

# GESTIONE DEI VERBALI E TUTELA DELLA PRIVACY

*Breve riflessione sulla tutela della privacy nella gestione del procedimento di applicazione delle sanzioni amministrative anche alla luce delle recenti modifiche al codice della privacy operate dalla legge di conversione del Decreto Milleproroghe.*

*A cura del Dott. Massimo Linarello*

- *Ufficiale di P.M. del Comune di Perugia*
- *Laurea in Giurisprudenza*
- *Diploma di Specializzazione per le Professioni Legali*
- *Idoneità all'Esame di Abilitazione per la Professione d'Avvocato*

***www.poliziamunicipale.it - riproduzione riservata***

*1) Ambito di applicazione del Codice della Privacy. – 2) Definizioni: trattamento, dati e soggetti. – 3) I diritti dell'interessato. – 4) Le modalità di trattamento dei dati. – 5) La c.d. "informativa" sulla privacy. – 6) Regole ulteriori per i soggetti pubblici. – 7) Le misure di sicurezza. – 8) Gli strumenti tutela della privacy. – 9) Le sanzioni.*

Le nuove frontiere del contenzioso davanti al Giudice di Pace si stanno spostando verso questioni pregiudiziali (art. 34 c.p.c.) che riguardano la normativa della privacy.

In questa scheda vi forniremo una concisa riflessione sulla tematica del trattamento dei dati personali nell'ambito del procedimento amministrativo di applicazione delle sanzioni amministrative, in modo che possiate replicare al meglio agli eventuali motivi di opposizione.

Il contributo è aggiornato alle recenti modifiche dell'apparato sanzionatorio del Codice della Privacy operate dal Decreto Milleproroghe (D.L. 30 dicembre 2008, n. 207 convertito in Legge 27 febbraio 2009, n. 14).

## **1) Ambito di applicazione del Codice della Privacy.**

Anzitutto il Codice della Privacy (Decreto legislativo 30/06/2003, n. 196 pubblicato in Gazzetta Ufficiale 29/07/2003, n. 174) disciplina **il trattamento dei dati personali** non effettuato da persone fisiche per fini esclusivamente personali, salvo destinati alla comunicazione sistematica o alla diffusione.

### **Art. 5 (Oggetto ed ambito di applicazione)**

- 1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.*
- 2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione*

europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

#### **Art. 6 (Disciplina del trattamento)**

1. Le disposizioni contenute nella presente Parte [Parte Prima, Disposizioni Generali, artt. 1-45] si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II.

## **2) Definizioni: trattamento, dati e soggetti.**

Per una prassi di origine comunitaria, divenuta ormai costante anche nel nostro ordinamento, il legislatore ha dettato una serie di definizioni che sono utilissime per limitare l'ambito di applicazione dello stesso Codice.

L'art. 4 del D.lgs. 196/03 definisce il trattamento dei dati

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;

distinguendo i possibili dati in categorie

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;

nonché definendo i soggetti del trattamento in:

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;

Le modalità di nomina o di individuazione di tali soggetti che effettuano il trattamento sono definite dagli art. 28, 29 e 30:

#### **Art. 28 (Titolare del trattamento)**

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

#### **Art. 29 (Responsabile del trattamento)**

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

#### **Art. 30 (Incaricati del trattamento)**

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

Il legislatore in definitiva ha previsto espressamente che vi debba essere obbligatoriamente un Titolare del trattamento, a cui possono aggiungersi dei Responsabili (facoltativamente) e degli Incaricati, senza specificare la natura del rapporto che lega il primo agli ultimi (lavoro subordinato, autonomo, collaborazione o appalto).

- Il **titolare** è colui (persona fisica, giuridica, PA o altro ente) che esercita il potere decisionale in materia di modalità, finalità e sicurezza del trattamento.
- Il **responsabile** è colui (persona fisica, giuridica, PA o altro ente) che è preposto dal titolare al trattamento, scelto per esperienza, capacità ed affidabilità, con indicazione scritta dei compiti che deve eseguire.
- L'**incaricato** invece è la persona fisica
  - o designata per iscritto al compimento di operazioni di trattamento dei dati,
  - o oppure preposta ad una unità specifica autorizzata per iscritto al trattamento di un ambito specifico di dati.

Quest'ultimo periodo semplifica notevolmente le procedure di individuazione degli incaricati al trattamento, in quanto **non bisogna necessariamente designarli per iscritto uno ad uno**, bensì è sufficiente (*si considera tale*) inserirli dentro una unità già autorizzata per iscritto al trattamento di certi dati.

### **3) I diritti dell'interessato.**

All'interessato sono riconosciuti una serie di diritti, da var valere secondo gli artt. 8 e ss. Cod.:

#### **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.

#### 4) Le modalità di trattamento dei dati.

Tutti i dati personali devono essere trattati in modo lecito, secondo correttezza, raccolti per scopi determinati, pertinenti, completi e non eccedenti dette finalità.

##### **Art. 11 (Modalità del trattamento e requisiti dei dati)**

1. I dati personali oggetto di trattamento sono:

- a) trattati in modo lecito e secondo correttezza;
- b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili 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.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Il comma 2 dell'art. 11 è di una importanza fondamentale perché vieta l'utilizzo dei dati trattati in violazione della disciplina "rilevante" in materia di trattamento.

Il legislatore non specifica il concetto di rilevanza, lasciando all'interprete l'annoso compito. In senso rigorosamente *letterale* "rilevante" ha un significato di ampia portata (*importante, notevole, consistente, significativo*) che potrebbe condurre a risultati completamente opposti, ovvero ad un allargamento od un restringimento del divieto.

In senso *ampliativo* rilevante indicherebbe tutte le norme, comprese quelle extra-codicistiche come i regolamenti o i codici deontologici che disciplinano il trattamento dei dati. Tuttavia in questa ipotesi l'aggettivo "rilevante" risulterebbe paradossalmente inutile, in quanto il riferimento alla "disciplina in materia di trattamento" sarebbe stata sufficiente per comprendere anche le norme extra-codicistiche. Quindi il legislatore ha sicuramente voluto dare un significato diverso al termine.

La rilevanza interpretata in senso *restrittivo* porterebbe ad escludere alcune violazioni dalla sanzione della inutilizzabilità. La limitazione potrebbe essere di tipo *qualitativo*, escludendo le fattispecie meno gravi come quelle sanzionate in modo amministrativo (non a titolo penale), oppure di tipo *quantitativo* facendo riferimento ad almeno una pluralità di violazioni.

In realtà, posto che nessuna delle suddette interpretazioni pare pienamente convincente, rilevante potrebbe significare “*determinante al fine del trattamento*”, ovvero sarebbe corretto inibire l’utilizzo dei dati in tutte quelle ipotesi di violazione che minerebbero alla radice il legittimo possesso dei dati. Detto in altri termini, se la norma violata è quella che legittima il potere di raccogliere e detenere i dati personali (*l’an* del trattamento) è sacrosanta la sanzione della inutilizzabilità, mentre nei casi in cui viene violata una norma procedurale irrilevante ai fini del possesso dei dati stessi (*il quomodo*), sia essa di natura codicistica o extra-codicistica, il divieto di utilizzazione non ricorrerebbe.

Così in caso di mancata informazione preventiva e consenso al trattamento (nei casi in cui esso è necessario), la raccolta dei dati sarebbe viziata *ab origine* in modo determinante, perché senza il consenso dell’interessato il titolare/responsabile/incaricato non ha il potere di possedere (trattare) quei dati, quindi sarebbe giusta la sanzione (aggiuntiva) dell’inutilizzabilità.

#### 5) La c.d. “informativa” sulla privacy.

A tutela dei diritti dell’interessato è posta la normativa sulla c.d. “**informativa**” che viene data all’interessato:

- prima della raccolta dei dati se questa avviene presso di lui (art. 13 c. 1)
- successivamente se la raccolta dei dati non avviene presso di lui (art. 13 c. 4).

L’informativa viene data funzionalmente per ottenere un consenso al trattamento dei dati anche se, come vedremo in seguito, per i soggetti pubblici, il consenso non è sempre necessario.

La distinzione di cui sopra ci permette di differenziare la raccolta di dati personali come *nome, cognome, luogo e data di nascita, codice fiscale e residenza*, essenziali ai fini dell’accertamento delle sanzioni amministrative e per far nascere l’obbligazione pecuniaria, a seconda che avvenga:

- direttamente presso l’interessato a seguito di contestazione immediata,
- ovvero presso i pubblici registri nei casi di contestazione differita.

Nel **primo caso** la raccolta di dati è disciplinata dal primo comma e l’informativa sulla privacy deve essere resa *previamente* alla raccolta e preferibilmente in modo scritto a tergo del verbale.

Nel **secondo caso** invece l’eventuale informativa seguirebbe le regole del quarto comma, ovvero sarebbe *successiva*, al momento della registrazione o al momento della comunicazione (ad esempio alla notifica del verbale di infrazione). Tuttavia tale **informativa del comma 4** (quella successiva perché la raccolta dei dati non è avvenuta presso l’interessato) **non è necessaria**, quindi può essere omessa, **nei casi in cui i dati sono trattati in base ad un obbligo previsto dalla legge**, così come avviene per le sanzioni amministrative in cui la legge (ad es. il D.lgs. 285/92 o la Lg. 689/81) impone di contestare l’infrazione trattando necessariamente i dati del trasgressore e dell’obbligato in solido (anche non presente). Si consiglia tuttavia di uniformare la modulistica inserendo comunque l’informativa *ex art. 13* in entrambe le casistiche per evitare inutili contenziosi.

### **Art. 13 (Informativa)**

1. 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;
- 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.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali **non sono raccolti presso l'interessato**, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al **comma 4 non si applica** quando:

- a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
- b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
- c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiara manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

## **6) Regole ulteriori per i soggetti pubblici.**

Al Capo II (artt. 18-22) del Titolo I sono indicate **regole ulteriori per i soggetti pubblici** distinguendo a seconda che si tratti di dati personali, dati sensibili o dati giudiziari.

Per quello che concerne l'attività di gestione delle sanzioni amministrative i dati che vengono generalmente trattati, nel rispetto del principio della pertinenza di cui all'art. 11, sono quelli personali c.d. identificativi (art. 4 c. 1 lett. C) dei soggetti obbligati al pagamento delle sanzioni amministrative, che non sono né sensibili (lett. D), né giudiziari (lett. E). Pertanto le norme da applicare sono gli art. 18 e 19 che legittimano il trattamento dei dati esclusivamente per i **fini istituzionali** e **senza** che sia necessario chiedere il **consenso** dell'interessato.

### **Art. 18 (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)**

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici **non devono richiedere il consenso dell'interessato.**

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

**Art. 19 (Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)**

1. 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, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. 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.

3. 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.

Accade spesso che la PA decida di affidare all'esterno (c.d. **esternalizzazione**) alcuni segmenti della gestione delle sanzioni amministrative, comportando questa scelta delle ricadute in materia di tutela della privacy.

Alcuni giudici<sup>1</sup> hanno sostenuto proprio in virtù dell'art. 19 c. 3 che la comunicazione o la diffusione di dati personali ai privati (ovvero alle ditte che gestiscono l'attività esternalizzata) non sarebbe consentita perché nessuna norma lo prevede espressamente (infatti né il C.d.S., né la Legge n. 689/81 lo prevedono espressamente).

Questa interpretazione parte da due errori di fondo:

- a) non considerare le ditte private appaltatrici o gestori di un servizio quali soggetti che curano il trattamento ai sensi degli artt. 4, 28, 29 e 30 Cod.
- b) nel considerare la comunicazione o diffusione illecita anche quella effettuata dal titolare al responsabile o incaricato.

Come potete ben capire la vicenda avrebbe del paradossale: da un lato il Codice prevede che più soggetti possano trattare i dati, dall'altro la norma ne vieterebbe la comunicazione tra gli stessi.

Ripartiamo dalle definizioni di cui all'art. 4:

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;

La vera "comunicazione" o "diffusione" disciplinata dall'art. 19 c. 3 è quella effettuata

- a) **dal rappresentante del titolare,**
- b) **dal responsabile**
- c) **e dagli incaricati**

ovvero dai soggetti che curano il trattamento (ex artt. 4, 28, 29 e 30),:

- 1) **a uno o più soggetti determinati diversi dall'interessato** (comunicazione)
- 2) **oppure a soggetti indeterminati** (diffusione).

E' palesemente errata l'interpretazione che considera illegittima la comunicazione tra i soggetti del trattamento, dal titolare e/o responsabile agli incaricati, perché è il Codice stesso che li legittima a

<sup>1</sup> **Giudice di pace di Vignola, 07 ottobre 2008, n. 273** "Inoltre, a parere del giudice, con la nomina della XXX quale Responsabile del trattamento dei dati rilevati dal sistema \*\*\*-RED viene a realizzarsi una palese violazione delle norme poste a tutela della riservatezza (Dlgs sulla c.d. privacy 30.6.2003 n. 196) in quantoché una società privata con fini di lucro è messa dall'ente pubblico nella condizione di disporre di migliaia di filmati riguardanti cittadini e veicoli di loro proprietà presenti in un determinato posto in giorno e ora precisi, nel momento in cui viene formalmente commessa una violazione. Secondo l'art. 19.3 del Dlgs 196/03, "3. 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." e se le norme del cds non consentono alla p.a., come in effetti non le consentono, la messa a disposizione di una società privata dei dati raccolti coi filmati \*\*\*-RED, a maggior ragione dovrà ritenersi vietata la raccolta per conto della p.a. di quei dati. Si rammenta che l'Autorità garante dei dati personali, con provvedimento del 5.11.2004 (Presidente Rodotà, Relatore Paissan) adottata nei confronti del comune di Teramo, già si è pronunciata nel senso suddetto. Pertanto, per la gravità di quanto sopra rilevato, il giudice dispone la trasmissione della presente sentenza al Procuratore della Repubblica di Modena per i provvedimenti di sua competenza."

raccogliere e trattare i dati. Diverso è il caso in cui un terzo estraneo al trattamento (ad es. un privato cittadino) chieda di ottenere dei dati inerenti le contravvenzioni altrui: la PA che li fornisce effettuerebbe una comunicazione (illecita se non prevista dalla legge).

La stessa sentenza richiama a proprio convincimento un **provvedimento dell'Autorità Garante del 5 novembre 2004** che testualmente vi riportiamo nella parte decisoria e più significativa:

*Il ricorso verte sul trattamento di dati personali effettuato da un comune in relazione al un procedimento di accertamento di un'infrazione al codice della strada.*

*Contrariamente a quanto sostenuto dall'ente resistente, il Comune di XXX è titolare del trattamento dei dati personali in questione, di cui la raccolta è iniziata già a cura dell'agente di polizia municipale che ha elevato la contravvenzione; dati comunicati poi a YYY S.p.A., società cui è stato affidato, con deliberazione comunale, il servizio per la gestione integrata delle contravvenzioni alle norme del codice della strada.*

*Il trattamento di dati personali da parte di soggetti pubblici è consentito per lo svolgimento delle funzioni istituzionali nei limiti già stabiliti dagli artt. 22 e 27 della legge n. 675/1996 e, ora, agli artt. 18 s. del citato Codice, senza che possa essere richiesto il consenso dell'interessato.*

*Tale Codice prevede apposite garanzie per quanto attiene all'eventuale comunicazione dei dati dall'ente pubblico ad altri soggetti pubblici o a soggetti privati. Per ciò che concerne, specificamente, **l'esternalizzazione di servizi** (ivi compresa l'ipotesi in oggetto), tale modalità di realizzazione del fine pubblico connesso all'attività per cui si richiede una collaborazione esterna può essere perseguita ferma restando la necessità che, nel rispetto delle indicate disposizioni del Codice, il trattamento dei dati personali di cittadini ed utenti sia conforme alle previsioni di legge. Ciò, in particolare, con riferimento alle forme e alle modalità idonee per legittimare al trattamento dei dati terzi estranei all'ente (designazione di eventuali **responsabili** del trattamento - art. 29 del Codice-; individuazione di tutte le persone fisiche cui è demandato il trattamento medesimo e quindi **incaricati** dello stesso art. 30 del medesimo Codice), alla specifica indicazione di istruzioni da parte del titolare del trattamento (che è l'ente pubblico, anche quando lo stesso affidi eventualmente a terzi singoli aspetti o procedure concernenti, come nel caso di specie, pubbliche funzioni) e alla necessaria adozione di idonee misure di sicurezza.*

***Nella documentazione prodotta dal resistente** (peraltro lacunosa ed in parte contraddittoria) compare solo una bozza incompleta di convenzione fra il Comune di XXX e YYY S.p.A., nella quale non vi è peraltro alcun cenno ai profili relativi alla protezione dei dati, né viene specificato se la predetta società rivesta o meno il ruolo di responsabile del trattamento.*

*Le modalità della preposizione di YYY S.p.A. non risulta inoltre da altri atti o documenti acquisiti.*

*Mancando idonei elementi comprovanti la liceità del trattamento in questione, va disposto ai sensi dell'art. 150, comma 2, del Codice che il Comune di XXX si astenga, entro e non oltre dieci giorni a far data dalla ricezione del presente provvedimento, da ogni trattamento dei dati personali del ricorrente attinenti alla predetta contestazione di violazione amministrativa. Ciò, ad eccezione della sola conservazione dei dati o del loro eventuale utilizzo in sede giudiziaria in rapporto ad eventuali iniziative assunte al riguardo dall'interessato.*

Come si può leggere con chiarezza dal provvedimento del Garante, benché sfavorevole alla PA (XXX), è ammesso pacificamente che, nell'ambito di una esternalizzazione di servizi, anche soggetti estranei possano trattare i dati a determinate condizioni:

- 1) vengano **nominati responsabili o incaricati** del trattamento
- 2) vengano date **specifiche istruzioni** sulle attività da effettuare
- 3) vengano adottate idonee **misure di sicurezza** (trasmissione telematica, password di accesso, crittografia, ecc.).

Per evitare un provvedimento inibitorio del Garante questi tre punti devono essere specificamente allegati e documentati. Analoga allegazione dovrà avvenire nei giudizi di **opposizione alle sanzioni amministrative**, in cui la questione dell'illecito trattamento può venire deciso incidentalmente (art. 34 c.p.c.) allo scopo di ottenere l'inutilizzabilità dei dati (art. 11 c. 2 Cod.) e provocando l'annullamento della sanzione amministrativa.

In questi casi una buona eccezione di merito ci viene fornita dall'**art. 21 octies c. 2 Lg. 241/90** *“Non è annullabile il provvedimento adottato in violazione di norme sul procedimento o sulla forma degli atti qualora, per la natura vincolata del provvedimento, sia palese che il suo contenuto dispositivo non avrebbe potuto essere diverso da quello in concreto adottato”*. Il verbale di contestazione delle sanzioni amministrative è sicuramente di natura vincolata (non vi sono margini di discrezionalità nella scelta di cosa comminare e quanto), in cui è palese (ovvero il giudice potrebbe dedurlo anche d'ufficio) che il contenuto dispositivo (ovvero la condanna al pagamento della sanzione) non sarebbe stato diverso da quello in concreto adottato con il rispetto delle norme sul procedimento o sulla forma (ad es. la normativa non rilevante sulla disciplina della privacy).

## 7) Le misure di sicurezza.

Il legislatore ha previsto una serie di obblighi di sicurezza a carico del titolare del trattamento finalizzati ad evitare la distruzione o la perdita anche accidentale dei dati, nonché l'accesso non autorizzato o il trattamento non consentito o non conforme alle finalità della raccolta.

Le misure minime di sicurezza sono indicate nell'art. 33, sanzionate in caso di inosservanza dalla norma penale (l'art. 169 c. 1 Cod.) nonché dalla norma amministrativa (l'art. 162 c. 2 bis), in virtù delle recenti modifiche operate dal Decreto Milleproroghe convertito in legge.

Per quanto riguarda la **gestione delle sanzioni amministrative**, vista la ormai diffusa informatizzazione delle attività di raccolta e conservazione dei dati, le prescrizioni da adottare sono, oltre quelle più generali dell'art. 31, anche le più specifiche dell'art. 34 (Trattamento con strumenti elettronici).

Tra queste una in particolare sta animando le riflessioni dei giuristi più attenti, l'obbligo di tenere un aggiornato **documento programmatico della sicurezza** (art. 34 c. 1 lett. G), essendo possibile ipotizzare la illiceità del trattamento in sua assenza con conseguente annullamento delle sanzioni amministrative contestate. Analizziamo analiticamente questa normativa.

Anzitutto che tipo di dati vengono trattati nell'ambito delle sanzioni amministrative?

Non sono né dati sensibili (art. 4 c. 1 lett. d), né dati giudiziari (lett. e) e, quindi rientrano tra i **dati personali** (lett. b), specificamente dati **identificativi** (lett. c) delle persone.

Quali obblighi deve rispettare il titolare del trattamento?

Gli obblighi di sicurezza sono indicati a livello generale dall'art. 31, ma sono indicati in modo più analitico dall'art. 33 che disciplina le misure minime da adottare, precetto sanzionato in modo penale e amministrativo come abbiamo già accennato.

L'art. 33 richiama sia l'art. 31 che speciali disposizioni in tema di sicurezza, nonché tutte le norme del capo II (artt. 33-36) a seconda del tipo di dati che vengono trattati.

In caso di dati trattati con strumenti elettronici, come avviene nella stragrande maggioranza dei comandi di polizia municipale, le regole da adottare sono indicate nell'art. 34 ed in particolare:

- a) autenticazione informatica,
- b) gestione delle credenziali di autenticazione,
- c) sistemi di autorizzazione,
- d) individuazione degli incaricati al trattamento,

- e) protezione dagli accessi esterni,
- f) copie di sicurezza dei dati,
- g) documento programmatico della sicurezza
- h) cifratura per determinati tipi di dati.

Il mancato rispetto di dette prescrizioni renderebbe il trattamento dei dati illecito (art. 34 c. 1) e conseguirebbe la inutilizzabilità dei dati ai sensi dell'art. 11 c. 2 Cod.

Così avverrebbe anche nel caso di **mancato aggiornamento del documento programmatico della sicurezza** tuttavia, il comma 2 *bis* dell'art. 34 Cod., aggiunto dall'articolo 29, comma 1, del D.L. 25 giugno 2008, n. 112, come modificato dalla legge 6 agosto 2008, n. 133, in sede di conversione, ha inserito una novità che interessa vivamente la PA.

Il tanto auspicato documento programmatico della sicurezza, nel caso in cui il trattamento riguardi esclusivamente i **dati personali non sensibili** (o dati sensibili costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale) può essere **sostituito da una autocertificazione** ex art. 47 DPR 445/00 resa dal titolare del trattamento in cui dichiararsi di aver adottato tutte le altre misure di sicurezza (lett. a, b, c, d, e, f, h).

In questi casi, qualora i contenziosi sulle sanzioni amministrative riguardino incidentalmente le questioni della privacy, ed in particolare l'aggiornamento di detto documento, è sufficiente allegare la prescritta autocertificazione del titolare del trattamento per far decadere *ex lege* l'eccezione.

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;

#### **Art.31 (Obblighi di sicurezza)**

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

#### **Art.33 (Misure minime)**

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo [Capo II, artt. 33-36] o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

#### **Art.34 (Trattamenti con strumenti elettronici)**

1. 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;
- 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.

1-bis. Per i soggetti che trattano soltanto dati personali non sensibili e che trattano come unici dati sensibili quelli costituiti dallo stato di salute o malattia dei propri dipendenti e collaboratori anche a progetto, senza indicazione della relativa diagnosi, ovvero dall'adesione ad organizzazioni sindacali o a carattere sindacale, la tenuta di un aggiornato documento programmatico sulla sicurezza e' sostituita dall'obbligo di autocertificazione, resa dal

titolare del trattamento ai sensi dell'articolo 47 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, di trattare soltanto tali dati in osservanza delle altre misure di sicurezza prescritte. In relazione a tali trattamenti, nonché a trattamenti comunque effettuati per correnti finalità amministrative e contabili, in particolare presso piccole e medie imprese, liberi professionisti e artigiani, il Garante, sentito il Ministro per la semplificazione normativa, individua con proprio provvedimento, da aggiornare periodicamente, modalità semplificate di applicazione del disciplinare tecnico di cui all'Allegato B) in ordine all'adozione delle misure minime di cui al comma 1 (1).

(1) Comma aggiunto dall'articolo 29, comma 1, del D.L. 25 giugno 2008, n. 112, come modificato dalla legge 6 agosto 2008, n. 133, in sede di conversione.

## **8) Gli strumenti tutela della privacy.**

La Parte III del Codice di occupa della tutela dei diritti dell'interessato e della sanzioni. Sono all'uopo previsti tre strumenti di tutela amministrativa:

### **Art. 141 (Forme di tutela)**

1. L'interessato può rivolgersi **al Garante**:

- a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
- b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
- c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo.

### **Art. 145 (Ricorsi)**

1. I diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante.
2. Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.
3. La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

In alternativa alla tutela amministrativa, salva l'opposizione ex art. 151 contro i provvedimenti del Garante, è possibile ricorrere all'Autorità giudiziaria Ordinaria (il tribunale in composizione monocratica, ai sensi dell'art. 152 Cod.).

### **Art. 152 (Autorità giudiziaria ordinaria)**

1. 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.
2. 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.
3. Il **tribunale** decide in ogni caso in composizione monocratica.

## 9) Le sanzioni.

ARTICOLI VIOLATI	SANZIONI AMMINISTRATIVE (7) (8)
<b>articolo 13</b> Omessa o inidonea informativa all'interessato	<b>Art. 161 c. 1</b> sanzione amministrativa da 6000 euro a 36000 euro (1)
<b>cessione dei dati in violazione:</b> - dell' <b>articolo 16, comma 1, lettera b)</b> - o di <b>altre disposizioni in materia di disciplina del trattamento</b>	<b>Art. 162 c. 1</b> sanzione amministrativa del pagamento di una somma da 10000 euro a 60000 euro (1)
<b>articolo 84, comma 1</b>	<b>Art. 162 c. 2</b> sanzione amministrativa del pagamento di una somma da 1000 euro a 6000 euro (2).
violazione - delle misure indicate nell' <b>articolo 33</b> - o delle disposizioni indicate nell' <b>articolo 167</b>	<b>Art. 162 c. 2 bis</b> e' altresì applicata in sede amministrativa, in ogni caso la sanzione del pagamento di una somma da 20000 euro a 120000 euro Nei casi di cui all'articolo 33 e' escluso il pagamento in misura ridotta (3).
inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui all' <b>articolo 154, comma 1, lettere c) e d)</b>	<b>Art. 162 c. 2 ter</b> la sanzione del pagamento di una somma da 30000 euro a 180000 euro (4).
<b>art. 132, commi 1 e 1-bis</b> conservazione dei dati di traffico	<b>Art. 162 bis (5)</b> la sanzione amministrativa pecuniaria da 10.000 euro a 50.000 euro
<b>articoli 37 e 38</b> Omessa o incompleta notificazione	<b>Art. 163</b> sanzione amministrativa del pagamento di una somma da 20000 euro a 120000 euro
<b>articoli 15, comma 2, e 157</b> Omessa informazione o esibizione al Garante	<b>Art. 164</b> la sanzione amministrativa del pagamento di una somma da 10000 euro a 60000 euro (6).
(1) Comma modificato dall'articolo 44, comma 3, lettera a), del D.L. 30 dicembre 2008, n. 207. (2) Comma modificato dall'articolo 44, comma 3, lettera b), del D.L. 30 dicembre 2008, n. 207. (3) Comma inserito dall'articolo 44, comma 3, lettera c), del D.L. 30 dicembre 2008, n. 207. (4) Comma inserito dall'articolo 44, comma 3, lettera c), del D.L. 30 dicembre 2008, n. 207. (5) Articolo inserito dall'articolo 5 del D.Lgs. 30 maggio 2008 n. 109 e successivamente modificato dall'articolo 44, comma 4, del D.L. 30 dicembre 2008, n. 207. (6) Articolo modificato dall'articolo 44, comma 6, del D.L. 30 dicembre 2008, n. 207. (7) Vedi Art.164 bis per casi di minore gravita' e ipotesi aggravate (Articolo inserito dall'articolo 44, comma 7, del D.L. 30 dicembre 2008, n. 207) (8) Vedi Art.166 per il procedimento di applicazione (1-8) Il D.L. 30 dicembre 2008, n. 207 (c.d. Decreto Milleproroghe) è stato convertito in Legge 27 febbraio 2009, n. 14	

ARTICOLI VIOLATI	SANZIONI PENALI
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 a) al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129 b) al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45	<b>Art. 167 c. 1</b> (Ipotesi a) - se dal fatto deriva nocumento, con la reclusione da 6 a 18 mesi - se il fatto consiste nella comunicazione o diffusione, con la reclusione da 6 a 24 mesi (Ipotesi b) - se dal fatto deriva nocumento, con la reclusione da 1 a 3 anni
Falsità nelle dichiarazioni e notificazioni al Garante	<b>Art. 168</b> reclusione da 6 mesi a 3 anni.
Omette di adottare le misure minime previste dall' <b>articolo 33</b>	<b>Art. 169 c. 1</b> è punito con l'arresto sino a 2 anni [o con l'ammenda da 10000 euro a 50000 euro.] (1)
Inosservanza di provvedimenti del Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c)	<b>Art. 170</b> reclusione da 3 mesi a 2 anni
articoli 113, comma 1, e 114	<b>Art. 171</b> sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300 (l'ammenda da lire 300.000 a lire 3.000.000 o con l'arresto da 15 giorni ad un anno)
(1) Comma modificato dall'articolo 44, comma 9, lettera a), del D.L. 30 dicembre 2008, n. 207.(c.d. Decreto Milleproroghe) convertito in Legge 27 febbraio 2009, n. 14	