiamante, nonché, ove necessario, il trattamento dei dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. I servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorità per le garanzie nelle comunicazioni.
Il Codice conferma il diritto a ricevere, su richiesta, fatture dettagliate (con le ultime tre cifre "in chiaro") in caso di contestazione».

è dedicato alla **"Tutela amministrativa e giurisdizionale"**

- ✓ **Capo I – "Tutela dinanzi al garante"** (Sezione I - Principi generali Sezione II - Tutela amministrativa Sezione III - Tutela alternativa a quella giurisdizionale)
- ✓ **Capo II – "Tutela giurisdizionale"**

- **Titolo II**

è dedicato a **"L'autorità"**

- ✓ **Capo I – "Il Garante per la protezione dei dati personali"**
- ✓ **Capo II – "L'ufficio del Garante"**
- ✓ **Capo III – "Accertamenti e controlli"**

- **Titolo III**

è dedicato alle **"Sanzioni[11]"**

- ✓ **Capo I – "Violazioni amministrative"**
- ✓ **Capo II – "Illeciti penali"**

- **Titolo IV**

è dedicato alle **"Disposizioni modificative, abrogative, transitorie e finali"**

- ✓ **Capo I – "Disposizioni di modifica"**
- ✓ **Capo II – "Disposizioni transitorie"**
- ✓ **Capo III – "Abrogazioni"**
- ✓ **Capo IV – "Norme finali"**

[11] Per quanto concerne le sanzioni, con il Codice sia le sanzioni pecuniarie sia quelle penali sono aumentate per chi viola la privacy, in particolare per l'uso dei dati senza consenso degli interessati, per il mancato adempimento nei confronti di un provvedimento del Garante, per la mancata informativa agli interessati sull'uso che si intende fare dei dati che li riguardano.

# Capitolo 3

# Le regole per i soggetti pubblici

Per quanto riguarda i soggetti pubblici[12] si osserva quanto segue:

- Le disposizioni contenute nella parte I del Codice sono, come accennato, disposizioni generali, che riguardano la posizione dell'interessato a prescindere dal soggetto titolare del trattamento, sia esso privato oppure pubblico.

- Le disposizioni del capo II della parte I "Regole ulteriori per i soggetti pubblici" contengono disposizioni specifiche sul trattamento dei dati da parte dei soggetti pubblici in generale.

- Nella parte II del Codice, infine, vi sono disposizioni specifiche per particolari settori (trattamenti in ambito giudiziario, trattamenti da parte di forze di polizia, ecc.).

- Alcuni chiarimenti sono contenuti nella Direttiva ministeriale 11 febbraio 2005, n. 1/2005 "Misure finalizzate all'attuazione nelle pubbliche amministrazioni delle disposizioni contenute nel d.lgs. 30 giugno 2003, n. 196, recante Codice in materia di protezione dei dati personali, con particolare riguardo alla gestione delle risorse umane"[13].

[12] Per un'analisi approfondita delle regole applicabili ai soggetti pubblici si rinvia a C. Zucchelli, *Regole generali per il trattamento dei dati nelle amministrazioni pubbliche*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 93-129.

[13] Il testo della direttiva è consultabile sul sito del Garante (www.garanteprivacy.it).

## 1. Articolo 18

Come già accennato l'art. 18, dopo aver escluso dall'ambito dei destinatari delle disposizioni gli enti pubblici economici (art. 18, comma 1), afferma che:

- qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali (art. 18, comma 2). Il trattamento è quindi proibito salvo che per lo svolgimento delle funzioni istituzionali.

- Nel trattare i dati personali il soggetto pubblico osserva i presupposti e i limiti stabiliti dal Codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti (art. 18, comma 3).

- Salvo quanto previsto nella parte II del Codice per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato (art. 18, comma 4)[14].

- Ai trattamenti effettuati da soggetti pubblici si applicano i divieti di comunicazione e diffusione dei dati previsti dall'art. 25 per i trattamenti effettuati dai soggetti privati (art. 18, comma 5).

## 2. Articolo 19

L'art. 19 contiene i principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari.

[14] L'art. 23, comma 1, stabilisce invece che «Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato».

- Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2 (trattamento consentito per lo svolgimento delle funzioni istituzionali), anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente (art. 19, comma 1).
  Salvo i casi dei dati sensibili e giudiziari non è quindi necessaria una norma specifica che autorizzi il trattamento.

- La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata (art. 19, comma 2).

Tale disposizione va quindi coordinata con quanto previsto dall’art. 39 (Obblighi di comunicazione). Nel caso in cui le amministrazioni abbiano necessità di fornire tali informazioni ad un'altra pubblica amministrazione, sempre ai fini dello svolgimento delle attività istituzionali, ma in assenza di idonea previsione normativa, possono informarne preventivamente il Garante, ai sensi dell'art. 39 del Codice. In base a tale nuovo meccanismo, decorsi quarantacinque giorni dalla comunicazione al Garante, l'operazione di comunicazione dei dati può essere avviata, ferma restando la possibilità di una diversa determinazione dell'Autorità adottata anche successivamente al decorso del termine.

Si rileva, infine, che deve essere effettuata una preventiva comunicazione al Garante, a norma dell'art. 39, anche nel caso di trattamento di dati idonei a rivelare lo stato di salute previsto da un programma di ricerca biomedica o sanitaria, conformemente a quanto dispone l'art. 110 del Codice.

Quindi, a differenza della comunicazione fra privati che, seppure sottoposta a regole, è libera, la comunicazione fra soggetti pubblici è vietata in linea di principio, salvo che sia prevista da una norma di legge o di regolamento o quando è comunque necessaria per lo svolgimento di funzioni istituzionali.

- La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento (art. 19, comma 3).

Con l'art. 19 finiscono le regole ulteriori per i soggetti pubblici in materia di dati diversi da quelli sensibili e giudiziari: gli articoli 20, 21 e 22 sono invece espressamente dedicati a questi ultimi. Prima di passare all'analisi di tali disposizioni è però importante evidenziare come la scelta di collegare, per le pubbliche amministrazioni, il trattamento dei dati personali con l'esercizio delle funzioni istituzionali ha conseguenze sul piano della responsabilità e delle sanzioni.

Infatti un trattamento dei dati effettuato al di fuori delle funzioni istituzionali comporta l'obbligo di risarcimento del danno al privato per quanto concerne versante civile, nonché le sanzioni amministrative e penali previste nella parte III del Codice.

## 3. Articolo 20

L'art. 20 enuncia i principi applicabili al trattamento di dati sensibili e prevede, innanzitutto, che il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge. E' quindi necessaria un'espressa autorizzazione legislativa (art. 20, comma 1) nella quale siano specificati:

- i tipi di dati che possono essere trattati;
- le operazioni eseguibili;
- le finalità di rilevante interesse pubblico perseguite.

Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili (art. 20, comma 2), il trattamento è consentito con atto di natura regolamentare (adottato in

conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo):

- solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento;

- in relazione alle specifiche finalità perseguite nei singoli casi;

- nel rispetto dei principi di cui all'articolo 22.

Riassumendo, l' articolo 20, comma 2 del Codice, come anche il successivo articolo 21, comma 2, prevede che, quando una disposizione di legge abbia specificato le finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari che possono essere trattati e le operazioni che possono essere svolte su di essi, le amministrazioni dovranno adottare un apposito regolamento con il quale identificare e rendere pubblici, a cura dei soggetti che ne effettuano il trattamento, i tipi di dati utilizzabili e le operazioni eseguibili, in relazione ai fini istituzionali perseguiti e nel rispetto dei principi affermati dall'art. 22 del Codice[15]. L'adozione di tali provvedimenti postula la previa ricognizione di tutte le attività poste in essere dal soggetto pubblico che comportano un trattamento di dati sensibili o giudiziari, nonché la valutazione della indispensabilità dei dati utilizzati e delle operazioni svolte nell'ambito di tali attività rispetto alle finalità di volta in volta perseguite. I dati trattati vanno indicati per categorie (ad esempio, dati sulla salute, vita sessuale, sull'origine razziale, sull'origine etnica, ecc.), tenendo conto che le tipologie di dati non individuate nel regolamento non potranno essere trattate.

In altri termini, tramite tali regolamenti dovrà risultare chiaro ai cittadini il collegamento tra le finalità di rilevante interesse pubblico perseguite dalle amministrazioni in relazione ai compiti ad esse attribuiti dall'ordinamento e le modalità con cui vengono effettivamente utilizzate le informazioni che li riguardano. Al fine di dare efficacia al sistema di garanzie delineato dal Codice per i dati sensibili

[15] Si segnala il provvedimento del Garante del 30 giugno 2005 "Trattamento dei dati sensibili nella pubblica amministrazione", consultabile sul sito internet del Garante (http://www.garanteprivacy.it/garante/doc.jsp?ID=1144445).

e giudiziari è pertanto necessario che le amministrazioni provvedano a tale identificazione, ove mancante, tramite atti di natura regolamentare. L'identificazione dei tipi di dati e di operazioni è poi aggiornata e integrata periodicamente, come indicato dal successivo art. 20, comma 4, del Codice[16].

Per rendere più agevole e rapida l'adozione di tali atti, il Codice prevede che il parere del Garante possa essere formulato anche su schemi tipo. Nel caso in cui gli schemi regolamentari predisposti dalle amministrazioni corrispondano ai modelli su cui il Garante ha reso un parere conforme, non sarà quindi necessario sottoporli caso per caso allo specifico esame da parte dell'Autorità.

Se il trattamento non è previsto espressamente da una disposizione di legge (art. 20, comma 3) i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili.

In tal caso, il trattamento è consentito soltanto se l'amministrazione interessata provveda altresì ad identificare e rendere pubblici i tipi di dati utilizzabili e le operazioni eseguibili con un atto di natura regolamentare

Molte amministrazioni hanno adottato provvedimenti in attuazione a quanto previsto dal presente comma.

L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente (art. 20, comma 4).

[16] Per quanto riguarda la Regione Piemonte, come già accennato, con decreto del Presidente della Giunta Regionale 11 maggio 2006, n. 3/R è stato adottato il regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie Regionali, degli Enti vigilati dalla Regione (Articoli 20 e 21 del decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali), pubblicato sul Supplemento Ordinario n. 3 al B.U. n. 19 dell'11 maggio 2006.
L'allegato C di tale regolamento contiene l' "Elenco trattamenti dei dati sensibili e giudiziari di competenza del Consiglio regionale, degli Organi consiliari e loro membri", riportato nella parte relativa alla documentazione.

## 4. Articolo 21

L’art. 21**,** sui principi applicabili al trattamento di dati giudiziari, prevede per questi una disciplina analoga a quella dell’art. 20 sui dati sensibili.

Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (art. 21, comma 1).

Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari (art. 21, comma 2).

## 5. Articolo 22

L’art. 22 enuncia ulteriori principi applicabili al trattamento di dati sensibili e giudiziari.

- Innanzitutto le pubbliche amministrazioni devono prestare particolare attenzione alla prevenzione di possibili danni per l’interessato: i soggetti pubblici sono tenuti infatti a conformare il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato (art. 22, comma 1).

- Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari (art. 22, comma 2).

- Di particolare rilievo la previsione del principio di indispensabilità, secondo il quale i soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere

adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa (art. 22, comma 3).

- I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato (art. 22, comma 4).

- In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti (art. 22, comma 5).

- I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità (art. 22, comma 6).

- I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6

anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici (art. 22, comma 7).

- I dati idonei a rivelare lo stato di salute non possono essere diffusi (art. 22, comma 8).

- Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi (art. 22, comma 9).

- I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi (art. 22, comma 10).

- In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge (art. 22, comma 11).

- Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale (art. 22, comma 12).

# Capitolo 4
# Le misure di sicurezza

Le misure di sicurezza sono disciplinate dal titolo V della parte I del Codice (articoli 31-36[17]) e sono costituite dal complesso delle misure organizzative, tecniche, informatiche, logistiche e procedurali volte a ridurre al minimo i rischi di:

- distruzione o perdita, anche accidentale, dei dati;
- accesso non autorizzato;
- trattamento non consentito o non conforme alle finalità della raccolta[18].

Il Codice, in conformità con la scelta già effettuata con la legge n. 675/1996 e con le indicazioni contenute nella direttiva 95/46/CE[19], prevede la distinzione fra:

- misure di sicurezza idonee e preventive;
- misure minime di sicurezza.

[17] Le definizioni sono contenute nell'articolo 4, 3° comma, del Codice.
[18] Questo elenco è interpretabile in modo estensivo ed in particolare alla formula "trattamento non consentito" "deve riconoscersi il valore di clausola di chiusura, con la quale si individua, con ampia definizione, qualunque trattamento che, comunque, risulti non conforme alla disciplina in materia di protezione dei dati personali per ragioni diverse da quelle corrispondenti alle altre tipologie di rischi individuate all'art. 31", come osserva P. Troiano, *Le misure di sicurezza*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 167-222, al quale si rinvia per un approfondimento del tema delle misure di sicurezza.
[19] In particolare, l'articolo 17 della direttiva 95/46/CE prevede che: «Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali. Tali misure devono garantire, tenuto conto delle attuali conoscenze in materia e dei costi dell'applicazione, un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere».

L'elemento che differenzia le due tipologie di misure è il diverso regime di responsabilità nel caso di omissione: l'omessa adozione di misure idonee e preventive può comportare la responsabilità civile ai sensi dell'articolo 15 del Codice per danno cagionato per effetto del trattamento[20], mentre per la mancata adozione delle misure minime di sicurezza scatta anche la responsabilità penale, prevedendo infatti il Codice, all'articolo 169, il reato di omessa adozione di misure di sicurezza.

A differenza delle misure minime di sicurezza, le misure preventive e idonee non possono essere predeterminate in modo preciso: l'articolo 31 del Codice evidenzia che i dati personali sono custoditi e controllati:

- anche in relazione alle conoscenze acquisite in base al progresso tecnico;
- alla natura dei dati;
- alle specifiche caratteristiche del trattamento.

L'articolo 32 del Codice si riferisce alla misure di sicurezza con riguardo ai trattamenti effettuati dal fornitore di un servizio di comunicazione elettronica accessibile al pubblico, il quale deve adottare, ai sensi dell'articolo 31, idonee misure tecniche e organizzative adeguate al rischio esistente per salvaguardare:

- la sicurezza dei suoi servizi;

[20] Con parere 22 marzo 2004 avente ad oggetto "*Prima applicazione del Codice in materia di protezione dei dati personali in materia di "misure minime" di sicurezza (artt. 31-36 e Allegato B) al d.lgs. n. 196/2003)*", il Garante ha osservato che «Occorre custodire e controllare i dati personali oggetto di trattamento per contenere nella misura più ampia possibile il rischio che i dati siano distrutti, dispersi anche accidentalmente, conoscibili fuori dei casi consentiti o altrimenti trattati in modo illecito. Resta in vigore, oltre alle cosiddette "misure minime", l'obbligo di adottare ogni altra misura di sicurezza idonea a fronteggiare le predette evenienze, avuto riguardo alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle caratteristiche del trattamento, di cui si devono valutare comunque i rischi (art. 31).
Come in passato, l'inosservanza di questo obbligo rende il trattamento illecito anche se non si determina un danno per gli interessati; viola inoltre i loro diritti, compreso il diritto fondamentale alla protezione dei dati personali che può essere esercitato nei confronti del titolare del trattamento (artt. 1 e 7, comma 3, del Codice), ed espone a responsabilità civile per danno anche non patrimoniale qualora, davanti al giudice ordinario, non si dimostri di aver adottato tutte le misure idonee ad evitarlo (artt. 15 e 152 del Codice)».

- l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni.

Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

## 1. Le misure minime di sicurezza

Le misure minime di sicurezza sono definite dall'articolo 4, terzo comma, lett. a) del Codice come il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31, cioè quelli, già citati nel precedente paragrafo, di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta.

Il Codice dedica alla disciplina delle misure minime di sicurezza il capo II del titolo V (articoli da 33 a 36).

L'allegato B al Codice contiene il Disciplinare tecnico in materia di misure minime di sicurezza, cioè l'insieme delle regole tecniche che il titolare, il responsabile ove designato e l'incaricato, devono adottare, a garanzia della sicurezza, in caso di trattamento con strumenti elettronici nonché di trattamento senza l'ausilio degli stessi[21].

[21] Il Disciplinare tecnico può essere consultato sul sito del Garante: www.garanteprivacy.it

Il disciplinare tecnico di cui all'allegato B) è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

Le **misure minime di sicurezza per il trattamento di dati personali effettuato con strumenti elettronici**[22] sono regolamentate dall'articolo 34 del Codice e dai paragrafi da 1 a 26 del Disciplinare tecnico.

L'articolo 34 del Codice stabilisce che il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;
b) adozione di procedure di gestione delle credenziali di autenticazione;
c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi[23];
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

L'autenticazione informatica è definita dal Codice come l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità (articolo 4, terzo comma, lettera c).

Il disciplinare tecnico prevede, per quanto concerne l'autenticazione informatica, che siano legittimati al trattamento di dati personali con strumenti

[22] Il Codice, all'articolo 4, terzo comma, prevede che per "strumenti elettronici"si intendono gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.
[23] Per le misure minime elencate dalla lettera d) alla lettera f) si rinvia alla lettura dei paragrafi 15, 16, 17 e 18 del Disciplinare.

elettronici gli incaricati dotati di credenziali di autenticazione[24] che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Le credenziali di autenticazione consistono:

- in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo;

- oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave;

- oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Secondo il disposto dell'articolo 4, terzo comma, lettera e), la "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, è costituita da una sequenza di caratteri o altri dati in forma elettronica.

Il Disciplinare tecnico specifica che la parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non deve contenere riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

Qualora l'accesso ai dati da parte dei singoli incaricati debba avvenire in modo selettivo, "consentendosi a ciascuno incaricato o gruppo di incaricati di accedere solo ad una parte dei dati personali complessivamente trattati o di compiere solo alcune

[24] "Credenziali di autenticazione", sono i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica (articolo 4, comma 3, lettera d) del Codice).

delle operazioni di trattamento previste"[25], il sistema di autenticazione informatica deve essere integrato da un "sistema di autorizzazione".

Il "sistema di autorizzazione" è l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione[26] del richiedente (articolo 4, terzo comma, lett. g) del Codice).

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento e periodicamente, comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Il disciplinare esclude, infine, l'applicazione delle disposizioni sul sistema di autenticazione e di quelle sul sistema di autorizzazione ai trattamenti dei dati personali destinati alla diffusone.

**2. Documento programmatico sulla sicurezza**.

La principale misura prescritta per i trattamenti di dati sensibili o di dati giudiziari è costituita dalla tenuta del documento programmatico sulla sicurezza[27].

Il Disciplinare prescrive che entro il 31 marzo di ogni anno[28], il titolare di un trattamento di dati sensibili o di dati giudiziari rediga, anche attraverso il responsabile,

[25] P. Troiano, *op. cit.*, pagg. 205 ss. L'autore fa l'esempio dei dati relativi al personale qualora possano essere trattati solo dai dipendenti assegnati al servizio competente per la gestione del personale e del caso in cui tutti gli incaricati possono registrare i dati, ma solo alcuni sono legittimati a cancellarli.

[26] Il "profilo di autorizzazione"è l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti (articolo 4, terzo comma, lett. f) del Codice).

[27] L'articolo 34, primo comma, lettera g) del Codice, prevede l'adozione di tale documento per tutti i trattamenti con strumenti elettronici, ma il Disciplinare tecnico si riferisce invece solamente al trattamento di dati sensibili e giudiziari effettuato con strumenti elettronici.
Per le ulteriori misure in caso di trattamento di dati sensibili o giudiziari nonché per le misure di tutela e garanzia si rinvia alla lettura dei paragrafi dal 20 al 26 del Disciplinare.

[28] Per quanto riguarda la Regione Piemonte si segnalano, per l'anno 2007, il decreto del Presidente della Giunta regionale 29 marzo 2007 n. 19 avente ad oggetto "D.Lgs. n. 196/2003 "Codice in materia di protezione dei dati personali", Allegato B. Adozione del Documento Programmatico sulla Sicurezza per le Strutture della Giunta della Regione Piemonte" e le delibere dell'Ufficio di Presidenza del

se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

- l'elenco dei trattamenti di dati personali;

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

- l'analisi dei rischi che incombono sui dati;

- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento[29];

- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

---

Consiglio regionale n. 39/2006 (D.Lgs. 30/6/2003, n. 196 “Codice in materia di protezione dei dati personali”. Approvazione del “Documento programmatico sulla sicurezza - Anno 2006”) e n. 52/2007 (D.Lgs. 30/6/2003, n. 196 “Codice in materia di protezione dei dati personali”. Approvazione del “Documento programmatico sulla sicurezza - Anno 2007”).

[29] Si rinvia alla lettura del paragrafo 23 del Disciplinare.

- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale[30], l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Le **misure minime di sicurezza per il trattamento di dati personali senza l'ausilio di strumenti elettronici** sono previste dall'articolo 35 del Codice e nei paragrafi 27, 28 e 29 del Disciplinare.

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione;

- previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate;

- previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata

[30] Si rinvia ala lettura del paragrafo 24 del Disciplinare.

all'identificazione degli incaricati. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono devono essere preventivamente autorizzate.

## 3. Il reato di omessa adozione di misure di sicurezza

L'omessa adozione da parte di chi, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 (misure minime) è punita (articolo 169 del Codice) con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro[31].

[31] Per l'analisi più dettagliata di tale contravvenzione si rinvia al capitolo relativo alla "Tutela dell'interessato nel trattamento dei dati personali".

# Capitolo 5
# La tutela della riservatezza nel rapporto di lavoro pubblico

Il rapporto di lavoro è forse uno dei primi ambiti in cui si pose il problema della tutela della riservatezza. Intrinseca alla posizione del datore di lavoro è, infatti, l'esigenza di esercitare un potere di controllo sulle attività compiute dal lavoratore nello svolgimento delle sue mansioni. Ma, d'altro canto, si pone la contrapposta esigenza che il potere di controllo del datore di lavoro venga esercitato nel rispetto della libertà e della dignità del dipendente assoggettato a tale potere. Di qui, fin dalla legge 20 maggio 1970, n. 300 (Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attività sindacale nel luoghi di lavoro e norme sul collocamento) - meglio nota come "Statuto dei lavoratori" - il riconoscimento del potere di controllo del datore di lavoro, ma con la contestuale introduzione di una serie di limitazioni relative ai casi di esercitabilità e alle procedure cui attenersi.

Lo Statuto dei lavoratori si preoccupava, in particolare, di vietare ogni indagine sulle opinioni politiche, religiose e sindacali dei lavoratori, nonché su ogni circostanza non attinente alla valutazione della loro attitudine professionale, essendo già ben evidente la violazione della sfera di autonomia individuale che sarebbe potuta derivare da indagini su tali oggetti. In questo senso - e limitatamente a quest'ambito - lo Statuto dei lavoratori può a ragione essere considerato precursore dell'attuale normativa in materia di tutela della riservatezza.

In linea generale, il trattamento dei dati personali da parte dei datori di lavoro pubblici è attualmente disciplinato con il fine di assicurare un livello elevato di tutela dei diritti e delle libertà fondamentali, in conformità con i principi di semplificazione, armonizzazione ed efficacia, sia per le modalità di esercizio dei diritti, sia per l'adempimento degli obblighi da parte dei titolari del trattamento. Dal canto loro, i lavoratori hanno diritto di ottenere che il trattamento dei dati sia effettuato nel rispetto dei ricordati diritti e libertà.

Il vigente codice in materia di trattamento dei dati personali disciplina la privacy nei rapporti di lavoro nella Parte II (Disposizioni relative a specifici settori), Titolo VIII (Lavoro e previdenza sociale), nel quale rientrano gli articoli dal 111 al

116. Altre disposizioni applicabili al tema qui trattato sono peraltro rinvenibili in diversi ulteriori articoli del codice, e in particolare nel Titolo X (Comunicazioni elettroniche), laddove viene disciplinato l'uso della posta elettronica, di internet e l'adozione di sistemi di videosorveglianza. Ma anche la raccolta di dati nei fascicoli personali dei lavoratori, e in particolari dei dati di carattere sanitario, rientrano a pieno titolo nel tema relativo alla privacy nei rapporti di lavoro.

L'intreccio normativo in materia ha recentemente portato l'Autorità garante per la protezione dei dati personali ad adottare tre deliberazioni volte a chiarire il quadro complessivo, contenenti, rispettivamente: (a) le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati (deliberazione n. 53 del 23 novembre 2006); (b) le Linee guida del Garante per posta elettronica e internet (deliberazione n. 13 del 1° marzo 2007); (c) le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (deliberazione n. 23 del 14 giugno 2007).

## 1. Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico (deliberazione n. 23 del 14 giugno 2007)

Le recenti linee guida in materia di privacy e pubblico impiego consentono di gettare uno sguardo d'insieme sull'argomento.

In sintesi, le principali novità contenute nel provvedimento sono le seguenti:

- assenze per malattia, certificati e visite mediche: in caso di assenza per malattia all'amministrazione vanno consegnati certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio deve astenersi dall'utilizzare queste informazioni e deve invitare il personale a non produrre altri certificati con le stesse

caratteristiche. Particolari cautele devono essere adottate dall'ente pubblico quando tratta dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio, abilitazioni al porto d'armi e alla guida;

- diffusione dei dati in internet: le amministrazioni devono assicurare l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete e garantire il cosiddetto «diritto all'oblio» (trascorso un certo periodo dalla pubblicazione è opportuno spostare i nominativi in un parte del sito dove non siano più rintracciabili dai motori di ricerca esterni). Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali, no a recapiti telefonici, codice fiscale ecc.). È sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati;

- dati biometrici dei lavoratori pubblici: non è, di regola, consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride, DNA) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare l'attivazione di tali sistemi di rilevazione solo in presenza di particolari esigenze (per esempio: aree adibite alla sicurezza dello Stato, conservazione di oggetti di particolare valore) e, in ogni caso, nel rispetto di precise garanzie (verifica preliminare dell'Autorità, divieto di archivi centralizzati, codice cifrato dell'impronta memorizzato solo nel badge del dipendente);

- comunicazioni tra amministrazione e lavoratore: per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione deve adottare forme di comunicazione con il dipendente protette e individualizzate: inoltrando le note in busta chiusa, inviandole all'indirizzo di posta elettronica personale o invitandolo a ritirare personalmente la documentazione.

## 2. Quadro generale

Regola di fondo in materia è che il datore di lavoro pubblico può lecitamente trattare dati personali dei lavoratori nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro, e avendo cura di operare secondo modalità di trattamento proporzionate agli scopi perseguiti.

Quanto alle modalità, il Codice in materia di protezione dei dati personali prescrive che il trattamento di dati personali per la gestione del rapporto di lavoro avvenga:

- rispettando i principi di necessità, di liceità e di qualità dei dati (artt. 3 e 11);

- attenendosi alle funzioni istituzionali e applicando i presupposti e i limiti previsti da leggi e regolamenti rilevanti per il trattamento, in particolare in materia di pubblico impiego (art. 18);

- dando applicazione effettiva e concreta al principio di indispensabilità nel trattamento dei dati sensibili e giudiziari, il quale vieta di trattare informazioni o di effettuare operazioni che non siano realmente indispensabili per raggiungere determinate finalità previste specificamente (artt. 4, comma 1, lettere d) ed e), 22, commi 3, 5 e 9, e 112);

- limitando il trattamento di dati sensibili e giudiziari alle sole informazioni ed operazioni di trattamento individuate e rese pubbliche con l'atto regolamentare adottato in conformità al parere del Garante (artt. 20, 21, 112 e 154);

- informando preventivamente e adeguatamente gli interessati (art. 13);

- adottando adeguate misure di sicurezza, idonee a preservare i dati da alcuni eventi tra cui accessi ed utilizzazioni indebiti, rispetto ai quali l'amministrazione può essere chiamata a rispondere civilmente e i pubblici funzionari anche penalmente (artt. 15 e 31 e ss.).

Per quel che invece attiene alle finalità, il trattamento dei dati personali, anche sensibili, dei lavoratori deve essere orientato all'esclusivo o prevalente scopo di adempiere agli obblighi e ai compiti in materia di rapporto di lavoro e di impiego alle dipendenze delle amministrazioni pubbliche. Tali obblighi e compiti sono disciplinati, oltre che da leggi e regolamenti, anche dai contratti collettivi (nazionali e integrativi), nei quali sono contenute previsioni che permettono di trattare lecitamente informazioni di natura personale (ad esempio, per determinare il trattamento economico fondamentale ed accessorio, per fruire di permessi o di aspettative sindacali, per accedere a qualifiche, per la mobilità o per la responsabilità disciplinare).

Il trattamento effettuato dal soggetto pubblico deve attenersi a queste disposizioni e restare compatibile con le finalità per le quali i dati sono stati inizialmente raccolti o già trattati (art. 11, comma 1, lett. b).

Particolare attenzione deve essere posta alle disposizioni dei contratti collettivi che prevedono la conoscenza di dati da parte di organizzazioni sindacali, avendo cura che il doveroso rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione che comportano la comunicazione di informazioni alle medesime organizzazioni avvenga nel rispetto dei principi di necessità e proporzionalità.

Naturalmente, in linea con i principi generali della materia, è sempre necessario che il datore di lavoro individui preliminarmente i diversi soggetti autorizzati a trattare i dati (titolare, responsabili, incaricati), definendo chiaramente le rispettive attribuzioni (artt. 4, comma 1, lett. f), g) e h), 28, 29 e 30). In particolare, le amministrazioni devono disciplinare le modalità del trattamento, designando gli eventuali soggetti responsabili e, in ogni caso, le persone fisiche incaricate che possono acquisire lecitamente conoscenza dei dati inerenti alla gestione del rapporto di lavoro, attenendosi alle funzioni svolte e a idonee istruzioni scritte (artt. 4, comma 1, lett. g) e h), 29 e 30).

Quanto ai casi in cui si deve procedere alla comunicazione di dati personali, al di là delle ipotesi in cui specifiche previsioni normative disciplinano forme e modalità della divulgazione (art. 174, comma 12, del codice), l'amministrazione deve utilizzare forme di comunicazione individualizzata con il lavoratore, adottando le misure più opportune per prevenire la conoscibilità ingiustificata di dati personali, in particolare se sensibili, da parte di soggetti diversi dal destinatario, ivi compresi gli incaricati di operazioni di trattamento (per esempio, inoltrando le comunicazioni in plico chiuso, invitando l'interessato a ritirare personalmente la documentazione presso l'ufficio competente, ricorrendo a comunicazioni telematiche individuali).

Venendo più al dettaglio delle questioni riconducibili alla tutela della riservatezza nell'ambito del pubblico impiego, possono essere utilmente distinti sei ambiti principali: (a) le comunicazioni elettroniche; (b) i dati biometrici; (c) il fascicolo personale del lavoratore; (d) i dati sanitari; (e) i dati raccolti nello svolgimento delle attività preposte alla tutela dell'integrità psico-fisica del lavoratore; (f) i dati idonei a rivelare le convinzioni religiose.

## 3. Le comunicazioni elettroniche

Un primo aspetto specifico rilevante della tutela della riservatezza nell'ambito del rapporto di lavoro è quello relativo all'utilizzo della posta elettronica e di internet da parte dei dipendenti.

In proposito, la regola fondamentale, più volte ribadita dal Garante attraverso i propri atti, è il divieto, se non in casi eccezionali, di effettuare controlli che grava sul datore di lavoro. La questione è ritenuta di particolare delicatezza, dal momento che da un'eventuale analisi dei siti web visitati dalle persone si possono trarre informazioni, anche sensibili, su interessi e preferenze delle persone, per non dire del contenuto di carattere privato che possono avere le comunicazioni effettuate tramite posta elettronica.

Naturalmente questo non significa che il lavoratore abbia il diritto di utilizzare a proprio piacimento e senza alcuna limitazione gli strumenti informatici: spetta però

al datore di lavoro di informare con chiarezza e in modo dettagliato i lavoratori – attraverso l'adozione di un disciplinare interno da definirsi con il coinvolgimento delle rappresentanze sindacali, che deve essere adeguatamente pubblicizzato e tenuto costantemente aggiornato – sulle modalità di utilizzo di internet e della posta elettronica, nonché sulla possibilità che vengano effettuati controlli.

Oltre ad indicare le regole di impiego, il datore di lavoro è inoltre chiamato ad adottare ogni misura idonea a prevenire il rischio di utilizzi impropri degli strumenti informatici da parte dei dipendenti, così da ridurre la possibilità che si rendano necessari controlli successivi.

Per quanto riguarda internet è, in particolare, opportuno:

- che siano preventivamente individuati i siti considerati correlati o meno con la prestazione lavorativa svolta dai dipendenti;

- che sia prevista l'utilizzazione di filtri idonei a prevenire determinate operazioni non consentite, quali l'accesso a siti inseriti in una c.d. «black list» o il download di file ritenuti non idonei (per esempio file musicali o multimediali).

Riguardo, invece, alla posta elettronica, si richiede al datore di lavoro di:

- rendere disponibili indirizzi condivisi tra più lavoratori (per es. info@ente.it; urp@ente.it; ufficioreclami@ente.it, ecc.), rendendo così chiara la natura non privata della corrispondenza indirizzata a tali caselle di posta;

- valutare la possibilità di attribuire al lavoratore un indirizzo ulteriore rispetto a quello di lavoro, affinché possa destinarlo all'utilizzo personale;

- prevedere, in caso di assenza del lavoratore, messaggi di risposta automatica che indichino a quali colleghi è possibile rivolgersi al posto dell'assente;

- consentire al dipendente di delegare un collega di sua fiducia il compito di verificare il contenuto dei messaggi a lui indirizzati in modo che questi possa inoltrare al responsabile dell'ufficio quelli risultanti di rilievo per l'attività lavorativa in caso di assenza prolungata o non prevista del lavoratore interessato e di improrogabili necessità legate all'attività lavorativa stessa.

Qualora, poi, le misure preventive sopra ricordate dovessero risultare insufficienti a evitare comportamenti anomali, il datore di lavoro è tenuto a effettuare gli eventuali controlli necessari ispirandosi a un criterio di gradualità: ogni verifica dovrà venire effettuata a partire dalla più ampia unità di afferenza del lavoratore (nel caso del Consiglio regionale del Piemonte: la Direzione), per poi passare ai livelli via via successivi (sempre nel caso del Consiglio regionale: Settore, Ufficio, eventuale gruppo di lavoro) e solo infine, se non è stato possibile procedendo in tal modo individuare l'area da richiamare all'osservanza delle regole, sarà possibile, di fronte al ripetersi dell'anomalia, passare a effettuare controlli su base individuale.

Quanto ai controlli, questi sono possibili se ricondotti al principio generale secondo il quale il datore di lavoro può, nel perseguimento di finalità determinate, esplicite e legittime, controllare l'effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro da parte del dipendente. Sempre in ottemperanza ai principi generali sanciti dalla legislazione in materia di rapporto di lavoro, resta comunque ferma la necessità di rispettare le procedure di informazione e consultazione di lavoratori e sindacati in relazione ai controlli effettuati e, in ogni caso, il datore di lavoro è chiamato ad adottare ogni misura volta a prevenire il rischio di utilizzi impropri dei dati raccolti attraverso i controlli e a minimizzare, per quanto possibile, l'uso di dati direttamente riferibili ai singoli lavoratori (per esempio i sistemi *software* devono essere programmati e configurati in modo tale da cancellare periodicamente ed automaticamente i dati personali relativi al traffico telematico la cui conservazione non risulti necessaria). Restano comunque sempre vietati la lettura e la registrazione sistematica delle e-mail e anche il monitoraggio sistematico delle pagine web visualizzate dal lavoratore (in entrambi i

casi si configurerebbero ipotesi di controllo a distanza dell'attività lavorativa in contrasto con le previsioni dello Statuto dei lavoratori).

Sempre in tema di comunicazioni elettroniche, si segnala il pericolo che comunicazioni destinate a un interlocutore precisamente individuato possano essere da questi, anche inavvertitamente, trasmesse a terzi, senza il consenso del mittente. Si tratta di un'ipotesi particolarmente delicata perché da tale comportamento potrebbero scaturire responsabilità di natura non solo civilistica, ma anche penalistica. Da un lato, la persona che ha inviato il messaggio potrebbe subire un danno se il contenuto della comunicazione viene portato a conoscenza di persone diverse da quelle cui il messaggio era stato indirizzato; dall'altro, la trasmissione a terzi di una comunicazione personale senza il consenso del mittente potrebbe configurare il reato di violazione di corrispondenza punito ai sensi dell'articolo 616, comma 2, del codice penale.

Al fine di avvertire del pericolo sopra indicato, il Garante per la privacy ha suggerito di inserire nelle comunicazioni inviate attraverso la posta elettronica un avviso sulla natura personale o non personale del messaggio, precisando se il contenuto possa o meno essere portato a conoscenza di soggetti diversi dal destinatario. Potrebbe inoltre essere opportuno evidenziare il rischio di un utilizzo fraudolento dell'indirizzo di posta elettronica del mittente da parte di terzi (o dell'impiego di indirizzi simili e ingannevoli), nonché la possibilità che il contenuto del messaggio sia da ricondurre alla responsabilità dello specifico mittente e non della struttura presso la quale egli è impiegato[32].

I profili della questione rimangono comunque non perfettamente definiti, dal momento che parte della dottrina e della giurisprudenza segnalano come lo strumento informatico sia, per sua stessa natura, non pienamente idoneo a garantire la riservatezza delle comunicazioni.

[32] Una formula di avvertenza, da inserire in calce alle e-mail, potrebbe essere la seguente:
«Questo documento e gli eventuali allegati contengono informazioni la cui lettura e il cui utilizzo sono riservati unicamente al destinatario. Se il ricevente non è il destinatario del messaggio, si prega di non utilizzarne il contenuto e di non portarlo a conoscenza di alcuno, nonché di voler cortesemente contattare i seguenti indirizzi di posta elettronica: …
Nel caso di utilizzo non autorizzato, il mittente si riserva di dar corso alle azioni più opportune a tutela dei propri diritti in sede civile e penale.
Si invita a tenere presente che le attuali tecnologie non consentono di garantire l'autenticità del mittente né l'intergità del contenuto del messaggio.
Le informazioni contenute nel messaggio possono rappresentare opinioni personali, a meno di diversa esplicita indicazione».

Per un approfondimento in argomento è possibile consultare le «Linee guida del Garante per posta elettronica e internet» adottate dal Garante con deliberazione n. 13 del 1° marzo 2007.

## 4. I dati biometrici

Sotto il profilo della tutela della privacy, i dati biometrici che vengono in rilievo sono quelli utilizzabili per procedere all'identificazione delle persone, quali, in particolare, la registrazione delle impronte digitali, la lettura dell'iride, la mappatura del contorno della mano, fino al trattamento del DNA.

La regola generale è che l'impiego di sistemi biometrici non è lecito se non è proporzionato agli scopi che si intendono raggiungere, in particolare nei casi in cui ciò comporta la creazione di archivi centralizzati. Le informazioni in quest'ambito archiviabili sono infatti particolarmente delicate e il loro uso può comportare rischi legati all'utilizzazione indebita delle informazioni desunte dalle tracce fisiche che una persona può lasciare anche senza rendersene conto.

Nell'ambito del rapporto di impiego, dove i sistemi biometrici potrebbero essere utilizzati soprattutto per registrare la presenza dei dipendenti sul luogo di lavoro, il Garante ha stabilito che non è consentito l'utilizzo generalizzato di tali sistemi, specie se rivolti a ricavare dati dalle impronte digitali. I principi generali che regolano la materia della privacy, impongono a ciascuna amministrazione titolare del trattamento di accertare se la finalità del controllo della presenza dei dipendenti possa essere realizzata senza fare ricorso alla raccolta di dati biometrici o, perlomeno, evitando ogni eccesso nel loro utilizzo che ne comporti un trattamento sproporzionato. Deve quindi essere preventivamente valutata l'idoneità di altri sistemi che possano egualmente assicurare una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro. Di regola, non è pertanto consentito il trattamento di dati relativi alle impronte digitali per accertare le ore di lavoro prestate effettivamente dal personale dislocato anche in sedi distaccate o addetto a servizi esterni.

Sistemi di rilevazione di impronte digitali nel luogo di lavoro possono essere lecitamente attivati soltanto per far fronte a particolari esigenze di controllo legate all'accesso a speciali aree dei luoghi di lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza. Per esempio: per lo svolgimento di attività aventi carattere di particolare segretezza o per la conservazione di oggetti di particolare valore o la cui disponibilità deve essere ristretta ad un numero circoscritto di dipendenti in quanto un loro utilizzo improprio può determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi.

In tali casi eccezionali, il trattamento di dati relativi alle impronte digitali è ammesso a condizione che:

- sia preliminarmente autorizzato dal Garante;

- sia fornita agli interessati un'adeguata informativa sul trattamento in questione;

- non venga registrata l'immagine integrale dell'impronta digitale, ma solo il modello matematico di riferimento ricavato da questa;

- tale modello non sia archiviato in una memoria centralizzata, bensì in un supporto posto nell'esclusiva disponibilità dell'interessato (smart card o dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale).

In un caso sottoposto alla sua valutazione, il Garante ha autorizzato, con particolari cautele, l'uso dei dati ricavati dalla conformazione della mano per accedere ad un complesso nel quale sono presenti imprese che lavorano e vendono metalli e pietre preziose. Non potrà però essere creato un archivio centralizzato dei dati biometrici, ma l'impronta cifrata della mano dovrà essere memorizzata solo sul badge del lavoratore o del personale autorizzato all'ingresso (sulla smart card sarà riportato il codice cifrato della mano e il profilo di autorizzazione personale – fascia oraria e

giorni consentiti per l'ingresso – mentre non saranno riportati foto e dei dati anagrafici della persona autorizzata all'ingresso, sostituiti da un codice identificativo individuale perché ritenuto più sicuro in caso di smarrimento). I dati relativi agli accessi dovranno essere cancellati automaticamente dopo sette giorni e, inoltre, dovrà essere comunque garantito un sistema alternativo di accesso. In un'altra circostanza il Garante ha utilizzato il trattamento dei dati biometrici, ma limitatamente allo stretto periodo di tempo necessario a far fronte a specifiche esigenze di sicurezza.

In un ulteriore caso l'Autorità Garante ha vietato il trattamento dei dati biometrici a un'industria del settore costruzioni, che intendeva utilizzare le impronte per controllare gli orari di ingresso e uscita dei propri dipendenti dai luoghi di lavoro. Il Garante, accertata l'esistenza di molti altri sistemi altrettanto rigorosi per controllare gli ingressi nei luoghi di lavoro, senza che venisse messa a rischio la dignità stessa dei lavoratori interessati, ha quindi precisato che l'uso generalizzato e incontrollato di dati biometrici dei lavoratori non è in linea di principio lecito, in particolare quando si tratta di impronte digitali le quali, per la loro particolare natura, impongono che siano prevenuti eventuali utilizzi impropri, nonché ogni possibile abuso.

Quanto alle amministrazioni pubbliche, il Garante è intervenuto in due casi, vietando l'utilizzo di sistemi idonei a rilevare dati biometrici per controllare gli accessi degli studenti in una mensa universitaria e per controllare la presenza sul lavoro dei dipendenti di una biblioteca comunale. Più in generale, il Provvedimento del Garante del 14 giugno 2007 «Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico»precisa, al punto 7 dedicato a «Impronte digitali e accesso al luogo di lavoro» che il principio di necessità impone a ciascuna amministrazione titolare del trattamento di accertare se la finalità perseguita possa essere realizzata senza dati biometrici ed evitando ogni eccesso nel loro utilizzo che ne comporti un trattamento sproporzionato. Ciò comporta la necessità di valutare preventivamente altri sistemi, dispositivi e misure di sicurezza, fisiche e logicistiche, che possano assicurare una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro. Resta in particolare privo di giuridico fondamento l'utilizzo di sistemi di rilevazione delle impronte digitali per verificare l'esatto adempimento di prestazioni lavorative, ove siano attivabili misure «convenzionali» non lesive dei diritti della persona quali, per

esempio, l'apposizione di firme anche in presenza di eventuale personale incaricato, l'uso di fogli di presenza o di sistemi di timbratura mediante badge magnetico.

Di regola, non è pertanto consentito il trattamento di dati relativi alle impronte digitali per accertare le ore di lavoro prestate effettivamente dal personale dislocato anche in sedi distaccate o addetto a servizi esterni, con riferimento, per esempio, all'esigenza di computare con sistemi oggettivi le turnazioni, l'orario flessibile, il recupero, i permessi, il lavoro straordinario, i buoni pasto, nonché di prevenire eventuali usi abusivi o dimenticanze del badge[33].

Infine, il Garante precisa che non può desumersi alcuna approvazione implicita dal semplice inoltro all'Autorità di note relative a progetti di installazione di impianti di rilevazione di impronte digitali ai quali non segua un esplicito riscontro, positivo o negativo, dell'Autorità.

[33] Il punto 7.2 delle «Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico» si sofferma anche su alcuni casi particolari: di regola, sistemi di rilevazione di impronte digitali nel luogo di lavoro possono essere quindi attivati soltanto per particolari esigenze di controllo dell'accesso a speciali aree dei luoghi di lavoro in cui si debbano assicurare elevati e specifici livelli di sicurezza, in relazione a specifiche necessità quali, ad esempio, la destinazione dell'area interessata:

1) allo svolgimento di attività aventi particolare carattere di segretezza, ovvero prestate da personale selezionato e impiegato in attività che comportano la necessità di trattare informazioni rigorosamente riservate (es. accesso a sale operative ove confluiscono segnalazioni afferenti alla sicurezza anticrimine; aree adibite ad attività inerenti alla difesa e alla sicurezza dello Stato; ambienti di torri di controllo aeroportuali);
2) alla conservazione di oggetti di particolare valore o la cui disponibilità deve essere ristretta ad un numero circoscritto di dipendenti in quanto un loro utilizzo improprio può determinare una grave e concreta situazione di rischio per la salute e l'incolumità degli stessi o di terzi (es. ambienti ove sono custodite sostanze stupefacenti o psicotrope).

Nelle ipotesi sopramenzionate il trattamento di dati relativi alle impronte digitali è ammesso a condizione che:

- sia sottoposto con esito positivo – di regola a seguito di un interpello del titolare (48) – alla verifica preliminare, che l'Autorità si riserva di effettuare ai sensi dell'art. 17 del Codice anche per determinate categorie di titolari o di trattamenti;
- venga effettuata preventivamente la notificazione al Garante (artt. 37, comma 1, lett. a) e 38 del Codice);
- non sia comunque registrata l'immagine integrale dell'impronta digitale, bensì solo il modello di riferimento da essa ricavato (template);
- tale modello non sia archiviato in una memoria centralizzata, bensì in un supporto posto nell'esclusiva disponibilità dell'interessato (smart card o dispositivo analogo) e privo di indicazioni nominative riferibili a quest'ultimo (essendo sufficiente attribuire a ciascun dipendente un codice individuale);
- sia fornita ai dipendenti interessati un'informativa specifica per il trattamento in questione (art. 13 del Codice).

## 5. Il fascicolo personale del lavoratore

Un altro aspetto della protezione dei dati personali sul luogo pubblico di lavoro che il Garante ha avuto occasione di approfondire è quello relativo alle informazioni contenute nel fascicolo personale dei singoli lavoratori.

Anche in questo ambito, coerentemente con l'impostazione generale della materia, le Pubbliche Amministrazioni sono chiamate a procedere adottando le più opportune cautele in tutti i casi in cui le informazioni personali da loro raccolte e detenute siano idonee a rivelare profili particolarmente delicati della vita privata dei propri dipendenti, quali specialmente la salute, le convinzioni politiche, sindacali, religiose, filosofiche o d'altro genere e l'origine razziale ed etnica.

In linea generale il datore di lavoro pubblico può utilizzare informazioni sensibili relative al proprio personale ai fini della instaurazione e gestione del rapporto di lavoro, ma si tenga presente che in numerose circostanze la normativa in materia prevede che vengano in rilievo informazioni che rivestono carattere di dato personale sensibile. Si pensi, per esempio, alla normativa sull'assunzione del personale che rientra nelle categorie protette, alla disciplina che tutela, anche sul versante delle assunzioni, le minoranze linguistiche o che comunque prevede la sussistenza di particolari requisiti per l'accesso a specifici impieghi, nonché a tutto ciò che attiene all'ambito previdenziale e assistenziale.

In tutti questi casi, ma più in generale in tutti i casi in cui vengano in rilievo dati sensibili e giudiziari, il datore di lavoro pubblico deve - oltre che attenersi strettamente al rispetto dei principi di necessità e di indispensabilità (che impongono di ridurre al minimo l'utilizzo di dati personali e, quando non si possa prescindere dall'uso di informazioni personali sensibili o giudiziarie, di trattare solo i dati e di svolgere solo le operazioni indispensabili) - conformare e limitare il trattamento alle operazioni individuate e rese pubbliche con l'atto regolamentare adottato in conformità alla normativa sulla privacy. Inoltre dovrà avvenire a cura del datore di lavoro la predisposizione di tutte le misure di sicurezza idonee a prevenire la possibile diffusione dei dati di cui la Pubblica Amministrazione è a conoscenza.

Dal canto suo, il lavoratore ha il diritto di accedere ai dati personali che lo riguardano e di ottenerne la comunicazione in forma completa e intelligibile, come è

stato riconosciuto dal Garante. Tale diritto di accesso ai propri dati non implica però la possibilità di venire a conoscenza di informazioni di carattere contrattuale o professionale (quali, ad esempio, gli accordi collettivi nazionali o aziendali) che non hanno natura di dati personali in qualche modo riferibili a persone identificate o identificabili. Inoltre il lavoratore non può chiedere l'inserimento di dati non presenti nell'archivio né che le informazioni vengano fornite sulla base di una rielaborazione personalizzata secondo i criteri da lui indicati.

## 6. I dati sanitari

In linea generale, la Pubblica Amministrazione può procedere al trattamento dei dati sanitari al fine di valutare l'idoneità al servizio o comunque allo svolgimento di un proficuo lavoro, procedere alle assunzioni relative alle categorie protette, accertare i casi di infermità che comportano un'incapacità lavorativa (temporanea o definitiva). I lavoratori e i candidati all'impiego devono considerare normale l'esecuzione di una visita medica per valutare l'attitudine allo svolgimento delle attività che saranno chiamati a ricoprire. Tuttavia, la visita medica non deve costituire un criterio di selezione, e deve essere effettuata solo dopo che la fase di selezione si è conclusa.

Trattandosi di un ambito particolarmente sensibile, nel trattare le informazioni in materia sanitaria l'amministrazione deve rispettare innanzitutto i principi di necessità e di indispensabilità, valutando specificamente il rapporto tra i dati sensibili sottoposti a trattamento e gli adempimenti derivanti da compiti e obblighi imposti dalla legge. È importante che le Pubbliche Amministrazioni valorizzino tali principi anche nell'applicare le disposizioni di servizio e i regolamenti interni precedenti alla disciplina in materia di protezione dei dati personali.

Quanto alle singole ipotesi nelle quali la Pubblica Amministrazione si può trovare a trattare dati sanitari dei propri dipendenti, nelle recenti linee guida sul rapporto di lavoro pubblico, il Garante per la privacy ha posto in particolare l'accento sui casi seguenti.

Il primo riguarda le assenze per ragioni di salute. Sulla base di quanto previsto dalla normativa sul rapporto di lavoro e dalle disposizioni contenute nei contratti collettivi, la Pubblica Amministrazione può, in linea generale, accertare i casi di infermità che comportano un'incapacità lavorativa e, a tal fine, il lavoratore è tenuto al rispetto di specifici obblighi volti a consentire al datore di lavoro di verificare lo stato delle sue condizioni di saluto, nel rispetto di quanto previsto dalla legge. In particolare, il dipendente deve fornire apposita documentazione a giustificazione dell'assenza, tramite la produzione di un certificato medico contenente la sola indicazione dell'inizio e della durata presunta dell'infermità (la prognosi); salvo diversa disposizione per specifiche figure professionali, il datore di lavoro pubblico non è legittimato infatti a raccogliere certificazioni mediche contenenti anche l'indicazione della diagnosi (al punto che qualora il lavoratore produca documentazione medica recante anche l'indicazione della diagnosi insieme a quella della prognosi, l'amministrazione deve astenersi dall'utilizzare ulteriormente tali informazioni, invitando anche il personale a non produrne altri con le medesime caratteristiche).

Anche riguardo all'esito delle visite di controllo sullo stato di infermità effettuate da medici dei servizi sanitari pubblici, il datore di lavoro pubblico è legittimato a conoscere i dati personali dei lavoratori riguardanti la capacità o l'incapacità al lavoro e la prognosi riscontrata, con esclusione di qualsiasi informazione attinente alla diagnosi. Questo non significa, naturalmente, che il datore di lavoro non possa, al fine di far valere i propri diritti in relazione a fenomeni di ritenuto assenteismo e di eventuale non veritiera certificazione sanitaria, redigere note informative, segnalazioni o denunce contenenti anche riferimenti circostanziati alle ragioni e alle modalità delle singole assenze.

Risulta inoltre giustificata, alla luce delle disposizioni contenute nei contratti collettivi, la conoscenza da parte dell'amministrazione di appartenenza di informazioni personali relative all'effettuazione di visite mediche, prestazioni specialistiche o accertamenti clinici, nonché alla presenza di patologie che richiedono terapie invalidanti, qualora il dipendente richieda di usufruire del trattamento di malattia o di permessi retribuiti per le assenze correlate a tali esigenze.

Il secondo ambito in merito al quale il Garante ha ritenuto opportuno richiamare l'attenzione è quello relativo agli obblighi di comunicazione relativi a dati sanitari che, in taluni casi, gravano sul datore di lavoro (in tal caso legittimato a venire a conoscenza delle condizioni di salute del lavoratore). Tra le fattispecie più ricorrenti va ricordata la denuncia all'istituto assicuratore (Inail) avente ad oggetto infortuni e malattie professionali occorsi ai lavoratori, denuncia che deve essere corredata da specifica certificazione medica.

In tali circostanze l'amministrazione, pur potendo conoscere la diagnosi, deve però comunicare all'ente assicurativo solo le informazioni sanitarie relative o collegate alla patologia denunciata, e non i dati sulla salute relativi ad altre assenze che si siano verificate nel corso del rapporto di lavoro (di fatto, devono essere evitate tutte le comunicazioni non rilevanti rispetto al caso oggetto di denuncia).

Il terzo caso su cui occorre soffermarsi è quello relativo alle visite medico-legali. In questo ambito le pubbliche amministrazioni possono trattare legittimamente dati idonei a rivelare lo stato di salute dei propri dipendenti, non solo per accertare, anche d'ufficio, attraverso le strutture sanitarie pubbliche competenti, la persistente idoneità al servizio, alle mansioni o allo svolgimento di un proficuo lavoro, ma anche per riconoscere la dipendenza di una patologia da causa di servizio, per concedere trattamenti pensionistici o di indennizzo ovvero per accertare, sempre per fini pensionistici, la sussistenza di stati invalidanti al servizio o di inabilità non dipendenti da causa di servizio. Nel disporre tali accertamenti le amministrazioni possono comunicare ai collegi medici competenti i dati personali sensibili del dipendente, dei quali dispongano, che siano indispensabili ai fini della valutazione dello stato di salute del dipendente. Nel fare ciò, la Pubblica Amministrazione deve operare in modo tale da prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

Analoghi accorgimenti devono essere adottati dagli organismi di accertamento sanitario all'atto sia della convocazione dell'interessato a visita medico-collegiale, sia della comunicazione dell'esito degli accertamenti effettuati all'amministrazione presso la quale presta servizio il lavoratore nonché, se necessario, all'interessato medesimo. In particolare, nel caso di accertamenti sanitari finalizzati ad accertare l'idoneità al servizio, alle mansioni o al proficuo lavoro del dipendente, i collegi

medici devono trasmettere all'amministrazione di appartenenza dell'interessato il relativo verbale di visita con la sola indicazione del giudizio medico-legale di idoneità, inidoneità o di forme di inabilità (anche in questo caso, qualora siano trasmessi dagli organismi di accertamento sanitario verbali recanti l'indicazione della diagnosi dell'infermità o della lesione che determinano un'incapacità lavorativa, i datori di lavoro non possono utilizzare ulteriormente tali informazioni).

Un'ulteriore ipotesi da trattare con adeguati accorgimenti – quarto caso – è quella relativa ai dati sulle abilitazioni al porto d'armi e alla guida. Di regola, le amministrazioni possono trattare i dati relativi agli esiti delle visite medico-legali cui sottopongono i propri dipendenti per consentire l'adozione da parte degli uffici competenti dei provvedimenti sull'arma di servizio, ove si tratti di agenti di pubblica sicurezza, abilitati al porto di pistola. La normativa di settore e le disposizioni contenute nei contratti collettivi non autorizzano, invece, le Pubbliche Amministrazioni a comunicare agli uffici competenti del Dipartimento per i trasporti terrestri informazioni idonee a rivelare lo stato di salute dei propri dipendenti, ancorché acquisite legittimamente, per consentire di verificare la persistenza in capo a questi ultimi dei requisiti fisici e psichici previsti dalla legge per il conseguimento della patente di guida.

Infine, altre circostanze nelle quali la Pubblica Amministrazione ha necessità di raccogliere dati relativi alla salute del lavoratore (e dei suoi congiunti) sono quelle nelle quali il lavoratore fa richiesta di godere di taluni benefici di legge, come per esempio le agevolazioni previste per l'assistenza a familiari disabili, ai permessi retribuiti e ai congedi per gravi motivi familiari. In occasione di istanze volte ad usufruire dei congedi a favore dei lavoratori con familiari disabili in situazione di gravità, l'amministrazione di appartenenza non deve venire a conoscenza di dati personali del congiunto portatore di handicap relativi alla diagnosi o all'anamnesi accertate dalle commissioni mediche a ciò preposte: è infatti sufficiente che il lavoratore presenti al datore di lavoro una certificazione dalla quale risulti esclusivamente la condizione di handicap grave accertata per opera delle competenti commissioni mediche. Al contrario, per usufruire di permessi o congedi per gravi infermità o altri gravi motivi familiari, il lavoratore è tenuto a produrre all'amministrazione idonea documentazione medica attestante le gravi infermità o le

gravi patologie da cui risultano affetti i propri familiari. Allo stesso modo, il datore di lavoro può venire a conoscenza dello stato di tossicodipendenza di un proprio dipendente o di un familiare di questi, in caso di richieste di accesso o concorso a programmi riabilitativi o terapeutici con conservazione del posto di lavoro (senza retribuzione): in questi casi è infatti necessario presentare specifica documentazione medica al datore di lavoro.

## 7. I dati raccolti nello svolgimento delle attività preposte alla tutela dell'integrità psico-fisica del lavoratore

Un'altro aspetto delicato con riferimento alla privacy nel rapporto di lavoro pubblico riguarda le attività che il datore di lavoro pubblico è chiamato a svolgere a tutela dell'integrità psico-fisica dei dipendenti. In proposito vengono in rilievo i trattamenti di dati che possono essere posti in essere dal medico competente in materia di igiene e sicurezza nei luoghi di lavoro preposto alla sorveglianza sanitaria obbligatoria. Un medico competente è chiamato a effettuare accertamenti preventivi e periodici sui lavoratori e istituisce, curandone l'aggiornamento, una cartella sanitaria e di rischio, che deve essere custodita presso l'amministrazione con salvaguardia del segreto professionale, e consegnata in copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro, ovvero quando lo stesso ne fa richiesta. È importante sottolineare che alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'efficace custodia nei locali dell'amministrazione; in caso di cessazione del rapporto di lavoro le cartelle sono trasmesse all'Istituto superiore prevenzione e sicurezza sul lavoro (Ispesl) in originale e in busta chiusa.

Il datore di lavoro pubblico è inoltre tenuto, su parere del medico competente o qualora quest'ultimo lo informi di anomalie imputabili all'esposizione a rischio, ad adottare le misure preventive e protettive per i lavoratori interessati; in questo specifico contesto il datore di lavoro può accedere al giudizio di idoneità del

lavoratore allo svolgimento di date mansioni, ma non al documento relativo alle specifiche patologie accertate.

Nello svolgimento della propria attività, il medico può farsi assistere da personale sanitario, anche dipendente dello stesso datore di lavoro pubblico, che deve essere designato quale incaricato del trattamento dei dati personali impartendo ad esso specifiche istruzioni per salvaguardare la segretezza delle informazioni trattate. In tal caso, a prescindere da quale sia il titolare del trattamento e dagli eventuali obblighi in tema di segreto d'ufficio, il medico competente deve predisporre misure idonee a garantire il rispetto del segreto professionale da parte dei propri collaboratori che non siano tenuti per legge al segreto professionale, mettendoli, tra l'altro, a conoscenza di tali disposizioni e delle relative sanzioni.

## 8. I dati idonei a rivelare le convinzioni religiose

Dati relativi alle convinzioni religiose dei dipendenti possono infine venire in rilievo, nel rapporto di lavoro, per consentire il diritto a rispettare i precetti rituali riconosciuto ai lavoratori appartenenti a determinate confessioni, in conformità alle disposizioni di legge e di regolamento che regolano i rapporti tra lo Stato e le varie confessioni.

Può sorgere la necessità di trattare dati sulle convinzioni religiose, in particolare, ai fini della concessione dei permessi per festività religiose su specifica richiesta dell'interessato, nonché per il rispetto di determinati dettami religiosi ai fini del servizio di mensa eventualmente apprestato presso il luogo di lavoro.

Una normativa peculiare (la legge 8 marzo 1989, n. 101) prevede, inoltre, che le prove, scritte e orali, dei concorsi per l'accesso al pubblico impiego non possono essere fissate nei giorni coincidenti con le festività religiose ebraiche e valdesi. Tale previsione rende ingiustificata la raccolta sistematica e preventiva dei dati relativi alle convinzioni religiose dei candidati, essendo sufficiente, per rispettare il credo religioso di tutti i possibili candidati, fissare le prove in giorni non coincidenti con dette festività.

# Capitolo 6
# La videosorveglianza

Le principali regole in materia di videosorveglianza sono contenute nel Provvedimento generale del Garante per la protezione dei dati personali del 29 aprile 2004[34].

Prima di questo provvedimento generale il Garante aveva già adottato, nel novembre 2000[35], delle prime linee guida con le quali si indicavano le regole per

[34] Il Provvedimento è consultabile sul sito del Garante per la protezione dei dati personali (www.garanteprivacy.it).

[35] Videosorveglianza - Il decalogo delle regole per non violare la privacy - 29 novembre 2000.
«Chi intende svolgere attività di videosorveglianza deve quindi osservare almeno le seguenti cautele, rispettando comunque il principio di proporzionalità tra mezzi impiegati e fini perseguiti:

1. Tutti gli interessati devono determinare esattamente le finalità perseguite attraverso la videosorveglianza e verificarne la liceità in base alle norme vigenti. Se l'attività è svolta in presenza di un pericolo concreto o per la prevenzione di specifici reati, occorre rispettare le competenze che le leggi assegnano per tali fini solo a determinate amministrazioni pubbliche, prevedendo che alle informazioni raccolte possano accedere solo queste amministrazioni.
2. Il trattamento dei dati deve avvenire secondo correttezza e per scopi determinati, espliciti e legittimi (art. 9, comma 1, lett. a) e b), legge 675/1996).
3. Nei casi in cui la legge impone la notificazione al Garante dei trattamenti di dati personali effettuati da determinati soggetti (art. 7 legge 675/1996), questi devono indicare fra le modalità di trattamento anche la raccolta di informazioni mediante apparecchiature di videosorveglianza. Non è prevista alcuna altra forma di specifica comunicazione o richiesta di autorizzazione al Garante.
4. Si devono fornire alle persone che possono essere riprese indicazioni chiare, anche se sintetiche, che avvertano della presenza di impianti di videosorveglianza, fornendo anche le informazioni necessarie ai sensi dell'art. 10 della legge n. 675/1996. Ciò è tanto più necessario quando le apparecchiature non siano immediatamente visibili.
5. Occorre rispettare scrupolosamente il divieto di controllo a distanza dei lavoratori e le precise garanzie previste al riguardo (art. 4 legge 300/1970).
6. Occorre rispettare i principi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando - quando non indispensabili - immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
7. Occorre determinare con precisione il periodo di eventuale conservazione delle immagini, prima della loro cancellazione, e prevedere la loro conservazione solo in relazione a illeciti che si siano verificati o a indagini delle autorità giudiziarie o di polizia.
8. Occorre designare per iscritto i soggetti - responsabili e incaricati del trattamento dei dati (artt. 8 e 19 della legge 675/1996) - che possono utilizzare gli impianti e prendere visione delle registrazioni, avendo cura che essi accedano ai soli dati personali strettamente necessari e vietando rigorosamente l'accesso di altri soggetti, salvo che si tratti di indagini giudiziarie o di polizia.
9. I dati raccolti per determinati fini (ad esempio, ragioni di sicurezza, tutela del patrimonio) non possono essere utilizzati per finalità diverse o ulteriori (ad esempio, pubblicità, analisi dei comportamenti di consumo), salvo le esigenze di polizia o di giustizia, e non possono essere diffusi o comunicati a terzi.

garantire che l'installazione di dispositivi per la videosorveglianza rispettasse le norme sulla privacy e sulla tutela della libertà delle persone, in particolare assicurando la proporzionalità tra mezzi impiegati e fini perseguiti.

Il Garante ha, inoltre, avviato le procedure per l'adozione di un codice deontologico e di buona condotta del settore che fissi regole precise e garanzie riguardo alla raccolta, all'uso e alla conservazione delle immagini rilevate attraverso videosorveglianza[36].

Il provvedimento del 29 aprile 2004 individua, al punto 2, quattro principi da osservare affinché la videosorveglianza sia legittima:

- principio di liceità
- principio di necessità
- principio di proporzionalità
- principio di finalità.

Per quanto riguarda il Consiglio regionale del Piemonte si segnalano le delibere dell'Ufficio di Presidenza n. 90/2005 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Provvedimenti in tema di videosorveglianza), n. 92/2006 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Provvedimenti in tema di videosorveglianza - Integrazione D.U.P. 20/06/2005, n. 90) e n. 35/2007 (D.Lgs. 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali". Provvedimenti in tema di videosorveglianza).

---

10. I particolari impianti per la rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato devono essere conformi anche alle disposizioni contenute nel d.p.r. 250/1999. E' altresì necessario che la relativa documentazione sia conservata per il solo periodo necessario per contestare le infrazioni e definire il relativo contenzioso e che ad essa si possa inoltre accedere solo a fini di indagine giudiziaria o di polizia».

[36] L'articolo 134 del Codice prevede espressamente che «Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11».

## 1. Principio di liceità

L'articolo 11, comma 1, lettera a) del Codice richiede che i dati personali oggetto di trattamento siano trattati in modo lecito e secondo correttezza.

Il trattamento dei dati attraverso sistemi di videosorveglianza è possibile solo se è fondato su uno dei presupposti di liceità.

Tali presupposti sono espressamente previsti dal Codice sia per gli organi pubblici (svolgimento di funzioni istituzionali: articoli 18-22) sia per soggetti privati e gli enti pubblici economici (adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" o consenso libero ed espresso: articoli 23-27).

La videosorveglianza deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati, di quanto prescritto da altre disposizioni di legge da osservare in caso di installazione di apparecchi audiovisivi. Vanno richiamate al riguardo le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, di tutela della dignità, dell'immagine, del domicilio e degli altri luoghi cui è riconosciuta analoga tutela.

## 2. Principio di necessità

Poiché l'installazione di un sistema di videosorveglianza comporta in sostanza l'introduzione di un vincolo per il cittadino, ovvero di una limitazione e comunque di un condizionamento, va applicato il principio di necessità e, quindi, va escluso ogni uso superfluo ed evitati eccessi e ridondanze.

Ciascun sistema informativo e il relativo programma informatico vanno conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi.

Il software va configurato anche in modo da cancellare periodicamente e automaticamente i dati eventualmente registrati.

L’articolo 3 del Codice enuncia il principio di necessità nel trattamento dei dati e stabilisce che “I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità”.

## 3. Principio di proporzionalità

Nel commisurare la necessità di un sistema al grado di rischio presente in concreto, va evitata la rilevazione di dati in aree o attività che non sono soggette a concreti pericoli, o per le quali non ricorre un’effettiva esigenza di deterrenza, (come quando, ad esempio, le telecamere vengono installate solo per meri fini di apparenza o di “prestigio”).

Gli impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente valutate insufficienti o inattuabili. Se la loro installazione è finalizzata alla protezione di beni, anche in relazione ad atti di vandalismo, devono risultare parimenti inefficaci altri idonei accorgimenti quali controlli da parte di addetti, sistemi di allarme, misure di protezione degli ingressi, abilitazioni agli ingressi.

Non va adottata la scelta semplicemente meno costosa, o meno complicata, o di più rapida attuazione, che potrebbe non tener conto dell’impatto sui diritti degli altri cittadini o di chi abbia diversi legittimi interessi.

La videosorveglianza è, quindi, lecita solo se è rispettato il c.d. principio di proporzionalità, sia nella scelta se e quali apparecchiature di ripresa installare, sia nelle varie fasi del trattamento. L’articolo 11, comma 1, lett. d) del Codice richiede che i dati personali oggetto del trattamento siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati.

Il principio di proporzionalità consente, ovviamente, margini di libertà nella valutazione da parte del titolare del trattamento, ma non comporta scelte del tutto

discrezionali e insindacabili. Il titolare del trattamento, prima di installare un impianto di videosorveglianza, deve valutare, obiettivamente e con un approccio selettivo, se l'utilizzazione ipotizzata sia in concreto realmente proporzionata agli scopi prefissi e legittimamente perseguibili, al fine di evitare un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali degli altri interessati.

**4. Principio di finalità**

Gli scopi perseguiti devono essere determinati, espliciti e legittimi (articolo 11, comma 1, lett. b), del Codice). Ciò comporta che il titolare possa perseguire solo finalità di sua pertinenza.

Nel provvedimento del 29 aprile 2004, a tale proposito, il Garante ha constatato, al punto 2.4, che "taluni soggetti pubblici e privati si propongono abusivamente, quale scopo della videosorveglianza, finalità di sicurezza pubblica, prevenzione o accertamento dei reati che invece competono solo ad organi giudiziari o di polizia giudiziaria oppure a forze armate o di polizia".

Sono invece diversi i casi in cui i sistemi di videosorveglianza sono in realtà introdotti come misura complementare volta a migliorare la sicurezza all'interno o all'esterno di edifici o impianti ove si svolgono attività produttive, industriali, commerciali o di servizi, o che hanno lo scopo di agevolare l'eventuale esercizio, in sede di giudizio civile o penale, del diritto di difesa del titolare del trattamento o di terzi sulla base di immagini utili in caso di fatti illeciti.

In ogni caso, possono essere perseguite solo finalità determinate e rese trasparenti, ossia direttamente conoscibili attraverso adeguate comunicazioni e/o cartelli di avvertimento al pubblico (fatta salva l'eventuale attività di acquisizione di dati disposta da organi giudiziari o di polizia giudiziaria), e non finalità generiche o indeterminate, tanto più quando esse siano incompatibili con gli scopi che vanno esplicitamente dichiarati e legittimamente perseguiti (articolo 11, comma 1, lett. b), del Codice). Le finalità così individuate devono essere correttamente riportate nell'informativa.

## 5. Informativa ed altri adempimenti[37]

A tale riguardo importanti regole sono contenute al punto 3 del provvedimento, relativo agli adempimenti.

Gli interessati devono essere informati che stanno per accedere o che si trovano in una zona videosorvegliata e dell'eventuale registrazione; ciò anche nei casi di eventi e in occasione di spettacoli pubblici (concerti, manifestazioni sportive) o di attività pubblicitarie (attraverso web cam).

L'informativa deve fornire gli elementi previsti dal Codice (art. 13) anche con formule sintetiche, ma chiare e senza ambiguità[38].

Il Garante ha altresì individuato, ai sensi dell'art. 13, comma 3 del Codice, un modello semplificato di informativa "minima", che può essere utilizzato in particolare in aree esterne, adattabile a varie circostanze[39].

---

[37] Il provvedimento contiene anche disposizioni sulla verifica preliminare: i trattamenti di dati personali nell'ambito di una attività di videosorveglianza devono essere effettuati rispettando le misure e gli accorgimenti prescritti dal Garante, anche con un provvedimento generale, come esito di una verifica preliminare attivata d'ufficio o a seguito di un interpello del titolare (articolo 17 del Codice), quando vi sono rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità degli interessati), su eventuali autorizzazioni, esami preventivi e notificazioni.
Vi sono poi prescrizioni concernenti i soggetti preposti e misure di sicurezza: si devono designare per iscritto tutte le persone fisiche, incaricate del trattamento, autorizzate ad utilizzare gli impianti e, nei casi in cui è indispensabile per gli scopi perseguiti, a visionare le registrazioni(articolo 30 del Codice). Deve trattarsi di un numero molto ristretto di soggetti, in particolare quando ci si avvale di una collaborazione esterna. Vanno osservate le regole ordinarie anche per ciò che attiene all'eventuale designazione di responsabili del trattamento, avendo particolare cura al caso in cui il titolare si avvalga di un organismo esterno anche di vigilanza privata (art. 29 del Codice).
Per quanto riguarda le misure di sicurezza i dati devono essere protetti da idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, perdita, anche accidentale, di accesso non autorizzato o trattamento non consentito o non conforme alle finalità della raccolta (art. 31 del Codice).

[38] L'articolo 13 del Codice, relativo all'informative, stabilisce, in particolare, che l'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7 ("Diritto di accesso ai dati personali ed altri diritti");
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

[39] Si allega il modello allegato al provvedimento del 29 aprile 2004.

In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, vanno installati più cartelli che avvisano che l'area è videosorvegliata.

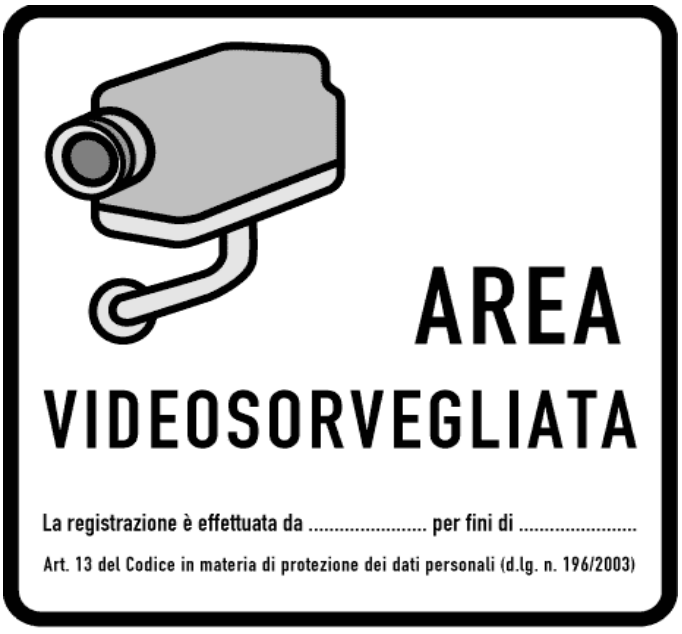
In luoghi diversi dalle aree esterne il modello di informativa va integrato con almeno un avviso circostanziato che riporti gli elementi del predetto articolo 13 con particolare riguardo alle finalità e all'eventuale conservazione.

Il supporto con l'informativa:

- deve essere collocato nei luoghi ripresi o nelle immediate vicinanze, non necessariamente a contatto con la telecamera;

- deve avere un formato ed un posizionamento tale da essere chiaramente visibile;

---




- Per le modalità di utilizzazione del modello si veda il paragrafo 3.1.
- Se le immagini non sono registrate, sostituire il termine "registrazione" con quello di "rilevazione".

- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati se le immagini sono solo visionate o anche registrate.

## 6. Durata dell'eventuale conservazione

In applicazione del principio di proporzionalità anche l'eventuale conservazione temporanea dei dati deve essere commisurata al grado di indispensabilità e per il solo tempo necessario - e predeterminato - a raggiungere la finalità perseguita.

L'articolo 11, comma 1, lettera e) del Codice richiede che i dati personali oggetto del trattamento siano conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Il Provvedimento sulla videosorveglianza aggiunge che la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione, fatte salve speciali esigenze di ulteriore conservazione in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si deve aderire ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria.

Solo in alcuni specifici casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell'attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l'esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), è ammesso un tempo più ampio di conservazione dei dati, che non può comunque superare la settimana.

Un eventuale allungamento dei tempi di conservazione deve essere valutato come eccezionale e comunque in relazione alla necessità derivante da un evento già accaduto o realmente incombente, oppure alla necessità di custodire o consegnare una copia specificamente richiesta dall'autorità giudiziaria o di polizia giudiziaria in relazione ad un'attività investigativa in corso.

Il sistema impiegato deve essere programmato in modo da operare al momento prefissato - ove tecnicamente possibile - la cancellazione automatica da ogni supporto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

## 7. Diritti degli interessati

Agli interessati identificabili deve essere assicurato l'effettivo esercizio dei propri diritti in conformità al Codice, in particolare quello di accedere ai dati che li riguardano, di verificare le finalità, le modalità e la logica del trattamento e di ottenere l'interruzione di un trattamento illecito, in specie quando non sono adottate idonee misure di sicurezza o il sistema è utilizzato da persone non debitamente autorizzate (art. 7 del Codice). La risposta ad una richiesta di accesso a dati conservati deve riguardare tutti quelli attinenti alla persona istante identificabile e può comprendere eventuali dati riferiti a terzi solo nei limiti previsti dal Codice (art. 10, commi 3 e seguenti del Codice). A tal fine può essere opportuno che la verifica dell'identità del richiedente avvenga mediante esibizione o allegazione di un documento di riconoscimento che evidenzi un'immagine riconoscibile dell'interessato.

## 8. Rapporti di lavoro

Il punto 4 del provvedimento regolamenta la videosorveglianza in "settori specifici" (rapporti di lavoro, ospedali e luoghi di cura, istituti scolastici, luoghi di culto e di sepoltura[40]).

[40] Negli ospedali e nei luoghi di cura è ammesso il monitoraggio di pazienti ricoverati in particolari reparti (es. rianimazione). Potranno accedere alle immagini solo il personale autorizzato e i familiari dei ricoverati.
Negli istituti scolastici l'installazione di sistemi di videosorveglianza è ammissibile solo quando strettamente indispensabile (es. atti vandalici) e solo negli orari di chiusura.

Per quanto riguarda i rapporti di lavoro nelle attività di sorveglianza occorre rispettare il divieto di controllo a distanza dell'attività lavorativa e ciò anche in caso di erogazione di servizi per via telematica mediante c.d. "web contact center".

Vanno poi osservate le garanzie previste in materia di lavoro quando la videosorveglianza è impiegata per esigenze organizzative e dei processi produttivi, ovvero è richiesta per la sicurezza del lavoro (art. 4 legge n. 300/1970[41]). Queste garanzie vanno osservate sia all'interno degli edifici, sia in altri luoghi di prestazione di lavoro, così come, ad esempio, si è rilevato in precedenti provvedimenti dell'Autorità a proposito di telecamere installate su autobus (le quali non devono riprendere in modo stabile la postazione di guida, e le cui immagini, raccolte per finalità di sicurezza e di eventuale accertamento di illeciti, non possono essere utilizzate per controlli, anche indiretti, sull'attività lavorativa degli addetti).

Ê inammissibile l'installazione di sistemi di videosorveglianza in luoghi riservati esclusivamente ai lavoratori o non destinati all'attività lavorativa (ad es. bagni, spogliatoi, docce, armadietti e luoghi ricreativi).

---

Al fine di garantire il rispetto dei luoghi di sepoltura, l'installazione di sistemi di videosorveglianza deve ritenersi ammissibile all'interno di tali aree solo quando si intenda tutelarle dal concreto rischio di atti vandalici.

[41] Articolo 4 ("Impianti audiovisivi") della legge 20 maggio 1970, n. 300 Norme sulla tutela della libertà e dignità del lavoratori, della libertà sindacale e dell'attività sindacale nel luoghi di lavoro e norme sul collocamento (statuto dei lavoratori): «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 rispondono 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 dei 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».
Per un approfondimento di tale aspetto si segnala il commento di A. Maresca, S. Lucrezio Monticelli, *Tutela della riservatezza nei rapporti di lavoro: divieto di controllo a distanza e telelavoro*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 537-558.

Eventuali riprese televisive sui luoghi di lavoro per documentare attività od operazioni solo per scopi divulgativi o di comunicazione istituzionale o aziendale, e che vedano coinvolto il personale dipendente, possono essere assimilati ai trattamenti temporanei finalizzati alla pubblicazione occasionale di articoli, saggi ed altre manifestazioni del pensiero. In tal caso, alle stesse si applicano le disposizioni sull'attività giornalistica contenute nel Codice, fermi restando, comunque, i limiti al diritto di cronaca posti a tutela della riservatezza, nonché l'osservanza del codice deontologico per l'attività giornalistica ed il diritto del lavoratore a tutelare la propria immagine opponendosi anche, per motivi legittimi, alla sua diffusione.

## 9. Attività di videosorveglianza dei soggetti pubblici

Come già evidenziato nei capitoli precedenti il Codice afferma che qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

Il punto 5 del Provvedimento sulla videosorveglianza contiene regole specifiche per i soggetti pubblici e, in particolare, si afferma che un soggetto pubblico può effettuare attività di videosorveglianza solo ed esclusivamente per svolgere funzioni istituzionali:

- che deve individuare ed esplicitare con esattezza;

- di cui è realmente titolare in base all'ordinamento di riferimento.

Diversamente, il trattamento dei dati non è lecito, anche se l'ente designa esponenti delle forze dell'ordine in qualità di responsabili del trattamento, oppure utilizza un collegamento telematico in violazione del Codice (art. 19, comma 2, del Codice).

Il Provvedimento osserva che tale circostanza si è ad esempio verificata presso alcuni enti locali che dichiarano di perseguire direttamente, in via amministrativa,

finalità di prevenzione e accertamento dei reati che competono alle autorità giudiziarie e alle forze di polizia (ad esempio ordinanze comunali in tema di prostituzione in luoghi pubblici).

Benché effettuata per la cura di un interesse pubblico, la videosorveglianza deve rispettare i principi richiamati.

Quando il soggetto è realmente titolare di un compito attribuito dalla legge in materia di sicurezza pubblica o di accertamento, prevenzione e repressione di reati, per procedere ad una videosorveglianza di soggetti identificabili deve ricorrere un'esigenza effettiva e proporzionata di prevenzione o repressione di pericoli concreti e specifici di lesione di un bene (ad esempio, in luoghi esposti a reale rischio o in caso di manifestazioni che siano ragionevolmente fonte di eventi pregiudizievoli). Non risulta quindi lecito procedere, senza le corrette valutazioni richiamate in premessa, ad una videosorveglianza capillare di intere aree cittadine "cablate", riprese integralmente e costantemente e senza adeguate esigenze. Del pari è vietato il collegamento telematico tra più soggetti, a volte raccordati ad un "centro" elettronico, che possa registrare un numero elevato di dati personali e ricostruire interi percorsi effettuati in un determinato arco di tempo.

Risulta parimenti priva di giustificazione l'installazione di impianti di videosorveglianza al solo fine (come risulta da casi sottoposti al Garante), di controllare il rispetto del divieto di fumare o gettare mozziconi, di calpestare aiuole, di affiggere o di fotografare, o di altri divieti relativi alle modalità nel depositare i sacchetti di immondizia entro gli appositi contenitori. Le specifiche norme di legge o di regolamento e le funzioni legittimamente individuate dall'ente costituiscono l'ambito operativo entro il quale il trattamento dei dati si intende consentito. Come prescritto dal Codice, l'eventuale comunicazione a terzi è lecita solo se espressamente prevista da una norma di legge o di regolamento (art. 19, comma 3, del Codice).

Il Codice individua poi specifiche regole volte invece a consentire, in un quadro di garanzie, riprese audio-video a fini di documentazione dell'attività istituzionale di organi pubblici (articoli dal 20 al 22 e 65 del Codice). Salvo i casi previsti per le professioni sanitarie e gli organismi sanitari, il soggetto pubblico non deve richiedere la manifestazione del consenso degli interessati (art. 18, comma 4, del Codice).

L'informativa agli interessati, contrariamente a quanto prospettato da alcuni enti locali, deve essere fornita nei termini illustrati nel paragrafo 3.1 del Provvedimento e non solo mediante pubblicazione sull'albo dell'ente, oppure attraverso una temporanea affissione di manifesti. Tali soluzioni possono concorrere ad assicurare trasparenza in materia, ma non sono di per sé sufficienti per l'informativa che deve aver luogo nei punti e nelle aree in cui si svolge la videosorveglianza.

Il punto 5 del provvedimento contiene altresì indicazioni specifiche su:

- accessi a centri storici;
- sicurezza nel trasporto urbano;
- deposito dei rifiuti.

Per quanto riguarda l'accesso ai centri storici è previsto che i comuni, qualora introducano sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato, dovranno rispettare quanto dettato dal d.p.r. 22 giugno 1999, n. 250[42]. Tale normativa impone ai comuni di richiedere una specifica autorizzazione amministrativa, nonché di limitare la raccolta dei dati sugli accessi rilevando le immagini solo in caso di infrazione (art. 3 d.p.r. n. 250/1999). I dati trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e definire il relativo contenzioso e si può accedere ad essi solo a fini di polizia giudiziaria o di indagine penale.

In materia di sicurezza nel trasporto urbano il provvedimento specifica che alcune situazioni di particolare rischio fanno ritenere lecita l'installazione su mezzi di trasporto pubblici di sistemi di videosorveglianza. Tali sistemi di rilevazione sono leciti anche presso talune fermate di mezzi urbani specie in aree periferiche che spesso sono interessate da episodi di criminalità (aggressioni, borseggi, ecc.). Valgono, anche

[42]d.p.r. 22 giugno 1999, n. 250 "Regolamento recante norme per l'autorizzazione alla installazione e all'esercizio di impianti per la rilevazione degli accessi di veicoli ai centri storici e alle zone a traffico limitato, a norma dell'articolo 7, comma 133-bis , della legge 15 maggio 1997, n. 127".

in questi casi, le considerazioni già espresse a proposito della titolarità in capo alle sole forze di polizia dei compiti di accertamento, prevenzione ed accertamento di reati, nonché del diritto di accesso alle immagini conservate per alcune ore, cui si dovrebbe accedere solo in caso di illeciti compiuti. Negli stessi casi, deve osservarsi particolare cura anche per ciò che riguarda l'angolo visuale delle apparecchiature di ripresa, nella collocazione di idonee informative a bordo dei veicoli pubblici e nelle aree di fermata - presso cui possono transitare anche soggetti estranei - e per quanto attiene alla ripresa sistematica di dettagli o di particolari non rilevanti riguardanti i passeggeri.

Per quanto concerne il deposito dei rifiuti, il controllo video di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose è lecito se risultano inefficaci o inattuabili altre misure. Il medesimo controllo non è invece lecito - e va effettuato in altra forma - se è volto ad accertare solo infrazioni amministrative rispetto a disposizioni concernenti modalità e orario di deposito dei rifiuti urbani.

## 10. Privati ed enti pubblici economici

Per quanto riguarda i soggetti privati il provvedimento generale sulla videosorveglianza del 2004, ricorda innanzitutto che, a differenza dei soggetti pubblici, i privati e gli enti pubblici economici possono trattare dati personali solo se vi è il consenso preventivo espresso dall'interessato, oppure uno dei presupposti di liceità previsti in alternativa al consenso (articoli 23 e 24 del Codice).

Il provvedimento, facendo poi riferimento al Codice laddove questo prevede, come idonea alternativa all'esplicito consenso, l'istituto del bilanciamento di interessi (articolo 24, comma 1, lett. g), del Codice) porta ad attuazione tale istituto, individuando i casi in cui la rilevazione delle immagini può avvenire senza consenso:

- si possono installare telecamere senza il consenso degli interessati, sulla base delle prescrizioni indicate dal Garante, quando chi intende rilevare le immagini

deve perseguire un interesse legittimo a fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di vandalismo, prevenzione incendi, sicurezza del lavoro ecc.;

- le riprese di aree condominiali da parte di più proprietari o condomini, di studi professionali, società ed enti sono ammesse esclusivamente per preservare, da concrete situazioni di pericolo, la sicurezza di persone e la tutela dei beni. L'installazione da parte di singoli condomini richiede comunque l'adozione di cautele: angolo visuale limitato ai soli spazi di propria pertinenza, nessuna ripresa di aree comuni o antistanti le abitazioni di altri condomini ecc. I videocitofoni sono ammessi per finalità identificative dei visitatori.

**11. Prescrizioni e sanzioni**

Il Garante invita tutti gli operatori interessati ad attenersi alle prescrizioni illustrate e a quelle definite opportune parimenti indicate nel sopra citato provvedimento, in attesa dei più specifici interventi che potranno derivare in materia da un c.d. provvedimento di verifica preliminare del garante stesso (art. 17 del Codice), oppure dal codice deontologico che il Garante ha promosso per disciplinare in dettaglio altri aspetti del trattamento dei dati personali effettuato "con strumenti elettronici di rilevamento di immagini" (articolo 134 del Codice).

Le misure necessarie prescritte dal provvedimento devono essere osservate da tutti i titolari di trattamento. In caso contrario il trattamento dei dati è, a seconda dei casi, illecito oppure non corretto, ed espone:

- all'inutilizzabilità dei dati personali trattati in violazione della relativa disciplina (articolo 11, comma 2, del Codice);

- all’adozione di provvedimenti di blocco o di divieto del trattamento disposti dal Garante (articolo 143, comma 1, lett. c), del Codice), e di analoghe decisioni adottate dall’autorità giudiziaria civile e penale;

- all’applicazione delle pertinenti sanzioni amministrative o penali (articoli 161 e seguenti del Codice).

# Capitolo 7
# Dati personali dei cittadini e propaganda elettorale

Un rilevante ambito nel quale viene in gioco l'utilizzo dei dati personali è quello relativo alla materia elettorale, e in particolare alla propaganda in vista delle elezioni.

Due sono le esigenze rilevanti potenzialmente contrapposte: da un lato, la necessità di consentire e agevolare la comunicazione politica, intesa come strumento fondamentale per la partecipazione di cittadini, delle forze politiche e dei candidati alla vita democratica; dall'altro, il diritto dei cittadini a essere informati durante le campagne elettorali politiche ed amministrative nel rispetto della loro riservatezza e delle loro libertà fondamentali.

La questione, più precisamente, riguarda l'individuazione dei casi in cui non è necessario richiedere il consenso degli elettori per l'invio del materiale di propaganda. Principi guida per una propaganda elettorale rispettosa dei cittadini sono, in linea generale:

- l'obbligo di raccogliere ed utilizzare solo dati indispensabili;

- l'obbligo di informare i cittadini su chi tratta i dati e sull'uso che ne viene fatto;

- l'obbligo di ottenere, nei casi previsti, consenso degli interessati quando si usano particolari forme di comunicazione (come i messaggi sms, mms, le e-mail, le telefonate preregistrate e i fax). Il consenso non è invece necessario quando si usano i dati personali contenuti nelle liste elettorali detenute dai comuni, i dati di iscritti ed aderenti a partiti e organismi politici o i dati degli abbonati presenti nei nuovi elenchi telefonici accanto ai quali figurino i due simboli che attestano la disponibilità a ricevere posta o telefonate;

- l’obbligo di raccogliere le informazioni da fonti lecitamente accessibili;

- l’obbligo di utilizzare i dati solo a fini di propaganda elettorale.

Il Garante è intervenuto, rivolgendosi a partiti, organismi politici, comitati di promotori e sostenitori e singoli candidati, con un proprio apposito provvedimento finalizzato a regolare il trattamento dei dati personali nelle attività di propaganda elettorale, collegate alle elezioni politiche e amministrative, ai referendum e alla selezione di candidati alle elezioni (c.d. primarie).

Il provvedimento si occupa di due questioni principali. In primo luogo, il tipo di dati utilizzabili, a proposito dei quali si distingue tra:

(a) dati utilizzabili senza consenso;
(b) dati utilizzabili previo consenso;
(c) fonti documentali non utilizzabili.

In secondo le modalità in base alle quali deve essere redatta l’informativa per i casi in cui sussiste l’obbligo di informativa. Infine sono previste alcune ulteriori previsioni normative.

## 1. I dati utilizzabili senza necessità del previo consenso dell’interessato

I dati personali utilizzabili senza consenso sono:

(a) quelli contenuti nelle liste elettorali e in altri elenchi o registri pubblici;
(b) quelli raccolti da titolari di cariche elettive e di altre funzioni pubbliche;
(c) quelli relativi agli iscritti a partiti, organismi politici e comitati nonché ad altri organismi associativi a carattere non politico.

Iniziando dai dati contenuti nelle liste elettorali, questi comprendono:

- i dati contenuti nelle liste tenute da ciascun comune;

- i dati contenuti nell'elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo;

- i dati contenuti nell'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato a predisporre le liste elettorali, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (Aire) e degli schedari consolari;

- i dati contenuti nell'elenco dei cittadini italiani residenti all'estero aventi diritto al voto per l'elezione del Comitato degli italiani all'estero (Comites);

- i dati contenuti nelle liste aggiunte degli elettori di uno Stato membro dell'Unione europea residenti in Italia e che intendano esercitare il diritto di voto alle elezioni del Parlamento europeo.

È bene peraltro precisare che i dati sopra ricordati possono essere lecitamente utilizzati solo a fini di propaganda elettorale, e non anche per effettuare comunicazioni pubblicitarie o commerciali. Risolvendo un quesito sottoposto al suo giudizio, il Garante ha, in proposito, precisato che anche i dati raccolti prima dell'entrata in vigore del nuovo Codice sulla privacy sono sottoposti alla medesima disciplina e devono quindi essere distrutti se raccolti per finalità non più consentite.

Possono inoltre essere utilizzate per la propaganda, anche in questo caso senza il consenso degli interessati, altre fonti documentali (e in proposito il Garante pare aver voluto mantenersi volutamente sul vago, così riservandosi di decidere nei casi specifici che dovessero essere eventualmente sottoposti alla sua valutazione), detenute da soggetti pubblici, liberamente accessibili a chiunque in base a specifiche disposizioni normative. In ogni caso occorre che siano rispettate le modalità eventualmente stabilite per accedere a tali fonti e per farne utilizzo (in particolare occorre aderire alle finalità per le quali determinati elenchi sono resi pubblici).

Passando alla seconda categoria di dati utilizzabili senza previo consenso degli interessati, vengono in rilievo i dati raccolti dai titolari di cariche elettive nel quadro

delle relazioni interpersonali intercorrenti tra gli eletti e i cittadini ed elettori. Occorre però precisare che non rientrano tra i dati utilizzabili a fini di propaganda elettorale quelli che gli eletti hanno facoltà di richiedere agli uffici pubblici in forza della normativa volta ad agevolare l'esercizio del loro mandato (a meno che le iniziative che si intende porre in essere possano risultare in concreto obiettivamente riconducibili ad attività e compiti espletati nel corso del mandato). Inoltre, non può ritenersi consentito, da parte di soggetti titolari di altre cariche pubbliche non elettive, l'utilizzo per finalità di propaganda di dati acquisiti per svolgere i relativi compiti istituzionali.

La terza e ultima categoria di dati che, per essere utilizzati a fini di propaganda politica, non necessitano di autorizzazione sono quelli relativi ai dati personali di iscritti e aderenti ai partiti politici, nonché ad altri enti, associazioni ed organismi senza scopo di lucro (associazioni sindacali, professionali, sportive, di categoria, ecc.) che abbiano tra i propri scopi anche finalità di propaganda elettorale. Tali dati sono peraltro utilizzabili solo nell'ambito delle organizzazioni che hanno provveduto alla loro raccolta.

## 2. I dati utilizzabili previo consenso dell'interessato

Diversamente dai casi precedenti, è necessario ottenere previamente il consenso dell'interessato per poter utilizzare a fini di propaganda elettorale le seguenti categorie di dati personali:

(a) quelli relativi a simpatizzanti e contatti di partiti politici, comitati promotori e singoli candidati;
(b) quelli relativi ai nominativi contenuti negli elenchi telefonici;
(c) quelli relativi agli abbonati ai servizi di telefonia mobile e utilizzatori di schede di traffico prepagato;
(d) quelli ricavati attraverso strumenti informatici;
(e) quelli messi a disposizione da parte di terzi.

Iniziando dai primi, i partiti e gli altri organismi politici, i comitati promotori e sostenitori, nonché i singoli candidati possono utilizzare lecitamente dati relativi a simpatizzanti o ad altre persone già contattate per singole iniziative o che hanno partecipato occasionalmente a iniziative promosse dal soggetto che intende utilizzare i dati (petizioni, proposte di legge, richieste di referendum, raccolte di firme, ecc). solo dopo aver ottenuto il preventivo consenso scritto degli interessati (si tratta infatti di dati sensibili), sebbene tale consenso possa anche essere manifestato una tantum.

Passando ai dati contenuti nei nuovi elenchi telefonici, cartacei ed elettronici, occorre fare riferimento ai simboli che compaiono accanto ai singoli nominativi, attestanti il consenso previamente prestato, rispettivamente, alla ricezione di posta a domicilio e alla ricezione di chiamate telefoniche per finalità diverse dalla comunicazione interpersonale. In tali casi, i nominativi sono utilizzabili anche per inviare a domicilio materiale di propaganda nonché, a seconda dei simboli apposti sull'elenco, per effettuare chiamate aventi finalità di propaganda.

Analoga è la disciplina relativa ai dati riguardanti gli abbonati ai servizi di telefonia mobile e utilizzatori di schede di traffico prepagato, il cui previo e specifico consenso (anche in questo caso acquisibile una tantum) è necessario per poter procedere all'invio di fax, messaggi di tipo sms e mms, nonché per effettuare chiamate telefoniche preregistrate e per inviare messaggi di posta elettronica.

Inoltre, senza un preventivo consenso informato non è lecito l'invio di messaggi, newsletter e di altro materiale di propaganda quando si utilizzano dati raccolti automaticamente in internet tramite appositi software, liste di abbonati ad un provider, dati pubblicati su siti web per specifiche finalità di informazione aziendale, comunicazione commerciale o attività istituzionale o associativa, dati ricavati da forum o newsgroup e dati consultabili in internet solo per le finalità di applicazione della disciplina sulla registrazione dei nomi a dominio.

Infine, è bene precisare che l'eventuale acquisizione dei dati personali da parte di un soggetto terzo (il quale potrebbe averli raccolti in base ad un consenso riferito ai più diversi scopi, come per esempio quelli di tipo promozionale o commerciale) non esime il partito, l'organismo politico, il comitato o il candidato dall'onere di verificare che il terzo abbia informato gli interessati riguardo all'utilizzo dei dati per finalità di propaganda e abbia ottenuto il loro consenso idoneo ed esplicito.

### 3. Le fonti documentali non utilizzabili

Vi è poi una terza categoria di informazioni, composta da quei dati che non risultano mai utilizzabili ai fini della propaganda elettorale. In particolare si fa qui riferimento alle fonti documentali detenute da soggetti pubblici che non sono utilizzabili, neanche da parte di titolari di cariche elettive, in ragione della specifica normativa che ne precluda l'acquisizione a fini di propaganda, oppure del segreto d'ufficio o della circostanza che esse sono state acquisite in base a una normativa che ne vincola l'utilizzo.

I casi maggiormente rilevanti sono i seguenti:

- gli archivi dello stato civile;

- l'anagrafe della popolazione residente (questa risulta però utilizzabile per la comunicazione istituzionale di amministrazioni pubbliche);

- le liste elettorali di sezione già utilizzate nei seggi, sulle quali sono annotati dati relativi ai non votanti e che sono utilizzabili solo per controllare la regolarità delle operazioni elettorali;

- i dati annotati privatamente nei seggi da scrutatori e rappresentanti di lista, durante operazioni elettorali;

- gli indirizzari e i dati raccolti solo per lo svolgimento delle attività istituzionali proprie del soggetto pubblico.

## 4. L'informativa

In tutti i casi in cui i dati non possono essere utilizzati senza il previo consenso dell'interessato (si veda il paragrafo 2), è necessario che a quest'ultimo sia offerta un'apposita informativa circa le caratteristiche del trattamento che verrà effettuato.

L'informativa può essere basata sulla seguente formula semplificata predisposta dall'Autorità Garante, che può essere inserita anche nei messaggi di posta elettronica e nelle missive di propaganda:

**INFORMATIVA**

(Art. 13 del Codice in materia di protezione dei dati personali)

I dati che ha fornito liberamente (oppure: che sono stati estratti da…) sono utilizzati da … (indicare il titolare del trattamento) solo a fini di propaganda (o per la selezione dei candidati …; indicare anche se i dati verranno utilizzati per analoghe iniziative o anche da singoli candidati, oltre che da parte degli organi della forza politica), anche con strumenti informatici, e non saranno comunicati a terzi (indicare, se utilizzata, l'eventuale organizzazione esterna che cura l'inoltro). Lei può in ogni momento accedere ai dati, ottenere di non ricevere più materiale di propaganda, opporsi al trattamento dei dati o chiedere di integrarli, rettificarli, ecc., rivolgendosi a … (indicare le coordinate del predetto titolare del trattamento o di un suo referente, ad esempio del responsabile del trattamento facoltativamente designato).

## 5. Ulteriori previsioni normative

In conformità con le regole generali vigenti in materia di privacy, il cittadino può, in ogni caso, opporsi all'ulteriore invio di materiale elettorale anche se in precedenza si era dichiarato disponibile a riceverlo.

Inoltre, nei casi in cui il cittadino non è chiamato a esprimere il consenso o non è prescritto che debba ricevere l'informativa, egli può avvalersi delle tutele previste

dal Codice sulla protezione dei dati personali. In quest'ottica può, per esempio, chiedere al partito o al candidato di avere accesso ai dati che lo riguardano, chiedere informazioni circa l'origine e le modalità del trattamento, opporsi all'ulteriore utilizzo dei dati per invii di materiale propagandistico o all'effettuazione di chiamate telefoniche.

Coloro che svolgono il trattamento sono tenuti a dare idoneo e tempestivo riscontro ad eventuali richieste con le quali gli interessati esercitino i propri diritti: se ciò non dovesse verificarsi, il cittadino può rivolgersi all'autorità giudiziaria o presentare un reclamo o un ricorso al Garante.

Dal canto loro, partiti, movimenti o comitati elettorali devono adottare idonee misure di sicurezza per provvedere adeguatamente alla salvaguardia dei dati dei cittadini e designare le persone fisiche incaricate di provvedere al trattamento. Le iniziative di propaganda elettorale non comportano però l'obbligo di notifica al Garante né l'obbligo di individuare il responsabile del trattamento.

# Capitolo 8
# La tutela dell'interessato nel trattamento dei dati personali

Il decreto legislativo n. 196/2003 garantisce l'interessato al diritto alla riservatezza sia mediante la tutela amministrativa sia mediante quella giurisdizionale, disciplinate nella parte III del Codice, intitolata appunto "Tutela dell'interessato e sanzioni".

La tutela amministrativa è quella che si può ottenere rivolgendosi, mediante gli strumenti appositamente previsti (reclamo, segnalazione, ricorso) al Garante per la protezione dei dati personali oppure quando è il Garante stesso che esercita d'ufficio poteri ispettivi e di controllo.

Per quanto concerne la tutela giurisdizionale, l'art 152 del Codice (Autorità giudiziaria ordinaria) prevede che tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.

Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.

Il tribunale decide in ogni caso in composizione monocratica.

Per quanto concerne le sanzioni, l'impianto del codice è sostanzialmente simile a quello previsto dalla legge n. 675/1996, anche se si nota una riduzione delle disposizioni concernenti l'illecito penale ed un contestuale potenziamento delle sanzioni amministrative.

## 1. La tutela civilistica

L'articolo 15 del d.lgs. n. 196/2003 nel disciplinare i "Danni cagionati per effetto del trattamento" prevede, al primo comma, che "Chiunque cagiona danno ad

altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile"[43].

Il secondo comma aggiunge che "Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11".

L'articolo 11, a sua volta, enunciando quelli che sono i principi generali sulle modalità della raccolta e sui requisiti dei dati personali, stabilisce che questi devono essere:

a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, e utilizzati in altre operazioni del trattamento in termini non incompatibili con tali scopi;
c) esatti e, se necessario, aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati".

L'art. 2050 del codice civile "Responsabilità per l'esercizio di attività pericolose" a sua volta prevede che: "Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di aver adottato tutte le misure idonee a evitare il danno".

[43] Già nella direttiva 95/46/CE il legislatore comunitario si è occupato del tema della responsabilità civile per i danni procurati per effetto del trattamento dei dati. Infatti l'articolo 23 (Responsabilità) prevede che «1. Gli Stati membri dispongono che chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della presente direttiva abbia il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento.
2. Il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabile». Una disposizione analoga al primo comma dell'art. 15 del Codice era contenuta nell'articolo 18 della legge n. 675/1996.

### 1.2. Il trattamento

Il “trattamento” è definito dall’art. 4, comma 1, lett. a) come “qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati”.

Dalla stessa definizione emerge come il trattamento dei dati costituisce un’attività in grado di ledere una molteplicità di diritti fondamentali della persona.

### 1.3. Il dato personale

Dato personale è “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” (art. 4, comma 1, lett. b).

### 1.4. Il danno

Il danno risarcibile ai sensi dell’art. 15 è sia il danno patrimoniale che il danno non patrimoniale, anche se, in realtà, il riferimento a quest’ultimo si ha solamente nel secondo comma dell’art. 15 che specifica che il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Si nota, in ogni caso, la volontà del legislatore di ampliare la risarcibilità del danno non patrimoniale, che non è assolutamente vincolato alle ipotesi di reato.

Data l’impossibilità di ancorare la valutazione del danno non patrimoniale a criteri oggettivi, il giudice, nel pronunciarsi sulla liquidazione, deve valutare secondo un criterio equitativo.

### 1.5. L’inversione dell’onere della prova

Il nostro ordinamento civile prevede, come regola generale in materia di responsabilità extracontrattuale che, chiunque si ritenga danneggiato da un fatto illecito, deve dar prova della responsabilità di colui che l’ha commesso. Non accade così, invece, nell’ipotesi regolata dall’art. 2050, dal quale emerge il c.d. principio dell’inversione dell’onere della prova, in base al quale il danneggiato deve provare solo il fatto storico, mentre colui che effettua il trattamento, e che quindi ha causato il fatto dannoso, a fini liberatori, deve dimostrare di aver adottato tutte le misure idonee ad evitarlo.

Non è il danneggiato a dover dimostrare che chi deteneva i dati non è stato attento, ma è quest'ultimo a dover dimostrare che ha fatto tutto il possibile per evitare il danno, il quale però evidentemente si è verificato.

Contrariamente a quanto disposto dall’ordinamento nelle ipotesi comuni di responsabilità per fatto illecito (chiunque si ritenga danneggiato da un fatto illecito, deve dar prova della responsabilità di colui che l’ha commesso) nel caso di esercizio di attività pericolosa è il gestore dell’attività a dover dimostrare di aver adottato tutte le misure idonee ad evitare il danno, sempre che il danneggiato abbia a sua volta preventivamente fornito la prova del danno stesso e del nesso di causalità tra il comportamento (attivo o omissivo) dell’esercente l’attività ed il danno subito.

### 1.6. Il trattamento di dati personali come attività pericolosa.

L'art. 15 non stabilisce espressamente che il trattamento dei dati è pericoloso: vi è però l'esplicito rinvio all'art. 2050 c.c. che disciplina la responsabilità per l'esercizio di attività pericolose.

Da alcuni autori viene fatto notare che, se il legislatore avesse voluto limitarsi a stabilire solamente un'inversione dell'onere della prova, lo avrebbe potuto fare direttamente nel testo dell'art. 15, senza operare il rinvio all'art. 2050 c.c.: la conseguenza che deriva dall'esplicito collegamento fra le due disposizioni è allora quella per cui il trattamento dei dati personali costituisce, ipso iure, un'attività pericolosa[44].

Il trattamento, come definito dall'art. 4, comma 1, lett. a) costituisce di per se un'attività pericolosa in quanto naturalmente idonea a ledere la tipologia dei diritti fondamentali della persona, diversi da quelli che attengono alla sfera fisica.

In altri termini, se sinora l'attività pericolosa di cui all'art. 2050 c.c. è stata sostanzialmente identificata come l'attività materiale posta in essere nell'esercizio dell'attività di impresa sostanzialmente lesiva del diritto all'integrità fisica della persona, d'ora innanzi si potrà ritenere che la combinazione normativa fra l'art. 15 e l'art. 2050 c.c. comporta che l'attività giuridica costituita dal trattamento dei dati abbia una predisposizione naturale a mettere in pericolo il diritto all'integrità morale della persona[45].

### 1.7. La prova di aver adottato tutte le misure idonee a evitare il danno.

La prova è particolarmente rigorosa, in quanto non è sufficiente la sola dimostrazione, in negativo, di non aver commesso alcuna violazione della legge o

[44] G.P. Cirillo, *La tutela civilistica nel trattamento pubblico dei dati personali*, in A. Loiodice e G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXVI, *La tutela della riservatezza*, Cedam, Padova 2000, pag. 113; S. Romeo, *Recensione a G.P. Cirillo, 'Trattamento pubblico dei dati personali e responsabilità civile della P.A., in Foro amm. 11-12/99*, in www.lexfor.it
[45] G.P. Cirillo, *op. cit.*, pagg. 95-127.

delle regole di comune prudenza, ma è necessaria la prova positiva, certamente non semplice, di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso[46].

Parte delle dottrina ritiene che la prova liberatoria consista essenzialmente nella prova di avere adottato ogni diligenza possibile (e spesso, quindi, nella prova dell'intervento di un fortuito). Anche buona parte della giurisprudenza argomenta in tal senso: solo un evento fortuito consentirebbe di superare l'obbligo di risarcire il danno in un contesto che sarebbe quindi di responsabilità oggettiva. Alcuni osservano però che ragionare in questa maniera significherebbe accollare all'esercente l'attività pericolosa la prova del fortuito, la quale, sebbene talvolta più semplice da fornire rispetto alla prova dell'adozione delle misure di sicurezza, potrebbe risultare paradossalmente insufficiente, essendo in certi casi a carico dello stesso l'adozione delle misure idonee ad evitare anche il fortuito.

Da alcuni autori viene fatto notare, però, che quando il legislatore ha inteso disporre in questo senso, lo ha fatto espressamente (si veda l'art. 2051 cod. civ.).

Secondo altri autori appare più aderente al dettato legislativo interpretare l'art. 2050 come un'ipotesi di responsabilità aggravata, come fa autorevole dottrina, che, richiamando un diverso orientamento giurisprudenziale, sia pure minoritario, sostiene si debba far riferimento all'ordinaria diligenza ed alla comune prudenza nella scelta e nell'adozione delle misure di sicurezza.

La prova da predisporre dovrà allora riguardare l'adozione delle misure che appaiono ragionevoli nel caso concreto, in relazione all'attività svolta, ecc. In tal caso, per liberarsi da responsabilità, sarà sufficiente allegare l'adozione di precisi ed oggettivi accorgimenti tecnici.

L'evento sarà non addebitabile all'esercente l'attività pericolosa qualora non sia prevedibile, né superabile, con l'adozione dell'ordinaria diligenza: il criterio di imputazione della responsabilità appare, dunque, fondato sulla colpa.

Il titolare del trattamento, comportandosi con la diligenza dovuta, dovrà adottare tutte quelle misure che appaiono idonee a fronteggiare il rischio, ed eventualmente anche solo a ridurlo[47].

---

[46] A. Lucarino, *Responsabilità e risarcimento dei danni in seguito al trattamento dei dati personali*, in www.privacy.it, maggio 2000

[47] Per quanto riguarda il dibattito sull'interpretazione della prova liberatoria si rinvia a G.P. Cirillo, *op. cit.*, pagg. 111-112; G. Fioriglio, *La tutela risarcitoria nel Codice della privacy*, in www.dirittodell'informatica.it

### 1.8. Il soggetto dell'illecito

Per quanto concerne il soggetto dell'illecito va osservato che la norma si riferisce a "chiunque" cagioni un danno, sia che "chiunque" sia un privato sia che si tratti di un soggetto pubblico.

Non viene specificato a quale categoria soggettiva (titolare, responsabile, incaricato) si riferisca la responsabilità civile e non viene prevista una normativa specifica relativa ai soggetti pubblici.

Nel caso in cui titolare del trattamento sia una persona giuridica pubblica, si dovranno applicare le regole sulla responsabilità dei pubblici dipendenti.

- L'art. 28 Cost. dispone, per il caso di responsabilità civile, che dipendenti e funzionari siano responsabili in solido con lo Stato o gli enti pubblici. I danneggiati possono quindi rivalersi indifferentemente sia nei confronti della pubblica amministrazione sia nei confronti dei funzionari e dei dipendenti.

- Lo statuto degli impiegati civili dello Stato (d.p.r. 10 gennaio 1957, n. 3)[48] e la legge n. 20/1994[49], precisano, però, che l'impiegato civile è personalmente tenuto a risarcire il danno cagionato a terzi solo ove lo stesso derivi da comportamento doloso o gravemente colposo. Laddove, pertanto, si rientri

---

[48] Articolo 22 del d.p.r. 3 del 10 gennaio 1957 (Responsabilità verso i terzi):
«1. L'impiegato che, nell'esercizio delle attribuzioni ad esso conferite dalle leggi o dai regolamenti, cagioni ad altri un danno ingiusto ai sensi dell'art. 23 è personalmente obbligato a risarcirlo. L'azione di risarcimento nei suoi confronti può essere esercitata congiuntamente con l'azione diretta nei confronti dell'Amministrazione qualora, in base alle norme ed ai principi vigenti dell'ordinamento giuridico, sussista anche la responsabilità dello Stato.
2. L'amministrazione che abbia risarcito il terzo del danno cagionato dal dipendente si rivale agendo contro quest'ultimo a norma degli articoli 18 e 19. Contro l'impiegato addetto alla conduzione di autoveicoli o di altri mezzi meccanici l'azione dell'Amministrazione è ammessa solo nel caso di danni arrecati per dolo o colpa grave».
Articolo 23 del d.p.r. 3 del 10 gennaio 1957 (Danno ingiusto):
«1. È danno ingiusto, agli effetti previsti dall'art. 22, quello derivante da ogni violazione dei diritti dei terzi che l'impiegato abbia commesso per dolo o per colpa grave; restano salve le responsabilità più gravi previste dalle leggi vigenti.
2.La responsabilità personale dell'impiegato sussiste tanto se la violazione del diritto del terzo sia cagionata dal compimento di atti od operazioni, quanto se la detta violazione consista nell'omissione o nel ritardo ingiustificato di atti od operazioni al cui compimento l'impiegato sia obbligato per legge o per regolamento».
[49] Legge 14 gennaio 1994 n. 20 (Disposizioni in materia di giurisdizione e controllo della Corte dei conti).

nell'ambito della mera colpa lieve, tenuta al risarcimento del danno sarà solo la pubblica amministrazione.

- Il dolo comporta una frattura del rapporto organico che viene ad escludere la responsabilità della P.A[50].

- L'amministrazione potrà rivalersi nei confronti del dipendente promuovendo un giudizio dinnanzi alla Corte dei Conti.

A norma dell'art. 4 la Pubblica Amministrazione può essere sia titolare sia responsabile del trattamento e, conseguentemente, sarà esperibile nei confronti della stessa un'azione civile per il risarcimento dei danni derivanti da un illecito trattamento dei dati.

### 1.9. Un caso concreto

Al momento non sono molte le sentenze di condanna per trattamento illecito dei dati personali ex art. 2050 del codice civile[51].

In tal senso è invece la sentenza del 29 settembre 2005 del Giudice di Pace di Napoli con la quale viene condannato un gestore telefonico a risarcire il danno causato

[50] La giurisprudenza ha però ampliato le ipotesi di responsabilità della P.A., considerando comunque responsabile l'ente pubblico nei casi nei quali la condotta del dipendente si è svolta in una situazione di «occasionalità necessaria con le attribuzioni sue proprie».

[51] Si segnala anche la sentenza del Tribunale di Palermo, sezione I civile, del 21 febbraio 2007 che afferma che la presunzione di colpa prevista dall'art. 2050 c.c. per gli esercenti attività pericolose, richiamata dall'art. 18 della legge 675/96 (disposizione analoga al primo comma dell'art. 15 del Codice), comporta che il giornalista, in presenza di un'azione per danni da illegittimo trattamento di dati personali, deve fornire la prova di avere fatto di tutto per evitare il danno.
In altre sentenze (ad esempio Giudice di Pace di Napoli in data 7-10 giugno 2004) si nota invece che, pur lamentando l'attore di aver subito un danno per effetto del trattamento dei suoi dati personali, il risarcimento è chiesto ex art. 2043 (e non ex art. 2050) del codice civile. Tale ultima norma libererebbe l'attore dall'onere di provare lo stretto nesso di causalità tra il danno subito e l'azione colposa del convenuto, essendo sufficiente, quando si chiede l'applicazione dell'art. 2050 c.c., dimostrare il fatto storico da cui è derivato il danno rimettendosi, poi, al convenuto l'onere di dimostrare di aver adottato tutte le cautele per evitare il danno stesso.

dal cosiddetto spamming telefonico, riconoscendo che il gestore di servizi telefonici esercita, comunque, un'attività pericolosa ai sensi dell'articolo 2050 del codice civile.

Nel caso affrontato l'attore ha citato in giudizio un gestore di telefonia mobile al fine di sentir accertare e dichiarare la responsabilità, inadempimento e violazioni perpetrate dal gestore stesso a suo danno per aver inviato spot sms senza consenso, di carattere commerciale e pubblicitario sul proprio cellulare, subendo continui fastidi, disagi e disturbi, chiedendo la condanna della società convenuta al risarcimento di tutti i danni subiti, personali e patrimoniali, nessuno escluso, da liquidarsi, secondo giustizia o in via equitativa.

Il Giudice di Pace ha osservato che, per giurisprudenza costante, nell'ambito della tutela dei diritti fondamentali dell'individuo, dei diritti soggettivi e della persona e della sua vita privata, senza dubbio è opportuno assicurare e garantire l'utente vittima di avvisi, chiamate o comunicazioni non desiderate, pregiudizievoli, importune o che gli rechino disturbo, riconoscendo allo stesso un equo ristoro e la dovuta tranquillità.

Per legge soprattutto a seguito delle recenti modifiche e riforme della normativa in materia di privacy va tutelata e protetta la sfera privata dell'individuo ed il suo diritto alla riservatezza riconoscendogli il ruolo di unico "sovrano" dei dati e delle informazioni che lo riguardano. Nella fattispecie, appare evidente la violazione del diritto al riposo, alla riservatezza ed alla privacy dell'istante, inteso come diritto di costruire liberamente e difendere la propria sfera privata, di scegliere il proprio stile di vita senza influenze ed intrornissioni indesiderate da parte di terzi, proprio, tramite l'invio di sms pubblicitari.

È chiaro che ogni gestore del servizio di telefonia mobile può utilizzare dati e numero dell'utenza mobile del cliente per scopi legati al servizio di telefonia richiesta dal consumatore oppure per scopo commerciale ma solo se l'utente abbia manifestato preventivamente il proprio consenso scritto, validamente prestato, espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, salvo rappresentazione all'interessato delle informazioni prescritte. Il trattamento dei dati personali, inteso come qualsiasi operazione concernente la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la selezione, l'estrazione, l'utilizzo, il blocco, la comunicazione, la diffusione, la

cancellazione e la distruzione dei dati, è ammesso solo con il consenso espresso dell'interessato pena ristoro danni, sanzioni e condanne di carattere penale.

Nel caso di specie la società convenuta, alla quale incombeva l'onere, non ha fornito alcuna prova circa il rilascio del consenso dell'istante al trattamento dei dati personali e, segnatamente, all'utilizzo del numero di telefono dell'istante per scopi commerciali e diversi dal servizio di telefonia.

Alla luce della normativa vigente quindi e di quanto risultante dai fatti di causa può ritenersi provato il nesso di causalità tra il comportamento, violazioni ed inadempimenti del gestore ed i pregiudizi tutti lamentati dall'istante per le continue interferenze e danni subiti nella sua sfera privata.

Pertanto, la società convenuta, tenuta al risarcimento dei danni subiti dall'istante ai sensi dell'articolo 2043 e dell'articolo 2050 del codice civile, richiamato dalla normativa in materia di protezione dei dati personali. A tal proposito, si osserva che la presunzione di responsabilità può essere vinta solo con una prova particolarmente rigorosa, essendo posto a carico dell'esercente l'attività l'onere di dimostrare l'adozione di tutte le misure idonee ad evitare il danno: pertanto, non basta la prova negativa di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma occorre quella positiva di aver impiegato ogni cura o misura atta ad impedire l'evento dannoso.

In ogni caso, la convenuta non ha provato di aver trattato in modo lecito e secondo correttezza i dati dell'istante e di aver adottato idonee e preventive misure onde eliminare o ridurre i rischi del trattamento con particolare riguardo alle interferenze nella sfera privata con comunicazioni di carattere commerciale, gestite mediante sistemi automatici di chiamata. Dunque è assolutamente illegittimo e lesivo quello che può ormai definirsi come lo spamming telefonico, ossia il predetto trattamento e sfruttamento dei dati personali dell'utente eseguito attraverso l'invio di corrispondenza informatica ed elettronica a scopo di lucro e pubblicitario effettuato senza la preventiva ed espressa autorizzazione o consenso informato dell'attore.

Come avviene in internet anche il cosiddetto "spamming telefonico", oltre a violare e disturbare la serenità, privacy e tranquillità dell'utente, provoca fastidi, danni e disagi, nonché continue distrazioni, stress ed ansie; infatti i predetti messaggi sms, quotidianamente inviati anche più volte al giorno, propongono notizie e contenuti

inutili, speculativi, promozionali, ripetitivi e fastidiosi, atti solo a disturbare e innervosire notevolmente l'utente, usurpando il suo tempo, distogliendo la sua attenzione e minando la sua concentrazione nel corso della giornata.

Tali messaggi sono quindi motivo di seri danni personali e patrimoniali, esistenziali e da perdita di chance: di conseguenza, il danneggiato matura un indiscutibile diritto al risarcimento di tutti i danni subiti, personali e patrimoniali, anche a causa dell'intasamento della memoria del telefono cellulare che non permette di ricevere importanti sms relativi alla propria vita sociale.

Infine sia i principi costituzionali che le attuali leggi ordinarie, come anche la normativa europea, prevedono l'introduzione di limiti e seria attenzione nell'utilizzo e nella gestione di dati personali degli utenti che, mal gestiti o senza consenso, possono arrecare danni all'individuo; quindi, può riconoscersi che il gestore di servizi telefonici esercita, comunque, un'attività pericolosa, ai sensi dell'articolo 2050 del Codice Civile per la ragione che i dati trattati contengono in sé una potenziale carica di pericolo e pregiudizio per la privacy dell'utente, ossia per uno dei beni primari dell'uomo, tutelato come diritto fondamentale, perciò lo stesso gestore di servizi telefonici è obbligato a usare ogni cautela per evitare che il rischio si tramuti in danno concreto.

Pertanto l'attore ha diritto al risarcimento del danno patrimoniale e personale.

- In ordine al danno patrimoniale, vanno considerate le attività compiute, con dispendio di tempo e di energie e le spese sostenute dall'istante, prima del giudizio, per opporsi al trattamento non consentito dei dati personali, mediante richieste e reclami al fine di ottenere la cessazione delle intrusioni, nella sua vita privata mediante l'invio di messaggi sms invasivi.

- Sotto il profilo del danno personale si considera il turbamento della qualità della vita ed i disturbi delle attività relazionali, il danno esistenziale, lo stress ed i patemi morali causati dalle continue e indesiderate interferenze e violazioni nella sfera privata e proprie abitudini.

## 2. Le sanzioni amministrative

Le sanzioni amministrative applicabili sono di tipo pecuniario, tuttavia in aggiunta alla sanzione pecuniaria è facoltà del Garante prevedere come sanzione accessoria, la pubblicazione in uno o più giornali, indicati nel provvedimento di applicazione, dell'ordinanza ingiunzione del Garante (art. 165). Tale sanzione accessoria è obbligatoria nel caso la violazione riguardi l'omessa o incompleta notificazione (art. 163).

Il potere sanzionatorio è attribuito dall'art. 166 al Garante, organo competente a ricevere il rapporto e ad irrogare le sanzioni. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689 ("Modifiche al sistema penale"), e successive modificazioni.

### 2.1. Omessa o inidonea informativa all'interessato

- L'omessa o inidonea informativa per trattamenti che non contengono dati sensibili (violazione delle disposizioni relative all'informativa di cui all'art. 13)[52] è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro[53].

- L'omessa o inidonea informativa nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17[54] o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati è punita con la sanzione amministrativa da cinquemila euro a trentamila euro.

- La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

[52] Art. 13 del d.lgs. 196/2003 "Informativa".
[53] Art. 161 del d.lgs. 196/2003.
[54] Art. 17 del d.lgs. 196/2003 "Trattamento che presenta rischi specifici".

## 2.2. Altre fattispecie

- La cessione dei dati in violazione di quanto previsto dall'articolo 16[55], comma 1, lettera b) (quando, ricorrendo l'ipotesi di cessazione del trattamento, i dati vengono ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti) è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.

- La cessione dei dati in violazione di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.

- La violazione della disposizione di cui all'articolo 84[56], comma 1 (quando vengono resi noti all'interessato o agli altri soggetti che, in determinate condizioni, possono riceverli in sua vece, dati idonei a rivelare lo stato di salute, facendo ciò non per il tramite di un medico designato dallo stesso interessato o dal titolare del trattamento) è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro[57].

## 2.3. Omessa o incompleta notificazione

Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37[58] e 38[59], ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione

[55] Art. 16 del d.lgs. 196/2003 "Cessazione del trattamento".
[56] Art. 84 del d.lgs. 196/2003 "Comunicazione di dati all'interessato".
[57] Art. 162 del d.lgs. 196/2003.
[58] Art. 37 d.lgs. 196/2003 "Notificazione del trattamento".
[59] Art. 38 d.lgs. 196/2003 "Modalità di notificazione".

dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica[60].

### 2.4. Omessa informazione o esibizione al Garante

Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2[61], e 157[62] è punito con la sanzione amministrativa del pagamento di una somma da quattromila euro a ventiquattromila euro[63].

## 3. Le sanzioni penali

Il Codice prevede tre delitti (articoli 167, 168 e 170) e due contravvenzioni[64] (articoli 169 e 171).

L'articolo 172 prevede che la condanna per uno dei delitti comporta l'applicazione della pena accessoria della pubblicazione della sentenza.

Per tutti i delitti è prevista la clausola "salvo che il fatto costituisca più grave reato".

[60] Art. 163 del d.lgs. 196/2003.
[61] Art**.** 150 d.lgs. 196/2003 "Provvedimenti a seguito del ricorso". Il comma 2 prevede che "Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto".
[62] Art**.** 38 d.lgs. 196/2003 "Richiesta di informazione e di esibizione di documenti".
[63] Art. 164 del d.lgs. 196/2003.
[64] Sono delitti i reati al cui verificarsi l'ordinamento penale ricollega la pena dell'ergastolo, della reclusione e della multa. Sono contravvenzioni i reati al cui verificarsi l'ordinamento penale ricollega la pena dell'arresto e dell'ammenda.

### 3.1. Trattamento illecito di dati

- Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18 e 19 (trattamenti effettuati da soggetti pubblici in relazione a dati diversi da quelli sensibili e giudiziari), 23 (disciplina della prestazione del consenso), 123 (dati relativi al traffico), 126 (dati relativi all'ubicazione) e 130 (comunicazioni indesiderate), ovvero in applicazione dell'articolo 129 (elenchi di abbonati), è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

- Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17 (trattamento che presenta rischi specifici), 20, 21, 22, commi 8 e 11 (trattamento di dati sensibili e giudiziari effettuato da soggetti pubblici), 25 (divieti di comunicazione e diffusione), 26 e 27 (garanzie per i dati sensibili e giudiziari) e 45 (trasferimenti vietati), è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni[65] [66].

[65] Art. 167 del d.lgs. 196/2003.
[66] Il Tribunale di Pescara, con una sentenza del 12 ottobre 2000 ha affermato che non risponde del reato previsto dall'art 167 del d.lgs. 196/2003 il giornalista che rivela dati relativi alla salute o sfera sessuale di un soggetto se hanno riguardo a fatti di interesse pubblico e abbiano la caratteristica della veridicità della notizia e l'essenzialità dell'informazione.
La Pretura di Palermo, con sentenza del 4 febbraio1999 ha ritenuto che costituisca trattamento illecito di dati l'archiviazione di dati raccolti in una banca dati elettronica per l'invio di lettere promozionali ai clienti senza il loro consenso.

### 3.2. Falsità nelle dichiarazioni e notificazioni al Garante

Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni[67].

### 3.3. Misure di sicurezza

- Chiunque, essendovi tenuto, omette di adottare le misure minime[68] previste dall'articolo 33 (misure minime) è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

- È previsto che all'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili[69].

[67] Art. 168 del d.lgs. 196/2003.
[68] Si rinvia al capitolo sulle misure di sicurezza.
[69] Art. 169 del d.lgs. 196/2003.

### 3.4. Inosservanza di provvedimenti del Garante

Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni[70].

### 3.5. Altre fattispecie

La violazione delle disposizioni di cui agli articoli 113, comma 1 ("Raccolta di dati e pertinenza") e 114 ("Controllo a distanza") è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300 "Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e nell'attività sindacale nei luoghi di lavoro e norme sul collocamento" (Statuto dei lavoratori)[71] [72].

.

[70] Art. 170 del d.lgs. 196/2003
[71] Art. 171 del d.lgs. 196/2003
[72] Articolo 38 della legge n. 300/1970 "Disposizioni penali":
«Le violazioni degli articoli 2, 5, 6, e 15, primo comma lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno.
Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente.
Quando per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.
Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale».

# SEZIONE II

# DOCUMENTAZIONE

# Indice documentazione

# REGOLAMENTO REGIONALE PER IL TRATTAMENTO DEI DATI SENSIBILI

Decreto del Presidente della Giunta Regionale 11 maggio 2006, n. 3/R

**Regolamento regionale recante: Regolamento per il trattamento dei dati personali sensibili e giudiziari di competenza della Regione, delle Aziende Sanitarie, degli Enti e Agenzie Regionali, degli Enti vigilati dalla Regione (Articoli 20 e 21 del decreto legislativo 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali)**

LA PRESIDENTE DELLA GIUNTA REGIONALE

Visto l'art. 121 della Costituzione (come modificato dalla Legge Costituzionale 22 novembre 1999, n. 1);

Visti gli art. 27 e 52 dello Statuto della Regione Piemonte;

Visti gli art. 20 e 21 del Decreto Legislativo 30 giugno 2006, n. 196;

vista la Deliberazione del Consiglio regionale n. 65-15263 del 9 maggio 2006;

emana

il seguente regolamento:

REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI DI COMPETENZA DELLA REGIONE, DELLE AZIENDE SANITARIE, DEGLI ENTI E AGENZIE REGIONALI, DEGLI ENTI VIGILATI DALLA REGIONE (ARTICOLI 20 E 21 DEL DECRETO LEGISLATIVO 30 GIUGNO 2003 N. 196 (CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI)

Art. 1

(Oggetto)

1. Il presente regolamento, ai sensi degli articoli 20 e 21 del Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), identifica i tipi di dati e le operazioni eseguibili da parte della Regione Piemonte, nonché da parte delle aziende sanitarie e organismi sanitari pubblici della Regione Piemonte, degli enti e agenzie regionali e degli altri enti per i quali la Regione esercita poteri di indirizzo e controllo, compresi gli enti che fanno riferimento a due o più regioni, nello svolgimento delle loro funzioni istituzionali, con riferimento ai trattamenti di dati sensibili e giudiziari:

a) effettuati per il perseguimento delle rilevanti finalità di interesse pubblico individuate dalla Parte seconda del d.lgs. 196/2003;

b) autorizzati da espressa disposizione di legge per rilevanti finalità di interesse pubblico, ove non sono legislativamente specificati i tipi di dati e le operazioni eseguibili.

Art. 2

(Disposizioni generali)

1. Ai fini del presente regolamento si applicano le definizioni contenute nell'articolo 4 del d.lgs. 196/2003.

2. Il trattamento dei dati avviene nel rispetto dei diritti e delle libertà fondamentali dell'interessato ed è compiuto quando, per lo svolgimento delle finalità di interesse pubblico, non è possibile il trattamento dei dati anonimi oppure di dati personali non sensibili o giudiziari.

Art. 3

(Tipi di dati e di operazioni eseguibili)

1. I dati sensibili e giudiziari oggetto di trattamento, le finalità di interesse pubblico perseguite, nonché le operazioni eseguibili sono individuati per i soggetti titolari di cui all'articolo 1, nelle schede allegate al presente regolamento.

Art. 4

(Pubblicazione sul Bollettino Ufficiale e diffusione su Internet)

1. Il presente regolamento è pubblicato sul Bollettino Ufficiale della Regione Piemonte ed è reso disponibile in Internet, nel sito WEB della Giunta e del Consiglio regionale.

Art. 5

(Dichiarazione d'urgenza)

1. Il presente regolamento è dichiarato urgente ai sensi dell'articolo 27, comma 7 dello Statuto ed entra in vigore il giorno successivo alla sua pubblicazione sul Bollettino Ufficiale della Regione.

Il presente regolamento sarà pubblicato nel Bollettino Ufficiale della Regione Piemonte.

È fatto obbligo a chiunque spetti di osservarlo e farlo osservare.

Torino, addì 11 maggio 2006

p. Mercedes Presso

Il Vicepresidente

Gianluca Susta

**ALLEGATO A (SCHEDE DA A1 A A33)**

Giunta regionale

Enti strumentali, ausiliari o comunque vigilati della Regione Piemonte:

- Agenzia regionale per la protezione ambientale;

- Agenzia regionale per i servizi sanitari;

- Istituto zooprofilattico sperimentale del Piemonte, Liguria e Valle d'Aosta;

- Agenzia Piemonte Lavoro;

- Ente per il Diritto allo studio universitario;

- Istituto di ricerche economico e sociali del Piemonte;

- Agenzie territoriali per la casa;

- Enti parco e riserve naturali,

- IPAB e aziende pubbliche di servizi alla persona;

- Agenzia regionale per le adozioni internazionali;

- Agenzia regionale delle strade del Piemonte (ARES);

- Agenzia interregionale per la gestione del fiume Po.

**ALLEGATO B (SCHEDE DA B1 A B41)**

Aziende unità sanitarie locali, aziende ospedaliere, istituti di ricerca e cura a carattere scientifico, aziende universitarie di qualsiasi tipo e natura operanti nell'ambito del servizio sanitario nazionale.

**ALLEGATO C (SCHEDE DA C1 A C14)**

Consiglio regionale.

**REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI**

(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione di dati personali)*

## ALLEGATO C

### Elenco trattamenti dei dati sensibili e giudiziari di competenza del Consiglio regionale, dagli Organi consiliari e loro membri

**Titolare: Consiglio regionale**

1 Nomine e designazioni

2 Instaurazione e gestione del rapporto di lavoro del personale *(compreso collocamento obbligatorio, assicurazioni integrative, assunzione oneri di difesa, procedure di conciliazione in materia di rapporto di lavoro, gestione cause di lavoro)*

3 Assicurazione rischi di morte, invalidità permanente e temporanea, dipendenti da infortunio o infermità, e assicurazione infortuni dei Consiglieri e Assessori regionali in carica

4
   A. Anagrafe patrimoniale dei titolari di cariche elettive e di cariche direttive
   B. Gestione economica, fiscale e previdenziale delle indennità, degli assegni vitalizi e delle reversibilità dei Consiglieri, ex Consiglieri e Assessori regionali

5 Attività di tutela amministrativa e giudiziaria

6 Difesa civica regionale

7 Strumenti di democrazia diretta (iniziativa legislativa popolare, petizioni e referendum)

8 Attività politica, di indirizzo e di controllo - sindacato ispettivo

9 Verifica elettorato passivo e requisiti per l'esercizio del mandato

10 Riconoscimento inabilità totale e permanente al lavoro degli eletti alla carica di Consigliere regionale

11 Documentazione dell'attività istituzionale del Consiglio (o Assemblea legislativa) regionale e degli Organi consiliari ( o assembleari)

12 Insindacabilità Consiglieri regionali

13 Patrocinio legale - rimborso spese legali amministratori e dipendenti regionali per fatti e atti connessi all'espletamento del servizio o del mandato

14 Attività del Comitato regionale per le comunicazioni

**REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI**

(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 1**

**DENOMINAZIONE DEL TRATTAMENTO:**

**NOMINE E DESIGNAZIONI**

**FONTI NORMATIVE:**

1. Statuto Regionale;
2. Legge Regionale n. 39/95 (Criteri e disciplina delle nomine ed incarichi pubblici di competenza regionale e dei rapporti tra la Regione ed i soggetti nominati)
3. Decreto del Presidente della Repubblica 22 dicembre 1986, n. 917 "Testo Unico delle imposte sui redditi (TUIR)".

**ALTRE FONTI ISTITUTIVE:**

Regolamento interno del Consiglio regionale.

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato alla designazione e nomina di rappresentanti in commissioni, enti, uffici, ecc. e all'applicazione di disposizioni in materia di tributi, deduzioni e detrazioni d'imposta).

Art. 65 D. Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".
Art. 66 D. Lgs. 196/2003 "Materia tributaria e doganale".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | **\|X\|** | | | | | | |
| Convinzioni religiose | \|_\| | filosofiche | \|_\| | d'altro genere | \|_\| | | |
| Opinioni politiche | \|_\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | | **\|X\|** |
| Stato di salute: | attuale | **\|X\|** | pregresso | **\| X \|** | anamnesi familiare | \|_\| | |
| | | | | | anche relativo a familiari dell'interessato | **\| X \|** | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | **\|X\|** | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato **|X|**
acquisizione da altri soggetti esterni **|X|**

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** **|X|**

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** **|X|**

Per le nomine e designazioni di competenza del Consiglio regionale, la comunicazione delle candidature, con specificazione del Consigliere regionale o del soggetto proponente, viene inviata a tutti i Consiglieri.
Successivamente alla decisione del Consiglio la comunicazione viene inviata, nel caso di designazione, al soggetto cui spetta la nomina.

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

1. **Fase di presentazione delle candidature**

a. Nella fase di presentazione delle candidature l'interessato dichiara l'insussistenza di situazioni di interdizione legale ovvero di interdizione temporanea dagli uffici ovvero di condanne con sentenze irrevocabili a pene detentive o reclusioni a seguito di particolari reati. Inoltre può dichiarare il possesso dei requisiti richiesti dalla legge oppure la sussistenza o meno di situazioni ostative (incompatibilità, ineleggibilità, incandidabilità), che siano prescritte per le funzioni da ricoprire.
Nell'espletamento delle procedure previste dalla normativa in materia copia di tale documentazione viene trasmessa ai Consiglieri ed all'Organo consiliare competente ad esaminare le candidature e a esprimere il parere di merito.

b. I dati giudiziari sono acquisiti dalla Procura della Repubblica e dal Tribunale nella fase di controllo della veridicità delle dichiarazioni dei candidati circa l'assenza di condanne e carichi pendenti; tale controllo può essere fatto a campione oppure periodicamente, secondo la normativa vigente.
Tali dichiarazioni entrano a far parte del fascicolo cartaceo relativo all'intera procedura della nomina.

**2. Fase successiva alla nomina o designazione**

a. Nella fase successiva alla nomina, fra gli adempimenti previsti, il nominato certifica/dichiara l'appartenenza a società, enti o associazioni di qualsiasi genere oppure quando tale appartenenza o vincolo associativo possa determinare un conflitto di interesse con l'incarico assunto.
Tali dichiarazioni possono essere integrate con riferimento alle appartenenze poste in essere successivamente al momento della nomina.
Inoltre dichiara l'assenza di cause ostative a ricoprire l'incarico.

b. Se richiesto dalla normativa l'Amministrazione verifica la veridicità delle dichiarazioni, acquisendo il certificato del casellario giudiziario ed il certificato di carichi pendenti.

c. L'Amministrazione verifica, altresì la rimozione di eventuali cause di incompatibilità con l'incarico assunto.

Per i nominati le dichiarazioni riferite alla gestione economico, fiscale e previdenziale delle indennità vengono acquisite dagli uffici competenti.

**3. Procedimento di decadenza o revoca**

Comunicazione dei dati sensibili solo nel caso di trasmissione all'Organo consiliare competente per attivazione del procedimento per la dichiarazione di decadenza o di revoca previsto dalla normativa.

**4. Procedimento di nomina o designazione in via sostitutiva**

Qualora il Consiglio non proceda alla nomina o designazione nei termini previsti dalla normativa la competenza è trasferita all'organo deputato in sede di esercizio dei poteri sostitutivi.

**5. Trattamento accidentale di dati sensibili**

I dati sensibili, relativi in particolare dati sanitari, possono essere accidentalmente rilevati, ma non costituiscono oggetto del trattamento in questione e comunque non vengono trattati per le finalità perseguite nell'ambito del trattamento descritto in questa scheda.

**6. Trattamento di dati sensibili nelle Regioni**

I dati sensibili relativi all'origine razziale ed etnica sono trattati, ove previsto da specifica normativa, per assicurare la rappresentanza di soggetti appartenenti a particolari gruppi di popolazione (minoranze etniche, immigrati, ecc.).

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente le nomine e designazioni di competenza regionale/provinciale e la relativa gestione economico, fiscale e previdenziale delle indennità.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 2**

**DENOMINAZIONE DEL TRATTAMENTO:**

**INSTAURAZIONE E GESTIONE DEL RAPPORTO DI LAVORO DEL PERSONALE (compreso collocamento obbligatorio, assicurazioni integrative, assunzione oneri di difesa, procedure di conciliazione in materia di rapporto di lavoro, gestione cause di lavoro)**

**FONTI NORMATIVE:**

1. Codice civile;
2. Decreto del Presidente della Repubblica 30 giugno 1965, n. 1124 "Testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali";
3. Legge 20 maggio 1970, n. 300 “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell'attività sindacale nei luoghi di lavoro e norme sul collocamento”;
4. Legge 5 febbraio 1992, n. 104 “Legge – quadro per l’assistenza, l’integrazione sociale e i diritti delle persone Handicappate”;
5. Decreto legislativo 19 settembre 1994, n. 626 “Attuazione della direttiva 89/391/CEE, della direttiva 89/654/CEE, della direttiva 89/655/CEE, della direttiva 89/656/CEE, della direttiva 90/269/CEE, della direttiva 90/270/CEE, della direttiva 90/394/CEE e della direttiva 90/679/CEE, riguardanti il miglioramento della sicurezza e della salute dei lavoratori durante il lavoro”;
6. Legge 8 agosto 1995, n. 335 "Riforma del sistema pensionistico obbligatorio e complementare";
7. Legge 12 marzo 1999, n. 68 “Norme per il diritto al lavoro dei disabili”;
8. Decreto del Presidente della Repubblica 29 ottobre 2001, n. 461 "Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermità da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonché per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie";
9. Decreto legislativo 30 marzo 2001, n. 165 “Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche”;
10. Legge 14 febbraio 2003, n. 30 “Delega al Governo in materia di occupazione e mercato del lavoro”;
11. Legge regionale n. 51/97 (Norme sull'organizzazione degli uffici e sull'ordinamento del personale regionale);
12. Legge regionale n. 33/98 (Nuovo assetto organizzativo dei gruppi consiliari e modifiche alla normativa sul personale dei gruppi);
13. Legge regionale n. 39/98 (Norme sull'organizzazione degli uffici di comunicazione e sull'ordinamento del personale assegnato).

**ALTRE FONTI ISTITUTIVE:**
Contratti collettivi, accordi di settore e decentrati, concertazioni con le organizzazioni sindacali, regolamenti consiliari e deliberazioni dell'Ufficio di Presidenza.

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'instaurazione e gestione dei rapporti di lavoro dipendente di qualunque tipo, anche a tempo parziale o temporaneo e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato, compresi gli adempimenti a specifici obblighi o allo svolgimento di compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro).

Art. 112 D.Lgs. 196/2003 "Finalità di rilevante interesse pubblico".
Art. 68 D.Lgs. 196/2003 "Benefici economici ed abilitazioni".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|**X**\| | | | | | | |
| Convinzioni religiose | \|**X**\| | filosofiche | \|_\| | d'altro genere | \|_\| | | |
| Opinioni politiche | \|**X**\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | | \|**X**\| |
| Stato di salute: | attuale | \|**X**\| | pregresso | \|**X**\| | anamnesi familiare | \|_\| | |
| | | | | | anche relativo a familiari dell'interessato | \|**X**\| | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|**X**\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

| | |
|---|---|
| informatizzato | \|**X**\| |
| manuale | \|**X**\| |

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

| | |
|---|---|
| raccolta diretta presso l'interessato | \|**X**\| |
| acquisizione da altri soggetti esterni | \|**X**\| |

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** \|**X**\|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|

- di altro titolare |_|

**Comunicazione** **|X|**

Vari soggetti pubblici e privati in sede di controllo delle dichiarazioni sostitutive rese ai sensi del D.P.R. 445/2000, Ufficio Imposte, EE.LL, INPDAP - INPS – INPGI – Istituti scolastici – UNIVERSITA'(per erogazione trattamento di pensione: L. 335/1995), commissioni mediche (per visite medico-collegiali: CCNL, CCNL di comparto; L. 335/1995; D.P.R. 461/2001; regolamenti regionali), comitato di verifica per le cause di servizio (nell'ambito della procedura per riconoscimento di causa di servizio/equo indennizzo ai sensi del D.P.R. 461/2001), INAIL e Autorità di P.S. (per denuncia infortunio: D.P.R. 1124/1965), Strutture sanitarie competenti (per visite fiscali: CCNL, CCNL di comparto), Enti di appartenenza dei collaboratori comandati in entrata, altri Enti per i dati dei collaboratori ivi trasferiti; Dipartimento Funzione Pubblica per i dati relativi ai permessi per cariche sindacali e funzioni pubbliche elettive (art. 50 D.Lgs. 165/2001) e per i dati relativi all'attività extra-impiego (art. 53 D.Lgs. 165/2001), soggetti pubblici e privati a cui ai sensi delle leggi regionali/provinciali viene affidato il servizio di formazione del personale (es. corsi per categorie protette); Amministrazioni provinciali e Centro regionale per l'impiego o all'Organismo competente in ordine al prospetto informativo delle assunzioni, cessazioni e modificazioni del rapporto di lavoro redatto ai sensi della L. 68/1999; Autorità giudiziaria (C.P. e C.P.P.), OO.SS. (dati relativi ai dipendenti che hanno conferito delega o hanno fruito di permessi sindacali per la specifica organizzazione sindacale e dati relativi ai dipendenti nell'ambito dell'istruttoria del progetto telelavoro). La comunicazione può essere effettuata anche sulla base di altre specifiche normative di settore e per perseguire le finalità di rilevante interesse pubblico oggetto della scheda in esame.

**Diffusione** |_|

***DESCRIZIONE DEL TRATTAMENTO:***

Il trattamento concerne tutti i dati relativi alla instaurazione e gestione del rapporto di lavoro a partire dai procedimenti concorsuali o altre procedure di selezione, nonché relativi ad altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato (collaborazioni coordinate e continuative, stages, tirocini, borse di studio, lavoro interinale, ecc.).

I dati sono oggetto di trattamento sia in modo centralizzato, presso le strutture organizzative competenti per materia, sia presso le strutture organizzative di assegnazione, limitatamente al personale assegnato.

I dati provengono all'Amministrazione su iniziativa degli interessati e/o su comunicazione di soggetti terzi, anche previa richiesta dell'Amministrazione. I dati sono registrati e conservati sia in forma cartacea che informatizzata e vengono trattati ai fini dell'applicazione dei vari istituti contrattuali e di legge. Il trattamento ha ad oggetto ogni attività ed operazioni

concernenti la gestione giuridica, economica, previdenziale, fiscale e pensionistica del personale comprese le attività di formazione del personale, assicurazioni integrative, procedure di conciliazione in materia di rapporto di lavoro, agevolazioni economiche, forme di contributi/agevolazioni al personale dipendente, adempimenti in materia di igiene e sicurezza D.Lgs. 626/1994, assunzioni oneri di difesa, adempimenti in materia di diritto al lavoro dei disabili (collocamento obbligatorio), "osservatorio delle competenze".

Si comunicano, per quanto di competenza, i seguenti dati:

- a vari soggetti pubblici e privati: quelli necessari per effettuare il controllo delle dichiarazioni sostitutive rese ai sensi del D.P.R. 445/2000;
- alle Organizzazioni sindacali: cognome e nome dei dipendenti che hanno rilasciato delega, nonché di coloro che hanno fruito di permessi sindacali per la specifica organizzazione sindacale; dati relativi ai dipendenti nell'ambito dell'istruttoria del progetto telelavoro;
- agli Istituti assicurativi (INPS-INAIL-INPGI), agli Enti assistenziali e previdenziali e alle strutture sanitarie competenti: stato di salute;
- agli Uffici giudiziari: su richiesta, dati di singoli dipendenti riferiti a indagini;
- ai soggetti pubblici e privati che svolgono attività di formazione per categorie protette: dati del personale da formare;
- alle Amministrazioni provinciali e al Centro regionale per l'impiego o all'Organismo competente: dati anagrafici degli assunti per le categorie protette;
- ad altre amministrazioni o enti in relazione ai collaboratori comandati e trasferiti: dati dei dipendenti.

***FLUSSO INFORMATIVO:***

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente l'instaurazione e gestione del rapporto di lavoro del personale.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 3**

**DENOMINAZIONE DEL TRATTAMENTO:**

**ASSICURAZIONE RISCHI DI MORTE, INVALIDITÀ PERMANENTE E TEMPORANEA, DIPENDENTI DA INFORTUNIO O INFERMITÀ, E ASSICURAZIONE INVALIDITÀ DEI CONSIGLIERI E ASSESSORI REGIONALI IN CARICA**

**FONTI NORMATIVE:**

1. Legge regionale n. 57/81 (Assicurazione contro gli infortuni dei Consiglieri regionali)

**ALTRE FONTI ISTITUTIVE:**

//

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato alla stipulazione di contratti di assicurazione e all'adempimento dei relativi obblighi).

Art.68 D.Lgs.196/2003 "Benefici economici ed abilitazioni".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\| | | | | | | |
| Convinzioni religiose | \|_\| | filosofiche | \|_\| | d'altro genere | \|_\| | | |
| Opinioni politiche | \|_\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | \|_\| | |
| Stato di salute: | attuale | \|**X**\| | pregresso | \|**X**\| | anamnesi familiare | \|**X**\| | |
| | | | | | anche relativo a familiari dell'interessato | \|_\| | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|_\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**
informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**
raccolta diretta presso l'interessato **|X|**
acquisizione da altri soggetti esterni **|X|**

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** **|X|**

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|

- di altro titolare **|_|**

**Comunicazione** **|X|**
Compagnia assicurativa
La comunicazione è effettuata solo in attuazione di specifici obblighi contrattuali o qualora l'interessato ne abbia fatto richiesta.

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

I dati concernenti l'anamnesi vengono acquisiti su moduli cartacei presso gli assicurati e trasmessi alla compagnia assicurativa

Qualora si verifichi uno degli eventi il cui rischio è coperto dalla polizza assicurativa, stipulata dall'Amministrazione regionale ai sensi della normativa vigente in materia, gli assicurati possono spedire all'Amministrazione i certificati sanitari necessari per la denuncia. L'Amministrazione li trasmette all'Assicurazione tramite comunicazione protocollata.

**FLUSSO INFORMATIVO:**

- L'amministrazione funge normalmente solo da tramite fra il Consigliere, l'Assessore regionale e la Compagnia Assicurativa, in tale ottica non viene protocollata la documentazione inerente l'anamnesi ed i certificati sanitari necessari per la denuncia, ma solamente la comunicazione con cui viene trasmessa tale documentazione, quindi viene classificata, fascicolata, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005).

- Assegnazione al servizio/struttura competente.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 4**

**DENOMINAZIONE DEL TRATTAMENTO:**

**A. ANAGRAFE PATRIMONIALE DEI TITOLARI DI CARICHE ELETTIVE E DI CARICHE DIRETTIVE**
**B. GESTIONE ECONOMICA, FISCALE E PREVIDENZIALE DELLE INDENNITA', DEGLI ASSEGNI VITALIZI E DELLE REVERSIBILITA' DEI CONSIGLIERI, EX CONSIGLIERI E ASSESSORI REGIONALI**

**FONTI NORMATIVE:**

1. Legge 5 luglio 1982, n. 441 "Disposizioni per la pubblicità della situazione patrimoniale di titolari di cariche elettive e di cariche direttive di alcuni enti";
2. Decreto del Presidente della Repubblica 22 dicembre 1986, n. 917 "Testo Unico delle imposte sui redditi (TUIR)";
3. Decreto legislativo 16 settembre 1996, n. 564 "Attuazione della delega conferita dall'art. 1, comma 39, della legge 8 agosto 1995, n. 335, in materia di contribuzione figurativa e di copertura assicurativa per periodi non coperti da contribuzione";
4. Legge regionale n. 16/83 (Norme per la pubblicita' dello stato patrimoniale e tributario dei Consiglieri regionali e degli Amministratori di Enti ed Istituti operanti nell'ambito della Regione Piemonte)

**ALTRE FONTI ISTITUTIVE:**

Regolamento interno, consiliare o dell'Ufficio di Presidenza.

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'applicazione di disposizioni in materia di tributi, deduzioni e detrazioni d'imposta ed al riconoscimento di benefici connessi all'invalidità civile).

Art. 65 D. Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".
Art. 66 D. Lgs. 196/2003 "Materia tributaria e doganale".
Art. 68 D. Lgs. 196/2003 "Benefici economici ed abilitazioni".

**TIPOLOGIA DEI DATI TRATTATI:**
Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\| | | | | | | |
| Convinzioni religiose | \|**X**\| | filosofiche | \|_\| | d'altro genere | \|**X**\| | | |
| Opinioni politiche | \|**X**\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | \|**X**\| | |
| Stato di salute: | attuale | \|**X**\| | pregresso | \| **X** \| | anamnesi familiare | \|_\| | |
| | | | | | anche relativo a familiari dell'interessato | \|**X**\| | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|**X**\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato \|**X**\|
manuale \|**X**\|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

| | |
|---|---|
| raccolta diretta presso l'interessato | \|**X**\| |
| acquisizione da altri soggetti esterni | \|_\| |

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** \|**X**\|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

| | |
|---|---|
| - dello stesso titolare | \|_\| |
| - di altro titolare | \|_\| |

**Comunicazione** \| **X** \|
Comunicazione al Ministero dell'interno dei dati relativi all'anagrafe degli amministratori regionali e provinciali.
Base normativa: art. 76 D.Lgs. 18/08/2000, n. 267.

**Diffusione** \|_\|

**DESCRIZIONE DEL TRATTAMENTO:**

1. Per i titolari di cariche – Consiglieri e Assessori - e/o di cariche direttive la dichiarazione riferita alla situazione patrimoniale viene acquisita dagli uffici competenti. Da elementi contenuti nella dichiarazione integrale dei redditi si possono desumere dati sensibili, come per esempio dai seguenti dati riguardanti:
i vari codici di identificazione che contraddistinguono gli oneri per i quali è prevista la detrazione d'imposta spettante per :
"erogazioni liberali in denaro a favore dei movimenti e partiti politici",
"erogazioni liberali in denaro a favore delle organizzazioni non lucrative di utilità sociale (ONLUS), delle iniziative umanitarie, religiose, o laiche, gestite da fondazioni, associazioni, comitati ed enti individuati con decreto del presidente del consiglio dei mInistri nei paesi non appartenenti all'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE)",
"i contributi associativi versati dai soci alle società di mutuo soccorso che operano esclusivamente nei settori di cui all'art. 1 della L. 15 aprile 1886, n. 3818, al fine di assicurare ai soci un sussidio nei casi di malattia, di impotenza al lavoro o di vecchiaia, ovvero, in caso di decesso, un aiuto alle loro famiglie",
"le spese sostenute per i servizi di interpretariato dai soggetti riconosciuti sordomuti ai sensi della L. 26 maggio 1970, n. 381",
"erogazioni liberali in denaro a favore delle istituzioni religiose" specificate nelle istruzioni per la compilazione delle dichiarazioni dei redditi,
"spese mediche e di assistenza specifica dei portatori di handicap".
2. Per i Consiglieri, ex Consiglieri e Assessori le dichiarazioni riferite alla gestione economico, fiscale e previdenziale delle indennità, degli assegni vitalizi e delle reversibilità vengono acquisite dagli uffici competenti. Dagli elementi indicati nelle dichiarazioni ai fini della deduzione per familiari a carico e per assicurare la progressività dell'imposizione si possono desumere dati sensibili, visto che coinvolgono la situazione familiare.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente la situazione patrimoniale dei Consiglieri, degli Assessori e dei titolari di cariche direttive e la gestione economico, fiscale e previdenziale dei Consiglieri, degli ex Consiglieri e degli Assessori.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Pubblicazione sul Bollettino Ufficiale della Regione ( supplemento straordinario, con diffusione limitata dalla L.R. 16/83).

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".
- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 5**

**DENOMINAZIONE DEL TRATTAMENTO:**

## ATTIVITÀ DI TUTELA AMMINISTRATIVA E GIUDIZIARIA

**FONTI NORMATIVE:**

1. Disciplina statale sul contenzioso di settore (costituzionale, civile, penale, amministrativo, contabile, ecc.).

**ALTRE FONTI ISTITUTIVE:**

//

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato alla tutela dei diritti in occasione di procedimenti inerenti fatti o atti connessi all'espletamento del mandato o del servizio).

Art. 65 D.Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".
Art. 67 D.Lgs. 196/2003 "Attività di controllo e ispettive".
Art. 71 D.Lgs. 196/2003 "Attività sanzionatorie e di tutela".
Art. 112 D.Lgs. 196/2003 "Finalità di rilevante interesse pubblico".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\| | | | | | | |
| Convinzioni religiose | \|_\| | filosofiche | \|_\| | d'altro genere | \|_\| | | |
| Opinioni politiche | \|**X**\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | | \|**X**\| |
| Stato di salute: attuale | \|**X**\| | pregresso | \|**X**\| | anamnesi familiare | \|_\| | | |
| | | | | anche relativo a familiari dell'interessato | \|**X**\| | | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|**X**\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |**X**|

In relazione e nell'ambito dei singoli procedimenti, cause e giudizi vengono comunicati i soli dati pertinenti e indispensabili per perseguire le esclusive finalità di tutela amministrativa e giudiziaria, secondo quanto previsto dalla normativa applicabile in particolare:
- per il processo civile c.c., c.p.c. e normativa connessa e speciale;
- per il processo penale c.p., c.p.p. e normativa connessa e speciale;
- per il processo amministrativo L. 1034/1971, R.D. 1054/1924 e normativa connessa e speciale ;
- per il giudizio contabile. R.D. 1214/1934, L. 20/1994 e normativa connessa e speciale.

a) strutture amministrative regionali, Autorità giudiziaria, Avvocati, consulenti tecnici incaricati dall'Autorità giudiziaria, Enti previdenziali, Enti di patronato, Sindacati, Incaricati di indagini difensive, proprie e altrui, Consulenti della controparte (per le finalità di corrispondenza sia in fase pregiudiziale sia in corso di causa),;

b) Società assicuratrici (per la valutazione e la copertura economica degli indennizzi, per la responsabilità civile verso terzi);

c) Struttura sanitaria e comitato di verifica per le cause di servizio (per la relativa trattazione amministrativa ai sensi del DPR 461/2001);

d) Alle Amministrazioni coinvolte nel caso in cui venga presentato il ricorso straordinario al Capo dello Stato (per la relativa trattazione ai sensi della legge n.1199/1971).

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

Il trattamento di dati sensibili e giudiziari può avvenire nell'ambito dell'intero procedimento di gestione dei contenziosi.

Il trattamento comprende la raccolta dei dati da parte dei soggetti del procedimento, il loro utilizzo, l'eventuale elaborazione ai fini istruttori nell'iter procedurale (i dati possono essere oggetto di memorie, ricorsi o controricorsi, corrispondenza fra uffici, organi giudiziari, cancellerie, avvocati di parte, altri soggetti del procedimento legale, ecc.) e la conclusiva archiviazione nell'archivio cartaceo dei fascicoli processuali e nella corrispondente banca dati su supporto informatico.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente l'attività legale e contenziosa.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 6**

**DENOMINAZIONE DEL TRATTAMENTO:**

**DIFESA CIVICA REGIONALE**

**FONTI NORMATIVE:**

1. Statuto regionale;
2. Legge regionale n. 50/81 (Istituzione dell'ufficio del Difensore Civico) e Legge regionale n. 47/85 (Norme relative alla estensione delle competenze del Difensore Civico alle strutture amministrative del Servizio Sanitario e delle UU.SS.SS.LL. operanti nel territorio regionale)
3. Legge 5 febbraio 1992 n. 104 "Legge – quadro per l'assistenza. l'integrazione sociale e i diritti delle persone handicappate";
4. Legge 15 maggio 1997, n. 127 "Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimento di decisione e controllo";
5. Legge 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
6. Decreto legislativo 18 agosto 2000, n. 267 "Testo unico delle leggi sull'ordinamento degli enti locali".

**ALTRE FONTI ISTITUTIVE:**

//

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato alla difesa civica).

Art. 73 D. Lgs. 196/2003 "Altre finalità in ambito amministrativo e sociale".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | **\|X\|** | | | | | | |
| Convinzioni religiose | **\|X\|** | filosofiche | **\|X\|** | d'altro genere | **\|X\|** | | |
| Opinioni politiche | **\|X\|** | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | **\|X\|** | |
| Stato di salute: attuale | **\|X\|** | pregresso | **\|X\|** | anamnesi familiare | **\|_\|** | | |
| | | | | anche relativo a familiari dell'interessato | **\|X\|** | | |
| Vita sessuale | **\|X\|** | | | | | | |
| Dati giudiziari | **\|X\|** | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato **|X|**
acquisizione da altri soggetti esterni **|X|**

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** **|X|**

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|

- di altro titolare |_|

**Comunicazione** **|X|**

Pubbliche amministrazioni, enti e soggetti privati, gestori o concessionari di pubblico servizio o privati coinvolti nell'attività istruttoria.
Base normativa: Statuto regionale - Legge regionale o provinciale in materia di difesa civica - L. 104/1992 – L. 127/1997 – L. 241/1990 – D. Lgs. 267/2000 - Regolamento consiliare.

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

Attivazione di interventi di difesa civica, a seguito d'istanza o d'ufficio, per la tutela di chiunque vi abbia diretto interesse o per la tutela di interessi collettivi e diffusi in riferimento a provvedimenti, atti, fatti, comportamenti ritardati, omessi o comunque irregolarmente compiuti da uffici e servizi:

1. dell'Amministrazione regionale o provinciale;
2. degli enti, istituti, consorzi e aziende dipendenti o sottoposti a vigilanza o controllo regionale/ provinciale oppure comunque costituiti con legge regionale/provinciale;
3. delle Strutture sanitarie locali e aziende ospedaliere; degli enti locali in riferimento alle funzioni amministrative ad essi delegate dalla Regione o dalla Provincia;
4. delle Amministrazioni periferiche dello Stato con esclusione di quelle che operano nei settori della difesa, della sicurezza pubblica e della giustizia (art. 16 legge 15 maggio 1997, n. 127);
5. delle società o altri soggetti gestori di pubblico servizio;
6. degli enti pubblici, che abbiano stipulato convenzioni per l'esercizio della difesa civica;
7. dei Comuni ed aziende municipalizzate o collegate.

Nei casi sopra indicati il Difensore civico interviene a richiesta di singoli interessati o d'ufficio, di enti, associazioni e formazioni sociali, allorché siano stati esperiti ragionevoli tentativi per rimuovere i ritardi, le irregolarità o le disfunzioni.
Il Difensore civico può intervenire anche in riferimento ad atti definitivi o a procedimenti conclusi. Il Difensore civico può anche segnalare eventuali disfunzioni riscontrate presso altre pubbliche amministrazioni, sollecitandone la collaborazione per il perseguimento delle finalità di imparzialità e buon andamento della pubblica amministrazione di cui all'art. 97 della Costituzione.
Il Difensore civico può inoltre intervenire invitando i soggetti pubblici o privati operanti nelle materie di competenza regionale/provinciale, a fornire notizie, documenti, chiarimenti.

**FLUSSO INFORMATIVO:**

- I dati sensibili pervengono al Difensore civico attraverso i reclami degli interessati o comunicazione di soggetti terzi, anche previa richiesta del Difensore civico.

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), dell'istanza e degli atti inerenti l'attività di difesa civica.

- Assegnazione al funzionario competente.

- Istruttoria e trattazione del caso, di norma mediante corrispondenza cartacea, colloqui telefonicime posta elettronica con i soggetti coinvolti, pubbliche amministrazioni o enti privati e con lo stesso cittadino ricorrente.

- Impostazione di un fascicolo cartaceo contenente l'istanza del cittadino e documentazione pertinente; il fascicolo può anche essere inserito in un archivio informatico.

- Comunicazione delle fasi istruttorie e dell'esito ai soggetti interessati.

- Aggregazione dei dati in forma anonima per indagini statistiche, per la relazione annuale e le relazioni saltuarie del Difensore civico.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- In tale fase, se l'interessato lo richiede, la documentazione sanitaria fornita dallo stesso viene restituita o ne viene rilasciata copia se acquisita direttamente dall'ufficio. Qualora si tratti di documentazione sanitaria non duplicabile agevolmente (es. lastre radiografiche) le strutture amministrative invitano l'interessato a ritirala; tale documentazione in caso di mancato ritiro viene comunque conservata in archivio con le modalità previste dalla legge.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi

dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 “Norme relative all'ordinamento ed al personale degli archivi di Stato”.

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 7**

**DENOMINAZIONE DEL TRATTAMENTO:**

**STRUMENTI DI DEMOCRAZIA DIRETTA (iniziativa legislativa popolare, petizioni e referendum)**

**FONTI NORMATIVE:**

1. Costituzione, art. 123 e ss.;
2. Statuto regionale;
3. Legge regionale n. 4/73 (Iniziativa popolare e degli enti locali e referendum abrogativo e consultivo).

**ALTRE FONTI ISTITUTIVE:**

Regolamento interno del Consiglio regionale;
Delibera Ufficio di Presidenza n. 8-1335 del 15.01.2003.

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'esercizio dell'iniziativa popolare, alle richieste di referendum, alla presentazione di petizioni e alla verifica della relativa regolarità).

Art. 65 D. Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".
Art. 67 D. Lgs. 196/2003 "Attività di controllo e ispettive".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|**X**\| | | | | | | |
| Convinzioni religiose | \|**X**\| | filosofiche | \|**X**\| | d'altro genere | \|**X**\| | | |
| Opinioni politiche | \|**X**\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | | \|**X**\| |
| Stato di salute: | attuale \|_\| | pregresso | \|_\| | anamnesi familiare | \|_\| | | |
| | | | | anche relativo a familiari dell'interessato | \|_\| | | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|_\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |_|

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

**A.** Per l'iniziativa popolare ed il referendum il trattamento dei dati, pur nella diversità delle procedure collegate al singolo istituto, prevede una serie di adempimenti comuni.

Limitando il discorso ai passaggi che possono coinvolgere dati sensibili, questi adempimenti comprendono una fase di promozione dell'iniziativa (con il deposito delle firme richieste e delle relative certificazioni anagrafiche comprovanti l'iscrizione nelle liste elettorali di un Comune della Regione o dichiarazioni sostitutive) e una fase di verifica della loro regolarità da parte della struttura incaricata.

Segue la raccolta delle sottoscrizioni (con le relative certificazioni come sopra indicato o dichiarazioni sostitutive), nelle modalità e nei termini previsti dalla normativa regionale per dare corso all'iniziativa.

I dati e i certificati anagrafici/dichiarazioni sostitutive relativi ai promotori e ai sottoscrittori possono anche essere elaborati e racchiusi in apposita banca dati accessibile alla sola struttura amministrativa interna al Consiglio.

**B.** Il trattamento e il flusso dei dati dei soggetti che depositano petizioni risulta più semplice: sono limitati nei contenuti (di regola nome, cognome e residenza), non sono certificati né verificati.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente gli strumenti di democrazia diretta.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 8**

**DENOMINAZIONE DEL TRATTAMENTO:**

**ATTIVITÀ POLITICA, DI INDIRIZZO E DI CONTROLLO - SINDACATO ISPETTIVO**

**FONTI NORMATIVE:**

4. Costituzione, art. 126 e ss.;
5. Statuto regionale.

**ALTRE FONTI ISTITUTIVE:**

Regolamento interno del Consiglio regionale.
Circolare Presidente C.R. "Istruttoria preliminare dei progetti di legge e degli atti in indirizzo e di sindacato ispettivo"

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'attività di controllo, di indirizzo politico e di sindacato ispettivo ed alla relativa documentazione).
Art. 65 D. Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".
Art. 67 D. Lgs. 196/2003 "Attività di controllo e ispettive".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | |**X**| | | | | |
| Convinzioni religiose | |**X**| filosofiche | |**X**| d'altro genere | |**X**| |
| Opinioni politiche | |**X**| | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | | |**X**| |
| Stato di salute: | attuale | |**X**| pregresso | |**X**| anamnesi familiare | |_| |
| | | | | | | anche relativo a familiari dell'interessato | | **X** | |
| Vita sessuale | |**X**| | | | | |
| Dati giudiziari | |**X**| | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |_|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |**X**|

Giunta regionale, Consiglieri e Gruppi consiliari,
Enti pubblici interessati, strutture amministrative interessate.
Base normativa: Statuto regionale e Regolamento interno del Consiglio.

**Diffusione** | **X** |

Vengono diffusi i soli dati indispensabili ad assicurare il rispetto del principio della pubblicità dell'attività istituzionale degli organi di indirizzo e controllo politico.
Base normativa: Regolamento interno del Consiglio, nel rispetto dello specifico quadro di garanzie riconducibili a quanto previsto dall'art. 65, comma 5 D.Lgs. 196/2003.

**DESCRIZIONE DEL TRATTAMENTO:**

### 4. Attività di sindacato ispettivo

Nell'ambito delle proprie prerogative il Consigliere regionale può formulare atti di sindacato ispettivo (interrogazioni e interpellanze) alla Giunta regionale, con le modalità stabilite dallo Statuto regionale e dal Regolamento interno del Consiglio regionale.

Questa attività può comportare il trattamento di dati sensibili e dati di carattere giudiziario riconducibili alle persone oggetto dell'atto ispettivo.

Agli atti di sindacato ispettivo può essere fornita risposta scritta, orale (in aula oppure in Commissione consiliare competente per materia).

### 5. Attività di indirizzo politico

Nell'ambito delle proprie prerogative il Consigliere regionale può formulare atti di indirizzo politico (mozioni, ordini del giorno, risoluzioni) secondo le modalità stabilite dallo Statuto regionale e dal Regolamento interno del Consiglio regionale.

Questa attività può comprendere (anche se in misura molto limitata) il trattamento di dati sensibili e di carattere giudiziario riconducibili a persone eventualmente citate in detti atti.

Quando l'atto è approvato dall'Assemblea segue la trasmissione agli organi interessati (Consiglieri, Giunta, strutture amministrative del Consiglio e della Giunta regionale, Enti pubblici).

### 6. Diffusione

La diffusione dei dati sensibili o giudiziari inerenti l'attività ispettiva e di indirizzo politico può essere effettuata nelle forme previste dal Regolamento interno del Consiglio e nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5, D.Lgs. 196/2003. Si rinvia anche a quanto specificato nell'apposita scheda n. 11 relativa alla "Documentazione dell'attività istituzionale del Consiglio regionale e degli organi consiliari".

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D. Lgs. 82/2005), della documentazione inerente l'attività di indirizzo, controllo e sindacato ispettivo.

- Assegnazione alla struttura competente.

- Espletamento delle procedure amministrative previste per l'iscrizione all'Ordine del giorno generale del Consiglio (o Assemblea legislativa), relativa comunicazione ai Consiglieri, alla Giunta ai Gruppi consiliari, alle strutture interessate del Consiglio (o Assemblea legislativa) e della Giunta regionale.

- Inserimento del testo degli atti nella relativa banca dati, che è consultabile anche tramite reti informatiche e telematiche; tale banca dati viene anche utilizzata dalla Giunta regionale/provinciale per assegnare l'atto all'Assessore competente a formulare la risposta e per adempiere agli impegni richiesti.

- Pubblicazione nei resoconti stenografici del testo:
  dell'atto di sindacato ispettivo e delle relative risposte (fornite in Aula oppure in Commissione);
  dell'atto di indirizzo politico proposto e di quello approvato dall'Assemblea.

- Deregistrazione (svolta da struttura interna o esterna) degli interventi orali svolti per la trattazione degli atti in oggetto.

- Trasmissione dei resoconti stenografici ai Consiglieri regionali ed eventuale diffusione tramite reti telematiche nelle forme previste dal Regolamento consiliare e nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5 D. Lgs. 196/2003. Si

rinvia anche a quanto specificato nell'apposita scheda n. 11 relativa alla "Documentazione dell'attività istituzionale del Consiglio regionale e degli organi consiliari .

- Trasmissione del materiale alla tipografia incaricata della stampa dei fascicoli e dei volumi.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali possono essere apportati solo previo parere del Garante per la protezione dei dati personali.

## 7. Attività della Conferenza di informazione

Nell'ambito della funzioni di controllo e di indirizzo politico rientra altresì l'istituto della Conferenza di informazione, la cui attività istruttoria potrebbe implicare il trattamento di dati sensibili e giudiziari in relazione alle seguenti fasi:
a) richiesta da acquisire al protocollo;
b) acquisizione di atti rilevanti e corrispondenza con i Consiglieri, Giunta, strutture amministrative interessate e soggetti interessati;
c) trasmissione della relazione conclusiva ai Consiglieri, alla Giunta e ai soggetti eventualmente interessati

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 9**

**DENOMINAZIONE DEL TRATTAMENTO:**

**VERIFICA ELETTORATO PASSIVO E REQUISITI PER L'ESERCIZIO DEL MANDATO**

**FONTI NORMATIVE:**

1. Statuto regionale;
2. Legge 17 febbraio 1968, n. 108 "Norme per la elezione dei Consigli regionali delle Regioni a statuto normale";
3. Legge 23 aprile 1981 n. 154 "Norme in materia di ineleggibilità ed incompatibilità alle cariche di Consigliere regionale, provinciale, comunale e circoscrizionale e in materia di incompatibilità degli addetti al Servizio sanitario Nazionale";
4. Legge 19 marzo 1990, n. 55 "Nuove disposizioni per la prevenzione della delinquenza di tipo mafioso e di altre gravi forme di manifestazione di pericolosità sociale";
5. Decreto legislativo 30 dicembre 1992, n. 502 "Riordino della disciplina in materia sanitaria, a norma dell'articolo 1 della legge 23 ottobre 1992, n. 421";
6. Legge 18 gennaio 1992, n. 16 " Norme in materia di elezioni presso le Regioni e gli enti locali";
7. Legge 23 febbraio 1995, n. 43 "Nuove norme per la elezione dei consigli delle regioni a statuto ordinario";
8. Legge 13 dicembre 1999, n. 475 "Modifiche all'articolo 15 della legge 19 marzo 1990, n. 55, e successive modificazioni";
9. Legge costituzionale 22 novembre 1999, n. 1 "Disposizioni concernenti l'elezione diretta del Presidente della Giunta regionale e l'autonomia statutaria delle Regioni";
10. Legge costituzionale 31 gennaio 2001, n. 2 "Disposizioni concernenti l'elezione diretta dei Presidenti delle Regioni a Statuto speciale e delle Province Autonome di Trento e Bolzano";
11. Legge 2 giugno 2004, n. 165 "Disposizione di attuazione dell'art. 122, primo comma della Costituzione".

**ALTRE FONTI ISTITUTIVE:**

Regolamento interno del Consiglio regionale

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'applicazione della disciplina in materia di elettorato passivo, nonché all'esercizio del mandato degli organi rappresentativi. In particolare per i seguenti compiti: accertamento delle cause di ineleggibilità, incompatibilità o decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi).

Art. 65 D. Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | |**X**| (Limitatamente alle Regioni nelle quali è giuridicamente rilevante l'origine etnica). | | | | |
| Convinzioni religiose | |**X**| | filosofiche | |**X**| | d'altro genere | |**X**| |
| Opinioni politiche | |**X**| | | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | | | | | | | | | | |**X**| |
| Stato di salute: | attuale | |**X**| | pregresso | |_| | anamnesi familiare | |_| |
| | | | | | | | | anche relativo a familiari dell'interessato | |_| |
| Vita sessuale | |_| | | | | | | | |
| Dati giudiziari | |**X**| | | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |_|

**Diffusione** |**X**|

Legge regionale - L'appartenenza a qualsiasi tipo di associazione viene pubblicata sul Bollettino Ufficiale della Regione, nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5 D.Lgs 196/2003.

**DESCRIZIONE DEL TRATTAMENTO:**

1. Le dichiarazioni sostitutive di certificazioni e di atto di notorietà, sottoscritte dai Consiglieri eletti, in materia di ineleggibilità ed incompatibilità previste dalla normativa vigente, vengono acquisite dall'Organo competente che ne verifica la regolarità.~~.~~

2. I dati vengono utilizzati ai fini della definizione della posizione giuridica dei singoli Consiglieri, della convalida o della eventuale contestazione delle cause di ineleggibilità o incompatibilità.

3. In caso di sospensione dalla carica per vicende giudiziarie, la struttura competente alla gestione economica, fiscale e previdenziale dei Consiglieri, ex Consiglieri ed Assessori, acquisiti i relativi atti giudiziari, sospende il trattamento economico.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D. Lgs. 82/2005), della documentazione inerente la verifica dell'elettorato passivo e dei requisiti per l'esercizio del mandato.

- Assegnazione alla struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Ai diretti interessati ed all'intero Consiglio regionale vengono comunicati i risultati istruttori svolti dall'Organo competente, individuato dalla normativa regionale.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali, possono essere apportati solo previo parere conforme del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 10**

**DENOMINAZIONE DEL TRATTAMENTO:**

**RICONOSCIMENTO INABILITÀ TOTALE E PERMANENTE AL LAVORO DEGLI ELETTI ALLA CARICA DI CONSIGLIERE REGIONALE**

**FONTI NORMATIVE:**

Legge regionale n. 24/01 (Disposizioni in materia di trattamento indennitario dei Consiglieri regionali)

**ALTRE FONTI ISTITUTIVE:**

//

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato al riconoscimento di benefici connessi all'inabilità).

Art.68 D. Lgs. 196/2003 "Benefici economici ed abilitazioni".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\| | | | | | | |
| Convinzioni religiose | \|_\| | filosofiche | \|_\| | d'altro genere | \|_\| | | |
| Opinioni politiche | \|_\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | \|_\| | | | | | | |
| Stato di salute: attuale | \|**X**\| | pregresso | \|**X**\| | anamnesi familiare | \|_\| | | |
| | | | | | anche relativo a familiari dell'interessato | \|**X**\| | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|_\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |_|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |_|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |**X**|
Collegio medico
base normativa: legge regionale in materia di assegno vitalizio.

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

Il Consigliere regionale chiede il riconoscimento dell'inabilità totale e permanente al lavoro, sia che si verifichi nel corso del mandato, sia che si verifichi dopo la cessazione del mandato.

Alla domanda è allegata la documentazione indicante il tipo di infermità o di lesione, che hanno causato l'inabilità e le eventuali conseguenze riguardanti l'integrità psicofisica.

L'accertamento di inabilità viene compiuto da un Collegio medico legale (diversamente composto) a cui viene trasmessa a documentazione sopra indicata allegata alla domanda.

Il Collegio medico legale trasmette al Responsabile del procedimento il verbale di accertamento con le conclusioni medico legali riguardanti la valutazione del caso.

Sulle citate conclusioni delibera l'Ufficio di Presidenza, che può disporre, prima di pronunciarsi, ulteriori accertamenti.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D. Lgs. 82/2005), della documentazione inerente il riconoscimento dell'inabilità totale e permanente al lavoro degli eletti alla carica di Consigliere regionale.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali, possono essere apportati solo previo parere conforme del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 11**

**DENOMINAZIONE DEL TRATTAMENTO:**

**DOCUMENTAZIONE DELL'ATTIVITÀ ISTITUZIONALE DEL CONSIGLIO (O ASSEMBLEA LEGISLATIVA) REGIONALE E DEGLI ORGANI CONSILIARI (O ASSEMBLEARI)**

**FONTI NORMATIVE:**

6. **Costituzione, art. 123 e ss.;**
7. **Statuto regionale.**

**ALTRE FONTI ISTITUTIVE:**

Regolamento interno del Consiglio regionale.
Legge regionale n. 7/05 (nuove disposizioni in materia di procedimento amministrativo di accesso ai documenti amministrativi).
Circolare Presidente Consiglio regionale "istruttoria preliminare dei progetti di legge e degli atti di indirizzo e di sindacato ispettivo"

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'applicazione della disciplina in materia di documentazione dell'attività istituzionale del Consiglio).

Art. 65 D. Lgs. 196/2003 "Diritti politici e pubblicità dell'attività di organi".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | **\|X\|** | | | | | | |
| Convinzioni religiose | **\|X\|** | filosofiche | **\|X\|** | d'altro genere | **\|X\|** | | |
| Opinioni politiche | **\|X\|** | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | **\|X\|** | | | | | | |
| Stato di salute: attuale | **\|X\|** | pregresso | **\|X\|** | anamnesi familiare | \|_\| | | |
| | | | | anche relativo a familiari dell'interessato | **\|X\|** | | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | **\|X\|** | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |**X**|

I Regolamenti consiliari individuano le categorie dei soggetti destinatari, quali Giunta, Gruppi consiliari, ecc.

**Diffusione** |**X**|

Base normativa: Regolamento interno del Consiglio, nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5 D.Lgs. 196/2003 e dall'art. 22, comma 8 del D.Lgs.196/2003.

**DESCRIZIONE DEL TRATTAMENTO:**

**8. Attività del Consiglio**

Di ogni seduta del Consiglio viene redatto il processo verbale e il resoconto stenografico, che possono contenere dati sensibili e giudiziari.
I processi verbali e i resoconti vengono pubblicati, raccolti in volumi e conservati presso la sede del Consiglio.
Trasmissione dei resoconti stenografici ai Consiglieri regionali ed eventuale diffusione tramite reti informatiche e telematiche, nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5 D. Lgs. 196/2003.

**9. Attività delle Commissioni permanenti, speciali, d'inchiesta o di indagine**

Delle sedute delle Commissioni permanenti, speciali, d'inchiesta o di indagine viene redatto un processo verbale e/o un resoconto sommario, che possono contenere dati sensibili e giudiziari.

Nello svolgimento dell'attività la Commissione di inchiesta o di indagine ha facoltà di chiedere informazioni e chiarimenti nonché l'esibizione di atti e documenti all'Amministrazione regionale, agli enti e aziende da essa dipendenti o sulle materie di competenza regionale o che comunque interessino la Regione.

I processi verbali e i resoconti delle sedute, le conclusioni, le informazioni, le notizie e i documenti, acquisiti da parte delle Commissioni, sono trasmesse - direttamente o tramite l'inserimento in una relazione conclusiva - all'Organo consiliare competente che ne cura la distribuzione a tutti i Consiglieri ed ai soggetti esterni interessati per materia.

Possono essere disposte registrazioni su supporti audio - visivi dei lavori del Consiglio, finalizzate alla trasmissione dell'attività dell'Assemblea legislativa o di altre attività riconducibili alle funzioni istituzionali del Consiglio; tali registrazioni possono essere irradiate tramite reti informatiche, telematiche e con emissioni televisive e nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5 D.Lgs. 196/2003 e dall'art. 22, comma 8, del medesimo decreto per quanto riguarda la diffusione dei dati idonei a rilevare lo stato di salute degli interessati.

**10. Atti consiliari in genere**

Più in generale, dati sensibili e giudiziari possono essere contenuti in tutti gli atti consiliari, anche in quelli che non sono soggetti al regime della resocontazione e verbalizzazione. Il trattamento degli eventuali dati sensibili e giudiziari contenuti in tali atti è regolato dal regime proprio degli atti stessi.
Per gli atti in questione vale il principio della pubblicità codificato dal Regolamento interno del Consiglio, pubblicità che si spinge non solo alla loro comunicazione ai soggetti titolati (in base alla tipologia del singolo atto), ma che prevede anche un'ampia diffusione, secondo sistemi tradizionali (diffusione cartacea, giornalistica, ecc.) e attraverso la collocazione in base dati informatiche accessibili in Internet e nel rispetto dello specifico quadro di garanzie previsto dall'art. 65, comma 5, D. Lgs. 196/2003 e dall'art. 22, comma 8, del medesimo decreto per quanto riguarda la diffusione dei dati idonei a rilevare lo stato di salute degli interessati.

Si rinvia anche a quanto specificato nell'apposita scheda n. 8 relativa alla "Attività politica, di indirizzo e di controllo - sindacato ispettivo".
.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D. Lgs. 82/2005), della documentazione inerente l'attività istituzionale degli Organi del Consiglio regionale.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Deregistrazione (svolta da struttura interna o esterna) degli interventi orali svolti per la trattazione degli atti in oggetto.

- Trasmissione del materiale alla tipografia incaricata della stampa dei fascicoli e dei volumi.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali, possono essere apportati solo previo parere conforme del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 12**

**DENOMINAZIONE DEL TRATTAMENTO:**

## INSINDACABILITÀ CONSIGLIERI REGIONALI

**FONTI NORMATIVE:**

1. Costituzione, art. 122, comma 4;
2. Statuto regionale;
3. Legge regionale n. 32/01 (Norme in materia di valutazione di insindacabilità dei Consiglieri regionali, ai sensi dell'articolo 122, comma 4, della Costituzione).

**ALTRE FONTI ISTITUTIVE:**

//

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per la redazione di verbali e resoconti dell'attività di Assemblee rappresentative).

Art. 65 "Diritti politici e pubblicità dell'attività di organi".
Art. 67 D. Lgs. 196/2003 "Attività di controllo e ispettive".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\|\| | | | | | | |
| Convinzioni religiose | \|**X**\| | filosofiche | \|**X**\| | d'altro genere | \|**X**\| | | |
| Opinioni politiche | \|**X**\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | \|**X**\| | | | | | | |
| Stato di salute: attuale | \|_\| | pregresso | \|_\| | anamnesi familiare | \|_\| | | |
| | | | | | anche relativo a familiari dell'interessato | \|_\| | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|**X**\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione** |**X**|
Comunicazione all'Autorità Giudiziaria
Base normativa: legge regionale

**Diffusione** |**X**|
Le deliberazioni del Consiglio regionale inerenti il trattamento in oggetto sono pubblicate sul Bollettino Ufficiale della Regione.
Base normativa: Statuto, nel rispetto dello specifico quadro di garanzie riconducibili a quanto previsto dall'art. 65, comma 5 D.Lgs. 196/2003.

**DESCRIZIONE DEL TRATTAMENTO:**

Qualora un Consigliere venga chiamato a rispondere davanti all'Autorità Giudiziaria per le opinioni espresse ed i voti dati nell'esercizio delle sue funzioni, ne dà comunicazione al Presidente del Consiglio il quale investe della questione il Consiglio. L'istruttoria sulla valutazione di insidacabilità delle opinioni espresse dal Consigliere viene svolta dall'Organo competente che trasmette le risultanze al Consiglio.
La decisione del Consiglio regionale in merito è trasmessa all'Autorità Giudiziaria.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente il procedimento.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione originale viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente); copia della documentazione viene consegnata ai componenti della Commissione che sono tenuti alla riservatezza ai sensi della deliberazione dell'Ufficio di Presidenza n. 11/2003.

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali, possono essere apportati solo previo parere conforme del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 13**

**DENOMINAZIONE DEL TRATTAMENTO:**

**PATROCINIO LEGALE - RIMBORSO SPESE LEGALI AMMINISTRATORI E DIPENDENTI REGIONALI PER FATTI E ATTI CONNESSI ALL'ESPLETAMENTO DEL SERVIZIO O DEL MANDATO**

**FONTI NORMATIVE:**

Legge regionale n. 51/97 *(Norme sull'organizzazione degli uffici e sull'ordinamento del personale regionale)*

**ALTRE FONTI ISTITUTIVE:**

per i dipendenti: CCLN e L.R. n. 21/89 *(Norme sul patrocinio legale a favore di dipendenti ed amministratori regionali per fatti connessi all'espletamento dei compiti d'ufficio)*

per gli Amministratori: L.R.n. 21/89 *(Norme sul patrocinio legale a favore di dipendenti ed amministratori regionali per fatti connessi all'espletamento dei compiti d'ufficio)*

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato alla tutela di diritti in occasione di procedimenti di responsabilità civile o penale nei confronti di dipendenti o amministratori per fatti o atti connessi all'espletamento del servizio o del mandato).

Art. 65 D. Lgs 196/2003 "Diritti politici e pubblicità dell'attività di organi".
Art. 71 D. Lgs 196/2003 "Attività sanzionatorie e di tutela".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | |
|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\| | | | | |
| Convinzioni religiose | \|_\| | filosofiche | \|_\| | d'altro genere | \|_\| |
| Opinioni politiche | \|_\| | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | \|_\| | | | | |
| Stato di salute: attuale | \|_\| | pregresso | \|_\| | anamnesi familiare | \|_\| |
| | | | | anche relativo a familiari dell'interessato | \|_\| |
| Vita sessuale | \|_\| | | | | |
| Dati giudiziari | \|**X**\| | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|

- di altro titolare |_|

.

**Comunicazione** |_|

Comunicazioni con l'Ufficio legale della Giunta.

Base normativa: legge regionale, Regolamento consiliare.

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

Sono previste due fattispecie procedurali:

1. il dipendente/amministratore informa che nei suoi confronti si è instaurato un procedimento giudiziario e chiede che gli venga messa a disposizione l'assistenza legale. In questa fattispecie deposita i provvedimenti dell'Autorità Giudiziaria;
2. il dipendente/amministratore non chiede l'assistenza legale, ma si difende con un proprio difensore di fiducia. Una volta assolto chiede che gli vengano rimborsate le spese legali. In questa fattispecie deposita la sentenza.

La richiesta viene inviata alla Giunta regionale che ne delibera il patrocinio. Qualora trattasi di amministratori o personale del Consiglio regionale, il provvedimento della Giunta regionale è adottato d'intesa con l'Ufficio di Presidenza del Consiglio regionale.

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D. Lgs. 82/2005), della documentazione inerente il procedimento.

- Assegnazione al servizio/struttura competente.

- Impostazione di fascicoli cartacei concernenti il trattamento.

- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali, possono essere apportati solo previo parere conforme del Garante per la protezione dei dati personali.

**REGOLAMENTO PER IL TRATTAMENTO DEI**
**DATI PERSONALI SENSIBILI E GIUDIZIARI**
(*Art.20 - 21 D.Lgs 196/2003 Codice in materia di protezione dei dati personali)*

**Scheda n° 14**

**DENOMINAZIONE DEL TRATTAMENTO:**

**ATTIVITÀ DEL COMITATO REGIONALE PER LE COMUNICAZIONI**

**FONTI NORMATIVE:**

**12.** Legge 31 luglio 1997, n. 249 "Istituzione dell'autorità per la garanzia nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo"
**13.** Legge regionale n. 1/2001 (Istituzione, organizzazione e funzionamento del Comitato regionale per le Comunicazioni)

**ALTRE FONTI ISTITUTIVE:**

//

**FINALITÀ DEL TRATTAMENTO:**

(Trattamento finalizzato all'espletamento delle funzioni di governo, garanzia, gestione, vigilanza e controllo in tema di comunicazione, delegate ai CO.RE.COM. da parte dell'Autorità garante, ai sensi dell'art. 1, comma 13 L. 249/1997.).

Art. 67 D.Lgs.196/2003 "Attività di controllo e ispettive".

**TIPOLOGIA DEI DATI TRATTATI:**

Dati idonei a rivelare:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Origine razziale ed etnica | \|_\| | | | | | | |
| Convinzioni religiose | \|_\| | filosofiche | \|_\| | d'altro genere | \|_\| | | |
| Opinioni politiche | \|_\| | | | | | | |
| Adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale | \|_\| | | | | | | |
| Stato di salute: attuale | \|_\| | pregresso | \|_\| | anamnesi familiare | \|_\| | | |
| | | | | | anche relativo a familiari dell'interessato | \|_\| | |
| Vita sessuale | \|_\| | | | | | | |
| Dati giudiziari | \|**X**\| | | | | | | |

**MODALITÀ DI TRATTAMENTO DEI DATI:**

informatizzato |**X**|
manuale |**X**|

**TIPOLOGIA DELLE OPERAZIONI ESEGUITE:**

***Operazioni standard***

**Raccolta:**

raccolta diretta presso l'interessato |**X**|
acquisizione da altri soggetti esterni |**X**|

**Registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione, distruzione.** |**X**|

***Operazioni particolari:***

**Interconnessione, raffronti di dati con altri trattamenti o archivi**

- dello stesso titolare |_|
- di altro titolare |_|

**Comunicazione**

|_|

**Diffusione** |_|

**DESCRIZIONE DEL TRATTAMENTO:**

Trattamento di dati giudiziari od extra giudiziari per azioni attivate dal Comitato regionale per le comunicazioni e per azioni per le quali è coinvolto o per conoscenze relative all'acquisizione di elementi legati alle funzioni istituzionali previste dalle deleghe dell'Autorità, ex-lege 249/97

**FLUSSO INFORMATIVO:**

- Ricezione di documenti esterni/produzione di atti interni, protocollazione, classificazione e fascicolazione, secondo il protocollo informatico (D.P.R. 445/2000 e Codice dell'amministrazione digitale D.Lgs. 82/2005), della documentazione inerente l'attività del Comitato regionale per le comunicazioni.
- Assegnazione al servizio/struttura competente.
- Impostazione di fascicoli cartacei concernenti il trattamento.
- Trattamento dei dati con modalità informatizzate.

- Per tutta la durata del procedimento la documentazione viene custodita in locali ad accesso controllato a cura del Responsabile del procedimento (archivio corrente).

- Terminato il procedimento e quando la documentazione non è più ritenuta utile alle normali attività d'ufficio viene versata - con atto formale - all'archivio che provvede all'ordinamento, all'inventariazione ed alla conservazione dei documenti.

- Gli archivi di deposito e storico, sono conservati secondo le disposizioni del Decreto legislativo 22 gennaio 2004, n. 42 "Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137" e del Decreto del Presidente della Repubblica 30 settembre 1963**,** n. 1409 "Norme relative all'ordinamento ed al personale degli archivi di Stato".

- Eventuali adattamenti che apportino modifiche sostanziali od integrazioni non formali, possono essere apportati solo previo parere conforme del Garante per la protezione dei dati personali.

# NOTIFICAZIONE ALL’AUTORITÀ GARANTE

## La Notificazione all'Autorità Garante: introduzione

### Che cosa è

La notificazione è una dichiarazione con la quale un soggetto pubblico o privato rende nota al Garante per la protezione dei dati personali l'esistenza di un'attività di raccolta e di utilizzazione dei dati personali, svolta quale autonomo titolare del trattamento.

### A chi è trasmessa

Al Garante, tramite questo sito e utilizzando la procedura indicata nelle istruzioni.

### In quale momento si presenta

Per le attività di trattamento dei dati che non esistevano prima del 1° gennaio 2004, la notificazione va effettuata prima che inizi il trattamento medesimo.

Per le attività che erano già in essere prima del 1° gennaio 2004, la notificazione si può effettuare entro il 30 aprile 2004.

### Quante volte si notifica

Una sola volta, indipendentemente dalla durata, dal tipo e dal numero delle operazioni di trattamento, sia che si effettui un solo trattamento, sia che si curino più attività di trattamento con finalità correlate tra loro.

### Che cosa riguarda

La notificazione riguarda l'attività di trattamento di dati personali (a volte solo se registrati in banche dati o archivi indicati dalla legge o dal Garante), ma non una banca dati o un archivio in quanto tale.

Può aversi, infatti, un trattamento anche se materialmente i dati non sono organizzati in una banca dati.

### Come si trasmette

Come già detto, solo per via telematica tramite questo sito, anche con la collaborazione di eventuali intermediari autorizzati.

**Va ripetuta?**

No. Una nuova notificazione è richiesta solo: a) prima che cessi definitivamente l'attività di trattamento; b) oppure prima che si apportino al trattamento alcune modifiche agli elementi da indicare nella notificazione.

**Cosa è cambiato dal 1° gennaio 2004**

A partire da tale data sono tenuti a notificare solo alcuni soggetti, ossia solo i titolari che effettuano una o più attività di trattamento tra quelle specificamente indicate dal Codice (la precedente normativa, invece, prevedeva per tutti i titolari l'obbligo di effettuare la notificazione, a meno che potessero avvalersi dei casi di esonero o di possibile utilizzazione di una notificazione semplificata).

Il Garante potrà individuare, con un proprio provvedimento, nell'ambito dei trattamenti che devono essere notificati, alcuni trattamenti che presentano minori rischi per i diritti degli interessati e che possono pertanto essere esonerati dalla notificazione; potrà, al contrario, anche indicare altri trattamenti al momento non indicati espressamente dalla legge, che dovranno essere notificati.

**È possibile una notificazione distinta se si trasferiscono dati all'estero?**

No. Se si trasferiscono dati all'estero, la circostanza va indicata nella stessa, unica notificazione che riguarda questi dati.

**Quale uso viene fatto della notificazione?**

Le notificazioni sono inserite in un registro pubblico che sarà consultabile gratuitamente da tutti *on-line*.

Il cittadino può così acquisire notizie e può utilizzarle per le finalità di applicazione della disciplina in materia di protezione dei dati personali (ad esempio, per esercitare il diritto di accesso ai dati o altri diritti riconosciuti dal Codice in materia di protezione dei dati personali).

Mediante il registro saranno effettuati controlli sui trattamenti oggetto di notificazione, verificando le notizie in essa contenute.

**A quale obbligo è soggetto chi non deve notificare?**

Il titolare che non è tenuto alla notificazione deve comunque fornire le notizie contenute nel modello di notificazione a chi ne fa richiesta (nell'esercizio del diritto di accesso e degli altri diritti riconosciuti all'interessato), a meno che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

**Nel registro dei trattamenti ci sono i nomi delle persone cui si riferiscono i dati?**

No. Tuttavia, le notizie accessibili mediante la consultazione del registro permettono di capire che tipo di dati sono trattati.

**Cosa accade se si omette la notificazione o la si presenta in ritardo o incompleta?**

Il titolare è punito con una sanzione pecuniaria (da diecimila euro a sessantamila euro) e con la pena accessoria della pubblicazione dell'ordinanza che applica la sanzione stessa in uno o più giornali, per intero o per estratto.

**Cosa accade se nella notificazione ci sono notizie non veritiere?**

La falsa dichiarazione è un reato, punito con la reclusione (da sei mesi a tre anni e salvo che il fatto configuri un reato più grave).

**Informativa sul trattamento dei dati personali inerenti alla notificazione**
(Art. 13 d.lg. 30 giugno 2003, n. 196, recante il "
*Codice in materia di trattamento dei dati personali"*)

Il Garante per la protezione dei dati personali (titolare del trattamento) informa che per effettuare all'Autorità la notificazione telematica dei trattamenti di dati devono essere fornite le informazioni di carattere personale richieste nei campi del presente modello contrassegnati con un asterisco.
Il mancato inserimento di tali informazioni non permette di completare la notificazione, con conseguente responsabilità per omessa notificazione (art. 163 del Codice).
L'indicazione dei dati personali nei campi non contrassegnati da un asterisco può risultare utile per agevolare i rapporti con il Garante e con gli interessati, ma è comunque facoltativa e, se omessa, non impedisce di completare la notificazione.
I dati personali indicati nella notificazione possono essere conosciuti (alcuni, anche dall'istituto bancario responsabile del trattamento tramite il quale sono versati i diritti di segreteria) da soggetti convenzionati con il Garante ai quali il notificante può rivolgersi per la trasmissione telematica della notificazione con apposizione di firma digitale. Si tratta di autonomi titolari di trattamento che possono trattare i dati nei limiti strettamente necessari per fornire il servizio e per questa sola finalità; per quanto qui non indicato, tali soggetti devono poi fornire una specifica informativa sul trattamento dei dati personali da essi effettuato.
I dati personali acquisiti tramite la procedura di notificazione telematica, descritta nelle istruzioni, sono trattati con modalità prevalentemente informatiche e telematiche ed inseriti in un registro elettronico dei trattamenti tenuto dal Garante, consultabile da chiunque anche per via telematica, oppure presso l'Autorità o soggetti pubblici convenzionati.
Le notizie accessibili tramite la consultazione del registro possono essere trattate, anche dai terzi che vi accedono, solo per finalità di applicazione della disciplina in materia di trattamento dei dati personali. In particolare, l'Autorità le utilizza per verifiche e controlli ed altre attività necessarie per svolgere i propri compiti istituzionali.
I codici identificativi assegnati all'utente, in via provvisoria o permanente, sono necessari per permettere, rispettivamente, la sospensione temporanea delle operazioni di notificazione, oppure la modifica di una notificazione già effettuata. Tali codici sono comunicati solo all'utente e possono essere conosciuti nei casi in cui ciò sia necessario per ragioni di servizio solo dal personale interno all'Autorità preposto alla gestione del registro dei trattamenti, o da incaricati esterni che collaborano alla manutenzione del registro (allo stato, svolge al riguardo funzioni di responsabile del trattamento la società AREA.IT s.r.l., Via Divisione Garibaldi n. 14, 52037 San Sepolcro (AR).
L'interessato può accedere direttamente in ogni momento ai dati che lo riguardano senza necessità di rivolgere un'istanza, consultando la notificazione tramite questo sito web (https://web.garanteprivacy.it/rgt/).
Fuori dei casi in cui il notificante deve modificare ai sensi di legge la notificazione perché sono mutati alcuni elementi, le richieste di esercizio dei diritti previsti dal Codice a favore dell'interessato (art. 7) possono essere rivolte al Garante per la protezione dei dati personali – Dipartimento registro dei trattamenti, Piazza di Monte Citorio n. 121, 00186 Roma, fax n. 06.69677785, e-mail: rgt-info@garanteprivacy.it.

# ISTRUZIONI PER LA NOTIFICAZIONE*

## 1. CHI DEVE NOTIFICARE

*A) Titolare del trattamento*

Solo i titolari dei trattamenti indicati dalla legge (art. 37 del Codice) o dal Garante con appositi provvedimenti (allo stato non adottati), sono obbligati a notificare i trattamenti al Garante secondo la nuova procedura di seguito descritta.

La notificazione precede l'inizio del trattamento (art. 38, comma 1, del Codice) e può riguardare uno o più trattamenti con finalità correlate.

Il titolare che abbia già iniziato un trattamento anteriormente al 1° gennaio 2004, indipendentemente dalla circostanza che lo abbia notificato in passato, deve procedere, se vi è tenuto, alla nuova notificazione entro il 30 aprile 2004 (art. 181, comma 1, lett. c), del Codice).

Chi esegue la notificazione secondo la nuova procedura deve dichiarare che effettua una "nuova notificazione", anche se in passato abbia già presentato una notificazione in base alla legge n. 675/1996.

Ulteriori eventuali notificazioni costituiscono "modifiche del trattamento", oppure "cessazione del trattamento" (nel caso in cui l'intero trattamento precedentemente notificato venga a cessare definitivamente).

*B) Contitolare del trattamento*

In caso di contitolarità del trattamento, ciascun contitolare è tenuto ad effettuare un'autonoma notificazione, nella quale indicherà tutti gli altri contitolari.

Ciascun titolare sottoscriverà solo la propria notificazione.

## 2. COME SI NOTIFICA

*A) Nuova notificazione*

La "nuova notificazione" va eseguita unicamente in via telematica, compilando i campi del modello disponibile sul sito Internet:

https://web.garanteprivacy.it/rgt/Modello_Notificazione_2004.pdf

**Allo stato non sono previste e ammesse altre modalità.** A differenza della notificazione prevista dalla legge n. 675/1996, non è quindi possibile utilizzare modelli cartacei o dischetti, né per la compilazione, né per l'invio.

*B) Modifica della notificazione*

Per quanto riguarda la modifica della notificazione, l'attività del notificante è semplificata.

Si può richiamare a video la notificazione già trasmessa, apportando le modifiche necessarie per i soli riquadri interessati. La notificazione, così modificata, è trasmessa osservando la procedura telematica prevista per la "nuova notificazione".

## 3. MODALITÀ DI COMPILAZIONE DELLA NOTIFICAZIONE

Nella compilazione della notificazione i campi contrassegnati con un asterisco sono obbligatori: la loro mancata compilazione impedisce il completamento della procedura di notificazione.

Il notificante deve osservare le seguenti indicazioni:

- selezionare dal menù principale "COMPILAZIONE DELLA NOTIFICAZIONE";
- selezionare la casella "NUOVA NOTIFICAZIONE";
- barrare una delle tre opzioni indicate ("prima notificazione"; "modifica alla precedente notificazione"; "cessazione del trattamento");
- compilare i campi di interesse, utilizzando anche i menù a tendina;
- al termine delle descritte operazioni, salvare il *file* mediante l'apposito tasto;
- versare i diritti di segreteria *on line*, oppure compilare l'apposito riquadro indicando gli estremi del pagamento avvenuto;
- sottoscrivere con firma digitale il *file* salvato;
- trasmettere al Garante per via telematica la notificazione così completata mediante l'apposito tasto.

Il Garante invierà all'indirizzo di posta elettronica indicato dal notificante un messaggio di conferma del ricevimento della notificazione che attesta il buon esito della procedura.

È possibile stampare copia della notificazione; tale copia cartacea, comunque, non deve essere trasmessa al Garante.

## 4. EVENTUALE SOSPENSIONE NELLA COMPILAZIONE DELLA NOTIFICAZIONE DEL TRATTAMENTO, DELLA SUA MODIFICA E DELLA SUA CESSAZIONE

La procedura di notificazione può essere eseguita in momenti diversi, anche da altra postazione (per esempio, la firma digitale potrebbe essere apposta in altra sede, presso gli organismi convenzionati), memorizzando comunque le informazioni già inserite. Affinché ciò sia possibile è necessario compilare almeno il riquadro relativo al titolare del trattamento; quindi, selezionare il tasto SOSPENDI.

Comparirà a video un codice (ID temporaneo) che, contestualmente, verrà inviato dal Garante all'indirizzo di posta elettronica indicato dal notificante nella notificazione.

Tale codice consentirà al notificante di riprendere, entro i 10 giorni successivi, la compilazione della notificazione.

Il codice è utilizzabile soltanto una volta; in caso di ulteriori sospensioni verranno attribuiti tanti ID temporanei, utilizzabili secondo la procedura descritta, quante sono le sospensioni effettuate.

## 5. RIPRESA DELLA COMPILAZIONE DELLA NOTIFICAZIONE A SEGUITO DI SOSPENSIONE

- selezionare "COMPILAZIONE DELLA NOTIFICAZIONE";
- selezionare "NOTIFICAZIONE SOSPESA";
- inserire, alla richiesta, l'ID temporaneo comunicato dal Garante al momento della sospensione.

## 6. DIRITTI DI SEGRETERIA

Ogni notificazione inviata al Garante (prima notificazione, modifica o cessazione del trattamento) deve essere accompagnata dal pagamento dei diritti di segreteria, il cui importo è fissato in euro 150,00.
Per indicare la modalità di pagamento prescelta va compilato l'apposito riquadro. Si suggerisce di privilegiare il pagamento on line mediante carta di credito su protocollo sicuro, pur essendo consentite altre modalità (bonifico bancario, conto corrente postale, banco posta); per questi casi occorre indicare gli estremi del pagamento nell'apposito riquadro.
Le coordinate bancarie per effettuare il pagamento sono: c.c. 000000018373 intestato a "Garante per la protezione dei dati personali" - cod. ABI 05164, cod. CAB 03202, cod. CIN C - presso Banca popolare italiana, ag. n. 2 di Roma, via Bevagna, 24, 00191 Roma; oppure su bancoposta, n. conto 51620359, cod. ABI 7601, cod. CAB 03200, cod. CIN O - intestato sempre a "Garante per la protezione dei dati personali"

Il pagamento può anche essere effettuato sul c.c. postale n. 51620359 intestato a "Garante per la protezione dei dati personali", Piazza di Monte Citorio, 115/121, 00186, Roma, indicando come causale "diritti di segreteria per notificazione".

## 7. FIRMA DIGITALE

Per perfezionare la notificazione è necessario sottoscriverla con firma digitale (art. 10, comma 3, d.P.R. n. 445/2000). A tal fine, il titolare del trattamento deve utilizzare un dispositivo di firma digitale disponibile presso uno dei certificatori accreditati ai sensi dell'art. 2, comma 1, lett. c), d. lgs. n. 10/2002. L'elenco dei certificatori è rinvenibile sul sito www.cnipa.gov.it.

La notificazione così sottoscritta va trasmessa per via telematica al Garante.

*Firma digitale presso soggetti qualificati*
Il Garante stipulerà apposite convenzioni con soggetti qualificati (di seguito denominati "intermediari"). Ciò per permettere la sottoscrizione della notificazione con firma digitale laddove il notificante non fosse in possesso del dispositivo di firma digitale. In questo caso il notificante deve recarsi presso uno dei soggetti convenzionati munito del proprio ID temporaneo e di un documento di riconoscimento (ed eventualmente della ricevuta di versamento dei diritti di segreteria, ove non avesse già provveduto ad inserire gli estremi nell'apposito campo) e, avvalendosi della firma digitale dell'intermediario, trasmettere in via telematica la notificazione. L'intermediario potrà annotare nella notificazione, ove non già eseguito dal notificante, gli estremi della ricevuta del pagamento dei diritti di segreteria.

L'elenco degli organismi convenzionati è visibile alla casella "convenzioni" del menù principale.

## 8. COMPLETAMENTO DELLA NOTIFICAZIONE E TRASMISSIONE AL GARANTE

ID permanente (Codice univoco del notificante-C.U.N.)

Eseguite le operazioni (inserimento dei dati, pagamento dei diritti di segreteria, apposizione della firma digitale e trasmissione in via telematica) e trasmessa la notificazione in via telematica, verrà inviato dal Garante con l'indicazione di giorno, ora e minuto, un ID permanente (C.U.N.) da conservare a cura del notificante. Il C.U.N. verrà comunicato al solo notificante per posta elettronica.
Solo con l'inserimento del C.U.N. il notificante potrà accedere, in tempi successivi, alla notificazione per modificarla o per provvedere alla notificazione della cessazione del trattamento; il C.U.N., inoltre, permette di "legare" le notificazioni effettuate nel tempo da uno stesso titolare.
L'intermediario rilascia ricevuta, controfirmata anche dal notificante, di avvenuto invio della notificazione. Consegna altresì, a richiesta del notificante, una copia a stampa della notificazione.

Concluse le operazioni, l'intermediario deve cancellare dal proprio sistema operativo il *file* contenente la notificazione inviata.

## 9. MODIFICHE DELLA NOTIFICAZIONE E CESSAZIONE DEL TRATTAMENTO

Per poter effettuare successive modifiche della notificazione oppure notificare la cessazione del trattamento è necessario indicare il C.U.N. attribuito in sede di "prima notificazione".

Qualora si dovesse sospendere la notificazione, si dovrà usare, per il suo completamento, l'ID temporaneo che di volta in volta verrà comunicato dal Garante (secondo la procedura sopra descritta).

## 10. ANOMALIE E REGOLARIZZAZIONI

Pervenuta la notificazione al Garante, viene effettuato un controllo sulla veridicità della firma digitale apposta e vengono segnalate al notificante eventuali anomalie; in tal caso il Garante invia un messaggio di richiesta di regolarizzazione/completamento assegnando un termine, decorso inutilmente il quale la notificazione viene eliminata dalla memoria del sistema informativo del Garante; di ciò è dato avviso al notificante.

La sottoscrizione digitale che, verificata, non risulti conforme, invalida la notificazione.

In caso di regolarizzazione, la data della notificazione è quella in cui la regolarizzazione stessa è memorizzata nel sistema informativo del Garante.

## 11. ASSISTENZA NELLA COMPILAZIONE

Per ciascuna tabella, riquadro o campo da compilare, sono inseriti alcuni *box* contenenti spiegazioni per la compilazione (contrassegnati con il simbolo "?"), quale ausilio in caso di dubbi.

Inoltre ci si può collegare al sito del Garante www.garanteprivacy.it per consultare la normativa di riferimento e le *faq*.

Infine, per brevi spiegazioni, può essere contattato l'Ufficio relazioni con il pubblico del Garante.

## 12. SINTESI DEL QUADRO NORMATIVO DI RIFERIMENTO

La disciplina in materia di notificazione del trattamento dei dati personali è contenuta negli artt. 37, 38, 154, comma 1, lett. l), 163, 168, 181, comma 1, lett. c), 16, 162, comma 1, del d.lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

Il Codice in materia di protezione dei dati personali è entrato in vigore il 1° gennaio 2004 ed ha abrogato la precedente disciplina della notificazione contenuta nella legge n. 675/1996.

## 13. TABELLE DELLA PROCEDURA DI NOTIFICAZIONE

È possibile consultare le tabelle relative a categorie di dati, categorie di interessati, finalità, modalità, che dovranno essere compilate nella notificazione. È inoltre possibile prelevare il facsimile del modello di notificazione.

---

(*) Le norme richiamate nel testo, ove non diversamente specificato, si riferiscono al decreto legislativo n. 196/2003 (Codice in materia di protezione dei dati personali).

# MODELLI

(Fac Simile)

**Informativa ex art. 13 d. lgs. 196/2003 per il trattamento di dati sensibili**
*(Da inserire in fondo al modello di raccolta dati)*

Gentile Signore/a,
ai sensi del d.lgs. 196/2003, sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali, il trattamento delle informazioni che La riguardano, sarà improntato ai principi di correttezza, liceità e trasparenza e tutelando la Sua riservatezza e i Suoi diritti.

In particolare, i dati idonei a rivelare l'origine razziale ed 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, possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante per la protezione dei dati personali (articolo 26).

Ai sensi dell'articolo 13 del predetto decreto, Le forniamo quindi le seguenti informazioni.

1. I dati sensibili da Lei forniti verranno trattati, nei limiti dell'Autorizzazione generale del Garante n.../200…, per le seguenti finalità: .....;

2. Il trattamento sarà effettuato con le seguenti modalità: .....….....;
*(Indicare le modalità del trattamento: manuale / informatizzato / altro.)*

3. Il conferimento dei dati è facoltativo/obbligatorio (*se obbligatorio specificare il motivo dell'obbligo*) e l'eventuale rifiuto a fornire tali dati non ha alcuna conseguenza / potrebbe comportare la mancata o parziale esecuzione del contratto / la mancata prosecuzione del rapporto.

4. I dati non saranno comunicati ad altri soggetti né saranno oggetto di diffusione

o

i dati potranno essere / saranno comunicati a: ..... o diffusi presso.....;
*(Scegliere l'opzione a seconda delle caratteristiche del trattamento e indicare, se presente, l'ambito di comunicazione e/o diffusione, fermo restando il divieto relativo ai dati idonei a rivelare lo stato di salute, di cui all'art. 26, comma 5 del d.lgs. 196/2003).*

5. Il titolare del trattamento è: .....;
*(Indicare la denominazione o la ragione sociale e il domicilio, la residenza o la sede del titolare)*

6. Il responsabile del trattamento è .....…….....;
*(indicare almeno un responsabile, e, se vi è un responsabile designato ai fini di cui all'articolo 7 del d.lgs. 196/2003, indicare quel soggetto; indicare, inoltre, il sito della rete di comunicazione o le modalità attraverso le quali è altrimenti conoscibile in modo agevole l'elenco aggiornato dei responsabili*)

7. il rappresentante del titolare nel territorio dello Stato è .....…….....;

(*se il titolare è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, mezzi situati nel territorio dello Stato anche diversi da quelli*

*elettronici o comunque automatizzati, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea*)

8. In ogni momento potrà esercitare i Suoi diritti nei confronti del titolare del trattamento, ai sensi dell'articolo 7 del d.lgs.196/2003, che per Sua comodità riproduciamo integralmente:

Decreto Legislativo n.196/2003, Art. 7 - Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

(Fac Simile)

**Formula di acquisizione del consenso per il trattamento di dati sensibili**

Luogo ..... Data .....

Cognome ..... Nome .....

Il/La sottoscritto/a, acquisite le informazioni fornite dal titolare del trattamento ai sensi dell'art. 13 del D.lgs. n. 196/2003, e consapevole, in particolare, che il trattamento riguarderà i dati "sensibili" di cui all'art.4 comma 1 lett. d), nonché art.26 del D.lgs.196/2003, vale a dire i dati *"idonei a rivelare l'origine razziale ed 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"*:

- presta il suo consenso per il trattamento dei dati necessari allo svolgimento delle operazioni indicate nell'informativa.

Firma leggibile .....

- presta il suo consenso per la comunicazione dei dati ai soggetti indicati nell'informativa.

*(nel caso in cui sia prevista anche la comunicazione dei dati sensibili dell'interessato)*

Firma leggibile .....

- presta il suo consenso per la diffusione dei dati nell'ambito indicato nell'informativa.

*(nel caso in cui sia prevista anche la diffusione dei dati sensibili* ***diversi da quelli idonei a rivelare lo stato di salute*** *dell'interessato; questi ultimi, infatti, non possono essere diffusi).*

Firma leggibile .....

(Fac Simile)

**Opposizione al trattamento dei dati per motivi legittimi**

Luogo, .....Data .....

Spett.le: _____

*(Indicare la denominazione del Titolare del trattamento)*

**Oggetto: D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali). Esercizio dei diritti dell'interessato, di cui all'art. 7 del D.lgs. 196/2003.**

Io sottoscritto ....., nato a ....., il ....., residente in ....., ai sensi dell'art. 7, comma 4, del Decreto Legislativo 30 giugno 2003 n. 196, mi oppongo al trattamento dei miei dati personali da Voi effettuato, per i seguenti motivi: .....

(indicare i "motivi legittimi" in base ai quali ci si oppone al trattamento, tenendo conto che la legge non individua una fattispecie precisa, ma prevede solo la "legittimità" del motivo di opposizione)

Distinti saluti.

Firma leggibile.....

---

NOTE:

1. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse.
2. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.
3. L’interessato deve dimostrare la propria identità, anche esibendo o allegando all’istanza una fotocopia del documento di riconoscimento (art. 9, comma 4, D.lgs. 196/2003).

(Fac Simile)

**Esercizio dei diritti dell'interessato di essere informato sull'esistenza di suoi dati personali presso archivi e sul trattamento che ne viene fatto**

Luogo, .....Data .....

Spett.le: _____
*(indicare la denominazione del Titolare del trattamento)*

**Oggetto:** **Decreto Legislativo 196/2003 (Codice in materia di trattamento dei dati personali). Esercizio del diritto di accesso ai dati personali ed altri diritti, di cui all'art. 7.**

Io sottoscritto ....., nato a ....., il ....., residente in....., ai sensi dell'art. 7, commi 2 e 3, del Decreto Legislativo 30 giugno 2003, n. 196, chiedo di essere informato circa:

1. la conferma dell'esistenza o meno nel vostro archivio o sistema informativo di dati personali che mi riguardano, anche se non ancora registrati;
2. la comunicazione in forma intelligibile dei medesimi dati e della loro origine;
3. le modalità del trattamento da voi effettuato sui dati personali;
4. la comunicazione dell'origine dei dati;
5. la comunicazione delle finalità del trattamento;
6. la comunicazione della logica applicata al trattamento effettuato con strumenti elettronici;
7. la comunicazione degli gli estremi identificativi del titolare del trattamento (ovvero della pubblica amministrazione, della persona giuridica pubblica o privata, dell'associazione od organismo che li tratta);
8. la comunicazione degli gli estremi identificativi del responsabile del trattamento, se designato;
9. la comunicazione dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza.

Ringraziando anticipatamente, porgo distinti saluti.

Firma leggibile .....

NOTE:
1. La richiesta può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.
2. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse.
3. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.
4. L'interessato deve dimostrare la propria identità, anche esibendo o allegando all'istanza una fotocopia del documento di riconoscimento (9, comma 4 D.Lgs. 196/2003).
5. Per ogni richiesta di cui all'art. 7, comma 3, del D.Lgs. 196/2003 (conferma dell'esistenza o meno di dati personali che riguardano l'interessato, anche se non ancora registrati; la

comunicazione in forma intelligibile dei medesimi dati e della loro origine; la comunicazione della logica e delle finalità su cui si basa il trattamento) può essere chiesto all'interessato - ove non risulti confermata l'esistenza di dati che lo riguardano - un contributo spese, non eccedente i costi effettivamente sostenuti per la ricerca effettuata nel caso specifico. Il contributo non può comunque superare l’importo stabilito dal Garante con provvedimento a carattere generale.
6. Restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

(Fac Simile)

**Esercizio dei diritti dell'interessato di ottenere la cancellazione o il blocco di dati dei quali già conosce l'esistenza presso gli archivi cui si rivolge e per i quali si è constatato il trattamento in violazione di legge**

Luogo, .....Data .....

Spett.le: _____
*(Indicare la denominazione del Titolare del trattamento)*

**Oggetto:** **Decreto Legislativo 196/2003 (Codice in materia di trattamento dei dati personali). Esercizio del diritto di accesso ai dati personali ed altri diritti, di cui all'art.7.**

Io sottoscritto .....……., nato a .....……., il .....……..,
residente in.....……., ho constatato che il trattamento dei miei dati personali da Voi detenuti per ..... *(indicare le finalità così come risultanti dall'informativa resa dal titolare)* è avvenuto in violazione di legge *(indicare sommariamente la violazione, ad esempio, quella dell'art. 23 del D.lgs. 196/2003).*

Ai sensi dell'articolo 7, comma 3, del D. Lgs. 196/2003, chiedo pertanto la cancellazione / la trasformazione in forma anonima / il blocco, dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati.
Richiedo altresì l'attestazione, da parte vostra, che le operazioni sopra descritte sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati in precedenza comunicati.
Distinti saluti

Firma leggibile .....

---
NOTE:
1. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse

2. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.

3. L’interessato deve dimostrare la propria identità, anche esibendo o allegando all’istanza una fotocopia del documento di riconoscimento (art. 9 comma 4 D.Lgs. 196/2003).

(Fac Simile)

**Esercizio dei diritti dell'interessato di ottenere la rettifica o l'aggiornamento di dati dei quali già conosce l'esistenza presso gli archivi cui si rivolge**

Luogo, .....Data .....

Spett.le: _____
*(Indicare la denominazione del Titolare del trattamento)*

Oggetto: Decreto Legislativo 196/2003 (Codice in materia di trattamento dei dati personali).
Esercizio del diritto di accesso ai dati personali ed altri diritti, di cui all'art. 7.

Io sottoscritto .....……., nato a .....……., il .....……..,
residente in.....……., ai sensi della normativa in oggetto, richiedo l'aggiornamento dei miei dati personali *(indicare gli aggiornamenti)* / la rettificazione dei miei dati personali *(indicare le rettifiche)* / l'integrazione dei dati *(indicare le integrazioni da fare e l'interesse a richiederle)* / la cancellazione dei dati trattati in violazione della legge, compresi quelli di cui non è necessaria la conservazione *(indicare le cancellazioni da fare)* / la trasformazione in forma anonima dei dati trattati in violazione della legge, compresi quelli di cui non è necessaria la conservazione *(indicare i dati trattare in forma anonima)* / il blocco dei dati trattati in violazione della legge, compresi quelli di cui non è necessaria la conservazione *(indicare i dati da bloccare)*.

Richiedo altresì l'attestazione che le operazioni sopra descritte sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati in precedenza comunicati.
Distinti saluti.

Firma leggibile.....

---
NOTE:
1. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse

2. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.

3. L’interessato deve dimostrare la propria identità, anche esibendo o allegando all’istanza una fotocopia del documento di riconoscimento (art. 9, comma 4, D.lgs. 196/2003).

(Fac Simile)

**Accesso al registro dei trattamenti tenuto dal Garante per la protezione dei dati personali**

Luogo, .....Data .....

AL GARANTE DELLA PROTEZIONE DEI DATI PERSONALI

Oggetto: Decreto Legislativo 196/2003 (Codice in materia di trattamento dei dati personali). Esercizio del diritto di accesso ai dati personali ed altri diritti, di cui all'art. 7.

Io sottoscritto .....……., nato a .....……., il .....……..,
residente in.....……., rivolgo cortese istanza al fine di conoscere, mediante accesso gratuito al registro di cui all'art. 154, comma 1, lettera L del D. Lgs. 196/2003, l'esistenza di trattamenti di dati che possono riguardarmi.

A tali fini, specifico che
.....
*(indicare le peculiarità del proprio lavoro, famiglia, stato civile, attività effettuate, appartenenza a circoli, corrispondenza intrattenuta con aziende, mezzi di trasporto utilizzati, acquisti, etc., dalle quali si possa individuare l'ambito di trattamenti che possono essere rilevanti).*

Distinti saluti.

Firma leggibile.....

---
NOTE:
1. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse
2. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.

(Fac Simile)

**Opposizione al trattamento dei dati per fini pubblicitari**

Luogo, .....Data .....

Spett.le: _____

*(Indicare la denominazione del Titolare del trattamento)*

**Oggetto: D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali). Esercizio dei diritti dell'interessato, di cui all'art. 7 del D.lgs. 196/2003.**

Io sottoscritto ....., nato a ....., il ....., residente in ....., ai sensi dell'art. 7, comma 4, del Decreto Legislativo 30 giugno 2003 n. 196, mi oppongo al trattamento dei miei dati personali da Voi effettuato a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Distinti saluti.

Firma leggibile.....

---

NOTE:

1. I diritti riferiti ai dati personali di persone decedute possono essere esercitati da chiunque abbia interesse.
2. Nell'esercizio dei diritti, l'interessato può dare delega o procura scritta a persone fisiche o associazioni. In tal caso, la circostanza deve essere esplicitata ed è preferibile allegare fotocopia dell'atto stesso.
3. L’interessato deve dimostrare la propria identità, anche esibendo o allegando all’istanza una fotocopia del documento di riconoscimento (art. 9, comma 4, D.lgs. 196/2003).

# Bibliografia

Aa. Vv., *La tutela della privacy*, 1 edizione, collana «L'Unione Europea», Consiglio regionale del Piemonte, Torino, 1997

Aa. Vv., *La tutela della privacy*, 2 edizione, collana «L'Unione Europea», Consiglio regionale del Piemonte, Torino, 1998

Aa. Vv., *Legge 31 dicembre 1996, n. 675 e successive modificazioni "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali". Commento*, collana «L'Unione Europea», Consiglio regionale del Piemonte, Torino, 1998

Aa. Vv., *Dati sensibili e soggetti pubblici. Commento sistematico al D. Lgs. n. 135/1999*, Giuffre, Milano, 2000

Aa. Vv., *Privacy: nuova normativa a seguito del decreto legislativo 28 dicembre 2001, n. 467*, Consiglio regionale del Piemonte, Torino, 2002

Aa. Vv., *Guida per la tutela della riservatezza del minore*, Consiglio regionale del Piemonte, Torino, 2003

Aa. Vv., *Codice della privacy, commento al decreto legislativo 30 giugno 2003, n. 196*, Giuffre, Milano, 2004

R. Acciai, *Privacy e banche dati pubbliche. Il trattamento dei dati personali nelle pubbliche amministrazioni*, Cedam, Padova, 2001

R. Acciai, (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini, 2004

M. Aimo, *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, Napoli 2003

G. Arcudi, V. Poli, *Il diritto alla riservatezza*, Ipsoa, Milano, 2000

A. Attanasio, *La responsabilità civile per danni conseguenti alla raccolta dei dati ed alla loro conservazione*, in www.e-privacy.winstonsmith.info, maggio 2005

E. Barilà, C. Caputo, *La tutela della privacy nella pubblica amministrazione. Riservatezza e gestione dell'informazione nel settore pubblico*, Giuffrè, Milano 2000

V. Bossi, M. Rovero, *Privacy. Nuova normativa a seguito del decreto legislativo 30 giugno 2003, n. 196: Codice in materia di protezione dei dati personali*, Consiglio regionale del Piemonte, Torino, 2004

G. Buttarelli, *Profili generali del trattamento dei dati personali*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 61-92

A. Cacciari, *La tutela della riservatezza dei dati personali nelle pubbliche amministrazioni e negli enti locali*, Sistemi editoriali, Napoli 2003

D. Caldirola, *Il diritto alla riservatezza*, Cedam, Padova 2006

F. Cardarelli, S. Sica, V. Zeno-Zencovich, *Il codice dei dati personali. Temi e problemi*, Giuffrè, Milano 2004

G. Cassano, S. Fadda, *Codice in materia di protezione dei dati personali. Commento articolo per articolo al testo unico sulla privacy*, Ipsoa, Milano 2004

G.P. Cirillo, *La tutela civilistica nel trattamento pubblico dei dati personali*, in A. Loiodice e G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXVI, *La tutela della riservatezza*, Cedam, Padova 2000, pagg. 95-127

G.P. Cirillo, *La tutela della privacy nel sistema del nuovo codice sulla protezione dei dati personali*, Giuffrè, Milano, 2004.

G.P. Cirillo, *La tutela in via amministrativa del trattamento dei dati personali*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 697-792

G.P. Cirillo, *La tutela penale e le sanzioni amministrative*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 793-842

F. Di Ciommo, *La responsabilità del danno non patrimoniale da illecito trattamento dei dati personali*, in «Danno e responsabilità», n. 7, 2005 (www.ipsoa.it)

G. Elli, R. Zallone, *Il nuovo codice della privacy, (commento al d. lgs. 30 giugno 2003, n. 196 con la giurisprudenza del Garante*), Giappichelli, Torino 2004

L. Failla, *Privacy e rapporto di lavoro*, Ipsoa, Milano 2002

G. Fioriglio, *La tutela risarcitoria nel Codice della privacy*, in www.dirittodell'informatica.it

S. Foà, *Il trattamento dei dati personali per finalità di rilevante interesse pubblico*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 343-427

P. Garri, *I soggetti che effettuano il trattamento: il titolare, il responsabile e l'incaricato*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 131-166

M. Gobbato, M. Barella, P. Mancone, *Danno da informazione. Uso illecito o diffusione da informazionifalse o parziali*, in «Altalex», n. 1796, 14 giugno 2007

R. Imperiali, R. Imperiali, *La tutela dei dati personali, Commento alla normativa sulla protezione dei dati personali*, Il sole 24, Milano 2004

A. Lisi, *Pubblica amministrazione e privacy. Istruzioni per l'uso*, Cierre, Roma 2006

A. Lucarino, *Responsabilità e risarcimento dei danni in seguito al trattamento dei dati personali*, in www.privacy.it, maggio 2000

M. Magliazza, *Profili internazionali ed europei del diritto all'informazione e alla riservatezza*, Giuffrè, Milano 2004

A. Maresca, S. Lucrezio Monticelli, *Tutela della riservatezza nei rapporti di lavoro: divieto di controllo a distanza e telelavoro*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 537-558

Marta Monaciliuni, *I nuovi rapporti tra l'art. 15 T.U. della privacy e l'art. 2050 c.c. in tema di attività pericolosa*, in www.formez.it

J. Monducci, G. Sartor (a di cura), *Codice in materia di protezione dei dati personali*, Cedam, Padova 2004

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

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

T. Perfetti, *Profili di responsabilità civile nel nuovo "Codice della Privacy" (d.lgs.196/2003)*, in www. computerlaw.it

S. Romeo, *Recensione a G.P. Cirillo, 'Trattamento pubblico dei dati personali e responsabilità civile della P.A., in Foro amm. 11-12/99*, in www.lexfor.it

A. Scalisi, *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

P. Stanzione, S. Sica, *La nuova disciplina della privacy*, Zanichelli, Bologna, 2004

F. Tavarelli, *Sicurezza ICT e trattamento dei dati*, in www.isticom.it

E. Tosi, *Il codice della privacy. Tutela e sicurezza dei dati personali, normativa nazionale e comunitaria*, La Tribuna, Piacenza 2004

P. Troiano, *Le misure di sicurezza*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 167-222

T. M. Umbertazzi, *Il diritto alla privacy. Natura e funzione giuridica*, Cedam, Padova 2004

C. Zucchelli, *Regole generali per il trattamento dei dati nelle amministrazioni pubbliche*, in G. Santaniello (a cura di), *Trattato di diritto amministrativo*, volume XXXVI, *La protezione dei dati personali*, Cedam, Padova 2005, pagg. 93-129

A. Zucchetti, *Privacy: dati personali e sensibili, sicurezza, regolamento, sanzioni. Problemi e casi pratici*, Giuffrè, Milano 2005