AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione
a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore: Prof. Giuseppe Di Gaspare

IL TRATTAMENTO DEI DATI PERSONALI DA PARTE DEI SOGGETTI PUBBLICI ALLA LUCE DEL NUOVO CODICE PRIVACY

Avv. Pierangela Rodilosso

SOMMARIO: 1. PREMESSA. 2. PRESUPPOSTI GENERALI DI LICEITÀ DEL TRATTAMENTO. 3. REGOLE SPECIFICAMENTE RIVOLTE AI SOGGETTI PUBBLICI. 4. LA VIDEOSORVEGLIANZA NEGLI ENTI PUBBLICI. 5. LA TUTELA RISARCITORIA. 6. LA TUTELA PENALE. 7. GLI ILLECITI AMMINISTRATIVI.

1. PREMESSA

Il 1° gennaio 2004 è entrato in vigore il D. Lgs. 30 giugno 2003 n. 196 (di seguito definito come "Codice Privacy"), contenente importanti principi innovativi, ispirati all'esigenza di rafforzare la tutela della riservatezza dei cittadini.

Il Codice Privacy disciplina il trattamento dei dati personali effettuato dai soggetti pubblici sia attraverso la previsione di norme di carattere generale, applicabili a qualsiasi trattamento, a prescindere dalla tipologia del dato elaborato o dalla natura giuridica del Titolare e volte a circoscrivere i limiti di liceità del trattamento, che attraverso una serie di disposizioni specificamente rivolte ai soggetti pubblici ed applicabili, pertanto, esclusivamente ai trattamenti da questi effettuati.

2. PRESUPPOSTI GENERALI DI LICEITÀ DEL TRATTAMENTO

Alla luce di quanto sopra premesso, pertanto, **i soggetti pubblici** che intendano procedere alla raccolta e all'elaborazione di dati personali devono, in primo luogo operare nel rispetto dei presupposti di liceità individuati in via generale dal legislatore.

In particolare, a tutela dell'identità personale e della riservatezza dell'interessato, l'art. 11 del Codice pone in capo al Titolare del trattamento l'obbligo di rispettare precise modalità di raccolta ed elaborazione dei dati e determinati requisiti degli stessi.

■ LICEITÀ E CORRETTEZZA

La prima regola imposta dal legislatore a tutti i Titolari del trattamento, indipendentemente dalla loro natura pubblica o privata, è quella che prescrive di gestire i dati trattati in modo lecito e secondo correttezza[1]. La **liceità del trattamento**, fulcro della tutela del diritto alla protezione dei propri dati personali consacrato dall'art. 1 del Codice[2], deve essere valutata

[1] Decreto Legislativo n. 196/2003, art. 11 *(Modalità del trattamento e requisiti dei dati)*, comma 1°, lett. a): *"1. I dati personali oggetto di trattamento sono:*
a) trattati in modo lecito e secondo correttezza".

[2] Decreto Legislativo n. 196/2003, art. 1 *(Diritto alla protezione dei dati personali)*: *"Chiunque ha diritto alla protezione dei dati personali che lo riguardano".*

non solo in relazione alle disposizioni in materia di tutela della privacy, ma anche alla luce di altre norme eventualmente rilevanti nell'ambito del trattamento stesso, quali ad esempio quelle relative al segreto d'ufficio o allo statuto dei lavoratori[3].

Il trattamento dei dati deve avvenire, inoltre, nel rispetto del **principio di correttezza**, riconducibile al più ampio principio di solidarietà sociale sancito dall'art. 2 della Costituzione e previsto dal legislatore al fine di evitare che l'elaborazione dei dati personali persegua propositi dolosi o rechi pregiudizio all'interessato[4].

■ TRASPARENZA DEGLI SCOPI PERSEGUITI

L'art. 11 del Codice Privacy, oltre a prescrivere la conformità del trattamento ai principi di liceità e correttezza, dispone che i dati vengano trattati nel rispetto della **trasparenza degli scopi perseguiti**, quindi secondo finalità determinate, legittime e rese esplicite attraverso strumenti quali l'informativa agli interessati, il diritto di accesso ai dati e la consultazione del registro generale dei trattamenti tenuto dal Garante[5].

Il principio di trasparenza rappresenta, inoltre, il presupposto logico del principio di necessità previsto dall'art. 3 del Codice con espresso riferimento ai trattamenti effettuati mediante l'impiego di sistemi informativi e programmi informatici[6]. La suddetta norma dispone, infatti, che i software siano configurati in modo tale da privilegiare l'uso di dati anonimi e tali da non consentire un'identificazione diretta dell'interessato[7].

■ PERTINENZA E NON ECCEDENZA DELLE INFORMAZIONI RACCOLTE

Strettamente connesso alla regola della trasparenza degli scopi perseguiti è il principio di pertinenza e non eccedenza delle informazioni raccolte, che impone ai Titolari di **limitare**

---

[3] Cfr. sull'argomento M. G. Losano, *Commento all'art. 9*, in E. Giannantonio – M. G. Losano – V. Zeno-Zencovich (a cura di), *La tutela dei dati personali. Commentario alla legge 675/96*, Padova, Cedam, 1999, p. 105.

[4] Cfr. P. Iamiceli, *Liceità, correttezza, finalità nel trattamento dei dati personali*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Vol. I, Milano, Giuffrè, 2003, pp. 419-435.

[5] Decreto Legislativo n. 196/2003, art. 11 *(Modalità del trattamento e requisiti dei dati)*, comma 1°, lett. b): *"1. I dati personali oggetto di trattamento sono:*
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi".
Cfr. anche R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, p. 70.

[6] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, p. 71.

[7] Decreto Legislativo n. 196/2003, art. 3 *(Principio di necessità nel trattamento dei dati)*: *"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".*

l'impiego dei dati personali, consentendo unicamente la raccolta e l'elaborazione di quelli indispensabili al raggiungimento degli scopi dichiarati[8].

Una specificazione del suddetto principio è riscontrabile, con specifico riferimento al trattamento di dati sensibili e giudiziari da parte dei soggetti pubblici, nell'art. 22, comma 3, del Codice, che consente unicamente l'elaborazione delle informazioni *"indispensabili"* per svolgere le attività istituzionali dell'ente, che non potrebbero essere svolte mediante il ricorso a dati anonimi o di natura non sensibile[9].

■ **ESATTEZZA, AGGIORNAMENTO E COMPLETEZZA DEI DATI**

La tutela dell'identità personale viene garantita dal legislatore anche attraverso la previsione, in capo al Titolare del trattamento, dell'obbligo di raccogliere **informazioni veritiere, aggiornate e complete**, tali dunque da ben rappresentare la reale specificità di un individuo[10].

Occorre altresì rilevare che all'obbligo del Titolare di garantire la qualità dei dati trattati corrisponde un potere di intervento diretto dell'interessato il quale, ai sensi dell'art. 7 del Codice, ha il diritto di richiedere l'aggiornamento, la rettificazione e, quando vi abbia interesse, anche l'integrazione delle informazioni raccolte.

■ **GARANZIA DEL DIRITTO ALL'OBLIO**

Il Titolare del trattamento, soggetto pubblico o privato che sia, deve inoltre garantire all'interessato il diritto ad essere dimenticato, tutelato dal legislatore attraverso la previsione di un limite temporale alla conservazione dei dati. Questi ultimi, infatti, devono essere **conservati solo per il periodo di tempo indispensabile al trattamento** e, una volta decorso tale periodo, devono essere cancellati o resi anonimi, onde evitare che siano registrate informazioni non più necessarie per il raggiungimento dello scopo dichiarato dal titolare nell'informativa fornita all'interessato[11].

Da una lettura combinata dell'art. 11, comma 1, lett. d) e dell'art. 7, comma 3, lett. b) (che attribuisce all'interessato il diritto di chiedere la cancellazione o la trasformazione in forma

---

[8] Decreto Legislativo n. 196/2003, art. 11 *(Modalità del trattamento e requisiti dei dati)*, comma 1°, lett. d): *"1. I dati personali oggetto di trattamento sono:*
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati".

[9] Decreto Legislativo n. 196/2003, art.22 *(Principi applicabili al trattamento di dati sensibili e giudiziari)*, comma 3°: *"3. 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 di natura diversa".*

[10] Decreto Legislativo n. 196/2003, art. 11 *(Modalità del trattamento e requisiti dei dati)*, comma 1°, lett. c) e d): *"1. I dati personali oggetto di trattamento sono:*
c) esatti e, se necessario aggiornati;
d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati".

[11] Decreto Legislativo n. 196/2003, art. 11 *(Modalità del trattamento e requisiti dei dati)*, comma 1°, lett. e): *"1. I dati personali oggetto di trattamento sono:*
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".

anonima dei dati trattati in violazione di legge), si evince che il diritto all'oblio può essere inteso sia come libertà negativa, quindi come diritto ad essere dimenticato riconducibile al tradizionale concetto di diritto alla riservatezza, sia come libertà positiva, identificabile nel potere di controllo attribuito all'interessato e vicino al diritto alla protezione dei dati personali sancito dall'art. 1 del Codice[12].

■ INUTILIZZABILITÀ DEI DATI TRATTATI

A chiusura del sistema di regole generali cui deve essere improntato il trattamento dei dati personali da parte dei soggetti pubblici si pone il secondo comma dell'art. 11 del Codice, che sanziona la violazione dei principi sopra esposti con l'obbligo di **inutilizzabilità** delle informazioni trattate[13]. In particolare, fino a quando l'interessato non eserciti il diritto di chiedere la cancellazione o la trasformazione in forma anonima dei dati trattati di cui all'art. 7, comma 3, lett. b), il Titolare potrà continuare a detenere le informazioni, senza però poterle utilizzare per ulteriori operazioni di trattamento. Ne deriva che il dato trattato in violazione della disciplina vigente resterà "congelato" nella banca dati del Titolare, in attesa che lo stesso adempia alle norme violate o che l'interessato ne chieda la cancellazione[14].

3. REGOLE SPECIFICAMENTE RIVOLTE AI SOGGETTI PUBBLICI

Accanto ai generali presupposti di liceità del trattamento, cui sono tenuti ad attenersi sia i soggetti pubblici che i privati e gli enti pubblici economici, il Codice Privacy contiene un gruppo di disposizioni destinate in modo specifico ai soggetti pubblici e, pertanto, applicabili esclusivamente ai trattamenti da questi effettuati.

■ ESENZIONE DALL'ONERE DI RICHIESTA DEL CONSENSO

In particolare, l'art. 18 codifica espressamente **l'esenzione dei soggetti pubblici dall'onere di preventiva richiesta del consenso** all'interessato, salvo però quanto previsto per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici[15]. Il consenso, quindi, non ha di regola per la P.A. alcuna utilità giuridica, così come, dal punto di vista giuridico, risultano privi di fondamento quei comportamenti, talvolta riscontrati nella prassi, posti in essere da alcuni Comuni che hanno ritenuto di rafforzare la liceità del trattamento richiedendo, per trattamenti dotati di per sé dei requisiti di legge, anche il consenso dell'interessato[16].

---

[12] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, p. 74.

[13] Decreto Legislativo n. 196/2003, art. 11 *(Modalità del trattamento e requisiti dei dati)*, comma 2°: *"I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati"*.

[14] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, p. 76.

[15] Decreto Legislativo n. 196/2003, art. 18 *(Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)*, comma 4°: *"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"*.

[16] L. De Zotti, *Il Codice Privacy negli enti locali*, articolo pubblicato sul sito www.commercialistatelematico.com, in collaborazione con V. Frediani.

■ RISPETTO DELLE FUNZIONI ISTITUZIONALI

Il requisito del consenso, tuttavia, è stato sostituito in ambito pubblico con quello della "necessità del trattamento per il raggiungimento delle funzioni istituzionali dell'ente"[17]: i soggetti pubblici, quindi, possono raccogliere e gestire dati personali "comuni"[18] anche in assenza di norma di legge o di regolamento che preveda espressamente il trattamento specifico[19], ma **solo nell'ambito delle proprie funzioni istituzionali**, comprensive non solo dei trattamenti indispensabili per l'espletamento dei compiti dell'ente, ma anche di quelli volti comunque ad agevolare o rendere più rapida la realizzazione degli interessi pubblici affidati alla Pubblica Amministrazione[20].

La scelta del legislatore è stata dettata dall'esigenza di prevedere, nei rapporti tra il cittadino e la P.A., un parametro di liceità del trattamento che tenga conto del fatto che il cittadino si pone nei confronti di quest'ultima in una posizione di sostanziale disparità, e che sia tale da consentire alla P.A. di svolgere le proprie funzioni senza essere condizionata dal consenso dell'interessato, laddove questo abbia natura autorizzatoria[21].

■ COMUNICAZIONE DEI DATI A TERZI

Per quanto riguarda le **comunicazioni dei dati a terzi** (altri soggetti pubblici, privati ed enti pubblici economici), il Codice la consente solo quando è ammessa da una norma di legge o di regolamento. Tuttavia, se la comunicazione dei dati è rivolta ad altri soggetti pubblici, può anche prescindere da un'espressa previsione di legge o di regolamento, ma solo nel caso in cui:

- sia comunque necessaria per lo svolgimento delle funzioni istituzionali dell'ente;
- sia preceduta da apposita comunicazione al Garante, che potrà vietare il flusso di dati entro 45 giorni dal ricevimento della comunicazione, o disporne l'interruzione anche oltre tale termine[22] [23].

---

[17] Decreto Legislativo n. 196/2003, art. 18 *(Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)*, comma 2°: *"2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali"*.

[18] Si ricorda in proposito che al trattamento dei dati personali sensibili e giudiziari il legislatore riserva una serie di cautele ulteriori.

[19] Decreto Legislativo n. 196/2003, art. 19 *(Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)*, comma 1°: *"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"*.

[20] Cfr. P. Troiano, *Commento all'art. 27*, in C.M. Bianca – F.D. Busnelli et al., *Tutela della privacy*, pp. 628-642.

[21] G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione*, Milano, Giuffrè, 1997, pp. 45-51.

[22] Decreto Legislativo n. 196/2003, art. 19 *(Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)*, commi 2° e 3°: *"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*

■ TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI:

A) I DATI SENSIBILI

Al trattamento dei dati sensibili[24] effettuato da soggetti pubblici il legislatore riserva una serie di cautele ulteriori rispetto a quanto previsto per il trattamento dei dati "comuni": tra queste rientrano, ad esempio, l'uso di tecniche di cifratura per i dati tenuti con l'ausilio di strumenti elettronici o la conservazione separata dei dati idonei a rivelare lo stato di salute e la vita sessuale[25].

Occorre, inoltre, evidenziare che, relativamente al trattamento dei dati sensibili da parte dei soggetti pubblici, il Codice Privacy individua **tre possibilità**:

1. i soggetti pubblici possono trattare i dati sensibili solo se il trattamento risulta autorizzato da una **espressa disposizione di legge** nella quale siano specificati:
   - i tipi di dati che possono essere trattati;
   - i tipi di operazioni eseguibili su tali dati;
   - le finalità di rilevante interesse pubblico perseguite dai trattamenti[26] [27].

---

comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'art. 39, comma 2, e non è stata adottata la diversa determinazione del Garante".

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".

[23] Decreto Legislativo n. 196/2003, art. 39 *(Obblighi di comunicazione)*, comma 2°: *"2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante".*

[24] Il Codice Privacy definisce i "dati sensibili" all'art. 4, comma 1, lett. d) come *"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".*

[25] Decreto Legislativo n. 196/2003, art. 22 *(Principi applicabili al trattamento di dati sensibili e giudiziari)*, commi 6° e 7°: *"6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche 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.*

7. 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".

[26] Decreto Legislativo n. 196/2003, art. 20 *(Principi applicabili al trattamento di dati sensibili)*, comma 1°: *"1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite".*

[27] A titolo meramente esemplificativo, si ricorda che l'art. 62 del Codice Privacy considera di rilevante interesse pubblico, ai sensi degli artt. 20 e 21, le finalità relative alla tenuta degli atti e dei registri dello stato civile, delle anagrafi della

2. qualora una disposizione di legge si limiti a specificare la finalità di rilevante interesse pubblico, ma non indichi i tipi di dati sensibili che possono essere trattati e i tipi di operazioni eseguibili, il trattamento è consentito solo se i Titolari hanno provveduto ad individuare e rendere pubblici i tipi di dati e di operazioni oggetto del trattamento. La suddetta individuazione deve essere effettuata attraverso un **atto di natura regolamentare**, da adottare **entro il 31 dicembre 2005** [28] e da sottoporre periodicamente ad aggiornamento ed integrazione. Una novità del codice è rappresentata dal fatto che tale regolamento, d'ora in poi, dovrà conformarsi al parere espresso, anche sulla base di schemi-tipo, dal Garante, pena l'illiceità del trattamento eventualmente posto in essere[29]. Poiché il regolamento suddetto può essere emanato solo "in conformità" al parere del Garante, ne deriva che, a differenza di quanto generalmente previsto per gli altri atti consultivi di competenza dell'Autorità, il suddetto parere è da ritenersi obbligatorio e vincolante. Occorre altresì rilevare che i tipi di operazioni non individuate e rese pubbliche secondo le citate modalità non possono essere utilizzati[30].

3. la terza ipotesi delineata dal legislatore si verifica quando un determinato trattamento non sia previsto da alcuna norma di legge: in tal caso i soggetti pubblici possono **chiedere al Garante di individuare**, tra le varie attività ad essi demandate dalla legge, quelle che perseguono **"finalità di rilevante interesse pubblico"** e per le quali il trattamento è conseguentemente autorizzato. Il Garante deve comunicare la propria decisione entro 45 giorni dal ricevimento dell'istanza di autorizzazione; decorso tale periodo, il silenzio equivale a rigetto; anche in questo caso, tuttavia, è necessario che l'ente pubblico provveda ad identificare e rendere pubblici i tipi di dati e di operazioni oggetto del trattamento[31].

B) I DATI GIUDIZIARI

---

popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché al rilascio di documenti di riconoscimento o al cambiamento delle generalità.

[28] Il termine entro il quale i soggetti pubblici devono provvedere all'emanazione del Regolamento, originariamente fissato dall'art. 181, comma 1°, lett. a) del Codice Privacy al 30 settembre 2004, è stato prorogato al 31 dicembre 2005 dall'art. 3 del D. L. 24 giugno 2004, n. 158.

[29] Decreto Legislativo n. 196/2003, art. 20 *(Principi applicabili al trattamento di dati sensibili)*, comma 2° e 4°: *"2. 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, il trattamento è consentito 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 e nel rispetto dei principi di cui all'art. 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'art. 154, comma 1, lettera g), anche su schemi tipo.*

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente".

[30] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, pp. 106-107.

[31] Decreto Legislativo n. 196/2003, art. 20 *(Principi applicabili al trattamento di dati sensibili)*, comma 3°: *"3. Se il trattamento non è previsto espressamente da una disposizione di legge 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'art. 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2".*

Con riferimento al trattamento dei dati giudiziari[32] da parte dei soggetti pubblici è riscontrabile, rispetto alle tre ipotesi previste dal Codice relativamente al trattamento dei dati sensibili, qualche differenza: in particolare le rilevanti finalità di interesse pubblico, i tipi di dati e di operazioni eseguibili possono essere individuati non solo dalla legge, ma **anche da un provvedimento del Garante**.

Nei casi in cui, invece, una disposizione di legge specifichi le finalità di rilevante interesse pubblico, ma non i tipi di dati e di operazioni eseguibili, trova applicazione l'art. 20, commi 2 e 4; pertanto, i soggetti pubblici devono provvedere all'individuazione suddetta con atto di natura regolamentare, curandone periodicamente l'aggiornamento e l'integrazione[33].

C) I REGOLAMENTI PER I DATI SENSIBILI E GIUDIZIARI

Entro il 31 dicembre 2005 tutti i soggetti pubblici che intendano procedere al trattamento di dati sensibili e giudiziari, in assenza di un'espressa previsione di legge che individui i tipi di dati trattabili e di operazioni eseguibili, devono procedere all'individuazione dei tipi di dati e di operazioni oggetto del trattamento attraverso un atto di natura regolamentare, da sottoporre al parere del Garante. Al fine di agevolare questo adempimento, il Codice prevede la possibilità di elaborare "schemi tipo" di regolamento per settori omogenei. I rapporti di collaborazione di recente avviati dal Garante con l'UPI (Unione delle Province d'Italia), l'ANCI (Associazione Nazionale dei Comuni Italiani) e l'UNCEM (Unione Nazionale Comuni Comunità Enti Montani) hanno portato all'elaborazione di **schemi tipo di regolamento** per il trattamento dei dati sensibili e giudiziari. Gli schemi di regolamento di province, comuni e comunità montane sono stati recentemente approvati dall'Autorità rispettivamente con i pareri favorevoli del 7 settembre, 21 settembre e 19 ottobre 2005[34] e costituiranno, pertanto, il modello al quale province, comuni e comunità montane dovranno conformarsi senza la necessità di ottenere un autonomo parere favorevole del Garante. I soggetti pubblici dovranno richiedere al Garante un parere specifico, solo se apporteranno modifiche sostanziali o integrazioni non formali riguardanti il trattamento di dati personali oppure lo svolgimento di operazioni non considerate nello schema tipo.

---

[32] I "dati giudiziari" sono definiti dal Codice Privacy all'art. 4, comma 1, lett. e) come *"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"*.

[33] Decreto Legislativo n. 196/2003, art. 21 *(Principi applicabili al trattamento di dati giudiziari)*: *"1. 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.*

2. Le disposizioni di cui all'art. 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari".

[34] Garante per la protezione dei dati personali, Parere sullo schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari delle province - 7 settembre 2005; Parere sullo schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari dei comuni - 21 settembre 2005; Parere sullo schema tipo di regolamento per il trattamento dei dati sensibili e giudiziari delle comunità montane - 19 ottobre 2005. (Cfr. sull'approvazione dello schema di regolamento per le comunità montane anche la Newsletter del Garante n. 265 del 28 ottobre 2005, "Garanzie per i dati nelle Comunità montane").

Gli schemi tipo suddetti contengono una delibera standard, l'indice dei trattamenti (15 per le province, 35 per i comuni e 19 per le comunità montane) e una scheda per ogni trattamento. Ogni scheda, a sua volta, è articolata in una serie di riquadri di dettaglio che evidenziano la denominazione del trattamento dati, la fonte normativa, le finalità di rilevante interesse pubblico, i tipi di dati trattati, l'iter procedurale seguito per l'archiviazione dei dati stessi. La scheda contiene anche una sintetica descrizione relativa al trattamento effettuato e al flusso informativo.

■ TITOLARE, RESPONSABILE E INCARICATI NELLA PUBBLICA AMMINISTRAZIONE

Per quanto riguarda la figura del **Titolare** del trattamento, secondo l'interpretazione sostenuta dal Garante, nella P.A. Titolare è l'Ente nel suo complesso. Quanto al **Responsabile**, invece, deve essere identificato nel dirigente o comunque nel soggetto che occupa posizioni organizzative, e che riceve istruzioni in materia da parte di chi rappresenta l'Amministrazione.

Alcune novità previste dal Codice Privacy riguardano, invece, la figura degli **Incaricati** al trattamento dei dati: questi, infatti, possono essere soltanto persone fisiche e non persone giuridiche e possono essere designati anche "per relationem" mediante *"la documentata preposizione della persona fisica ad un'unità per la quale è individuato per iscritto l'ambito del trattamento consentito agli addetti all'unità medesima"*[35].

Si rileva, inoltre, che il nuovo Codice non contiene specifiche previsioni rispetto ai soggetti che, pur estranei alla struttura organizzativa dell'Ente svolgano per conto della P.A. attività di trattamento di dati personali. Si pensi, ad esempio, ai commissari di concorso esterni o ai collaboratori esterni dei sistemi informatici. Nei confronti di tali soggetti si ritiene necessario procedere ad una specifica e formale designazione a responsabile o ad incaricato per conto dell'ente, in modo da evitare paradossali complicazioni nello svolgimento delle attività, quali ad esempio la necessità di richiedere preventivamente il consenso al trattamento dei dati[36].

4. LA VIDEOSORVEGLIANZA NEGLI ENTI PUBBLICI

Da alcuni anni molti enti pubblici ricorrono massicciamente all'uso di impianti di videosorveglianza per molteplici scopi, quali ad esempio il monitoraggio del traffico veicolare, la sicurezza pubblica e la prevenzione di atti di vandalismo.

Con il **provvedimento a carattere generale del 29 aprile 2004** il Garante ha stabilito quando i sistemi di videosorveglianza possono essere legittimamente attivati, con quali modalità e con quali misure di sicurezza per il cittadino che, più o meno consapevolmente viene monitorato.

---

[35] Decreto Legislativo n. 196/2003, art. 30 *(Incaricati del trattamento)*, comma 2°: *"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"*.

[36] L. De Zotti, *Il Codice Privacy negli enti locali*, articolo pubblicato sul sito www.commercialistatelematico.com, in collaborazione con V. Frediani.

Nel provvedimento generale sopra citato, il Garante individua una serie di principi ai quali l'attività di videosorveglianza, sebbene effettuata per la cura di un interesse pubblico, deve attenersi. In particolare:

- Un soggetto pubblico può effettuare attività di videosorveglianza solo ed esclusivamente per svolgere le proprie **funzioni istituzionali**, che deve individuare ed esplicitare con chiarezza e di cui sia realmente titolare in base all'ordinamento di riferimento. Altrimenti, il trattamento dei dati non è da ritenersi lecito, anche nel caso in cui l'ente designa esponenti delle forze dell'ordine come responsabili del trattamento o utilizza un collegamento telematico in violazione di quanto stabilito dall'art. 19, comma 2[37], del Codice Privacy.

  Alla luce di tale principio, non è stata ritenuta lecita l'installazione, da parte di alcuni enti locali, di sistemi di videosorveglianza allo scopo di perseguire direttamente, in via amministrativa, finalità di prevenzione e accertamento dei reati, che invece rientrano nell'ambito di competenza delle autorità giudiziarie e delle forze di polizia[38].

- Deve sussistere un'**effettiva e proporzionata esigenza di prevenzione o repressione di pericoli concreti e specifici** di lesione di un bene (circostanza che, ad esempio, si potrebbe verificare in caso di manifestazioni che siano ragionevolmente fonte di eventi pregiudizievoli).

  Sulla base di tale principio, il Garante ha sottolineato l'illiceità della costante ed integrale ripresa capillare di intere aree cittadine "cablate", senza che ve ne sia la reale esigenza, oppure il collegamento telematico tra più soggetti al fine di registrare un numero elevato di dati personali e ricostruire interi percorsi effettuati in un determinato arco di tempo. E' stata, inoltre, evidenziata l'illiceità dell'attività di videosorveglianza effettuata al solo scopo 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 di deposito dei sacchetti di immondizia negli appositi contenitori.

- Deve essere sempre fornita l'**informativa** agli interessati, oltre che mediante pubblicazione nell'albo dell'ente o attraverso una temporanea affissione di manifesti, in tutti i punti e le aree in cui viene effettuata l'attività di videosorveglianza.

- La **rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato** può avvenire unicamente dietro rilascio di autorizzazione amministrativa al Comune e la rilevazione delle immagini deve essere limitata soltanto ai casi di infrazione[39]. I dati

[37] Decreto Legislativo n. 196/2003, art. 19 *(Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari)*, comma 2°: 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"*.

[38] Provvedimento generale sulla videosorveglianza, 29 aprile 2004, Garante per la protezione dei dati personali, pp. 19-20.

[39] Secondo quanto stabilito dal Garante nel citato provvedimento generale sulla videosorveglianza, i Comuni sono tenuti a rispettare il dettato del D.P.R. 22 giugno 1999, n. 250.

trattati, inoltre, possono essere conservati solo per il periodo necessario alla contestazione delle infrazioni e alla definizione del relativo contenzioso e l'accesso ad essi è consentito esclusivamente per fini di polizia giudiziaria o di indagine penale.

- Quanto alla tematica **della sicurezza nel trasporto urbano**, dal provvedimento generale del Garante si evince la liceità dell'installazione di sistemi di videosorveglianza su mezzi di trasporto e presso alcune fermate di mezzi urbani, in considerazione dei frequenti rischi di aggressioni e borseggi, soprattutto nelle aree periferiche. Si ritiene, tuttavia, opportuno osservare particolare cura in relazione all'angolo visuale delle apparecchiature di ripresa ed alla collocazione di idonee informative a bordo dei veicoli pubblici e nelle aree di fermata.

- Il **controllo video di aree abusivamente impiegate come discariche di materiali e sostanze pericolose** è ritenuto lecito soltanto qualora risultino inefficaci o inattuabili altre misure. Qualora, invece, l'attività di controllo sia volta unicamente ad accertare eventuali violazioni amministrative delle disposizioni relative a modalità e orario di deposito dei rifiuti urbani, è opportuno che venga effettuata attraverso forme differenti[40].

- L'attività di videosorveglianza all'interno dei **luoghi di sepoltura** è consentita unicamente se effettuata al fine di tutelare tali aree dal concreto rischio di atti vandalici[41].

5. LA TUTELA RISARCITORIA

In considerazione dei rischi che l'interessato può correre per effetto del trattamento dei suoi dati personali, il legislatore ha previsto a suo favore una specifica tutela risarcitoria per i danni provocati nell'attività di elaborazione dei dati: infatti, **chiunque cagioni un danno ad altri a causa di un trattamento, è tenuto al risarcimento ai sensi dell'art. 2050 cod. civ.**[42] [43]. Il trattamento dei dati viene, pertanto, considerato "attività pericolosa" e l'onere della prova di aver posto in essere ogni misura idonea ad evitare il danno è a carico del Titolare. Occorre altresì precisare che l'aver fornito preventivamente l'informativa all'interessato o l'aver acquisito, ove previsto, il suo consenso non è sufficiente ad escludere la responsabilità del danneggiante. Quest'ultimo, infatti, dovrà dimostrare di aver adoperato ogni accorgimento tale da escludere il nesso di causalità tra

[40] Provvedimento generale sulla videosorveglianza, 29 aprile 2004, Garante per la protezione dei dati personali, p. 22.

[41] Provvedimento generale sulla videosorveglianza, 29 aprile 2004, Garante per la protezione dei dati personali, p. 19. Cfr. inoltre sull'argomento la recente Newsletter del 22 novembre 2004, *Familiari spiati nelle camere ardenti. Interviene il Garante*. Nell'ambito degli accertamenti effettuati per verificare il rispetto delle regole in materia di videosorveglianza, è stato rilevato che gli uffici di un Comune toscano avevano dotato di telecamere a circuito chiuso l'edificio all'interno del quale vengono allestite camere ardenti per la veglia dei defunti omettendo, tra l'altro di segnalarne la presenza ai cittadini mediante adeguate informative.

[42] Decreto Legislativo n. 196/2003, art. 15 *(Danni cagionati per effetto del trattamento)*, comma 1°: *"1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile"*.

[43] Art. 2050, cod. civ. *(Responsabilità per l'esercizio di attività pericolose)*: *"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 avere adottato tutte le misure idonee a evitare il danno"*.

l'attività di trattamento dei dati e l'evento[44]. Si evidenzia, inoltre, che la tutela risarcitoria prevista dal legislatore, oltre ad esonerare l'interessato dall'onere probatorio in merito ai danni subiti, gli consente di richiedere anche il risarcimento del danno **non patrimoniale**[45].

Quanto ai **soggetti tenuti al risarcimento**, sebbene il Codice non li abbia chiaramente individuati, si ritiene che le forme di responsabilità previste siano più facilmente riconducibili alle figure del Titolare e del Responsabile del trattamento, in ragione dell'attribuzione ad essi della facoltà di decidere in merito alle fasi del trattamento o alle operazioni che hanno causato o permesso la realizzazione del danno[46].

L'applicabilità della suddetta forma di tutela alle attività svolte dalla Pubblica Amministrazione veniva inizialmente negata, in quanto la norma veniva ricondotta unicamente al perseguimento di fini utilitaristici, ritenuti estranei all'attività statale. Successivamente, la dottrina ne ha esteso l'applicabilità soltanto agli enti pubblici economici e agli organi imprese, in ragione dell'elemento imprenditoriale che caratterizza tali strutture. Di recente, tuttavia, in considerazione delle numerose previsioni normative che impongono alla Pubblica Amministrazione di perseguire criteri di efficienza ed economicità, l'art. 15 del Codice è stato ritenuto applicabile anche alle attività pericolose poste in essere dai soggetti pubblici[47].

6. LA TUTELA PENALE

Le fattispecie criminose previste dal Codice Privacy si configurano per lo più come reati propri, in quanto non realizzabili da chiunque, ma soltanto da coloro che rivestono particolari qualifiche giuridiche e naturalistiche; sono previsti, in particolare, **tre delitti e due contravvenzioni**:

- **TRATTAMENTO ILLECITO DI DATI**: tale delitto si integra nei casi di trattamento di dati personali in violazione degli artt. 18, 19, 23, 123, 126 e 130, o in applicazione dell'art. 129, **se dal fatto deriva nocumento**. E' fatta salva l'ipotesi in cui il fatto costituisca più grave reato[48]. Il nocumento può essere riferito sia alla persona del soggetto cui i dati

[44] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, pp. 83-85.

[45] Decreto Legislativo n. 196/2003, art. 15 *(Danni cagionati per effetto del trattamento)*, comma 2°: *"2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 11".*

[46] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, pp. 87-88.

[47] R. Galli, *Corso di diritto amministrativo*, Padova, Cedam, 1996, pp. 852.854.

[48] Decreto Legislativo n. 196/2003, art. 167 *(Trattamento illecito di dati)*: *"1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per al-tri profitto o di recare ad altri un danno, procede al trattamento di dati personali in vio-lazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, 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.*

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per al-tri profitto o di recare ad altri un danno, procede al trattamento di dati personali in vio-lazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni".

si riferiscono, che al suo patrimonio in termini di perdita patrimoniale o di mancato guadagno derivante dalla circolazione non autorizzata di informazioni personali[49].

- **Pena applicabile**: **reclusione** fino a tre anni.

- **FALSITÀ NELLE DICHIARAZIONI E NOTIFICAZIONI AL GARANTE**: ci si trova in presenza di tale figura delittuosa quando, nella notificazione o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi all'Autorità o nel corso di accertamenti, si dichiarino o attestino falsamente notizie o circostanze o si producano documenti falsi[50]. La fattispecie in esame è volta a salvaguardare e rafforzare la funzione del Garante e ad evitare di fuorviarne le determinazioni sulla base di presupposti erronei[51].

  - **Pena applicabile: reclusione** fino a tre anni.

- **INOSSERVANZA DI PROVVEDIMENTI DEL GARANTE**: la fattispecie delittuosa si riferisce all'inosservanza dei provvedimenti adottati dal Garante ai sensi degli artt. 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lett. c)[52]. La condotta tipica si realizza attraverso modalità differenti a seconda del contenuto del provvedimento violato.

  - **Pena applicabile**: **reclusione** fino a due anni.

- **OMESSA ADOZIONE DELLE MISURE DI SICUREZZA**: trattasi di una contravvenzione, consistente nella omessa adozione, da parte di chiunque vi sia tenuto, delle misure minime di sicurezza volte ad evitare il rischio di distruzione o perdita anche accidentale dei dati, di accesso non autorizzato, di trattamento non consentito o non conforme alle modalità di raccolta. Si evidenzia che, per la contravvenzione suddetta, è prevista una speciale causa di estinzione del reato, consistente nell'adozione, nel termine stabilito, delle prescrizioni tecniche idonee e nel pagamento di una somma pari al quarto del massimo dell'ammenda stabilita[53].

---

[49] R. Acciai e S. Melchionna, in R. Acciai (cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, pp.354-355.

[50] Decreto Legislativo n. 196/2003, art. 168 *(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 accer-tamenti, 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"*.

[51] R. Acciai e S. Melchionna, in R. Acciai (a cura di), Il diritto alla protezione dei dati personali, Maggioli Editore, 2003, pp. 355-356.

[52] Decreto Legislativo n. 196/2003, art. 170 *(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"*.

[53] Decreto Legislativo n. 196/2003, art. 169 *(Misure di sicurezza)*: *"1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.*

- **Pena applicabile**: **arresto** fino a due anni o **ammenda** fino a Euro 50.000.

- **ALTRE FATTISPECIE**: la norma fa riferimento alla violazione delle norme in materia di annunci di lavoro e dati riguardanti i prestatori di lavoro, ed inoltre in materia di divieto di controllo a distanza e di telelavoro[54].

  - **Pena applicabile**: ai sensi dell'art. 38 della legge n. 300/1970, **arresto** fino a un anno e **ammenda** fino a Euro 1.549,37 (Lire 3.000.000).

7. GLI ILLECITI AMMINISTRATIVI

Le sanzioni amministrative previste dal Codice Privacy sono applicabili alle seguenti condotte illecite:

- **OMESSA O INIDONEA INFORMATIVA ALL'INTERESSATO**, nel caso di violazione delle disposizioni di cui all'art. 13 (art. 161).

  - **Pena applicabile**: **sanzione amministrativa** consistente nel pagamento di una somma da Euro 3.000 fino a Euro 30.000. La somma può essere aumentata fino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

- **CESSIONE DI DATI IN VIOLAZIONE DI QUANTO PREVISTO DALL'ART. 16, COMMA 1, LETT. B)**, o di altre disposizioni concernenti il trattamento dei dati personali (art. 162, comma 1).

  - **Pena applicabile**: **sanzione amministrativa** consistente nel pagamento di una somma da Euro 5.000 a Euro 30.000.

- **VIOLAZIONE DELLA DISPOSIZIONE DI CUI ALL'ART. 84, COMMA 1**, concernente la comunicazione dei dati idonei a rivelare lo stato di salute relativamente ai trattamenti effettuati in ambito sanitario (art. 162, comma 2).

  - **Pena applicabile**: **sanzione amministrativa** consistente nel pagamento di una somma da Euro 500 a Euro 3.000.

---

2. 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".

[54] Decreto Legislativo n. 196/2003, art. 171 *(Altre fattispecie)*: *"La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300".*

- **OMESSA, TARDIVA O INCOMPLETA NOTIFICAZIONE**, nel caso in cui non si provveda tempestivamente, ove previsto, alla notificazione di cui agli artt. 37 e 38 o si indichino in essa notizie incomplete (art. 163).

  - **Pena applicabile**: **sanzione amministrativa** consistente nel pagamento di una somma da Euro 10.000 a Euro 60.000, oltre alla **sanzione amministrativa accessoria** della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto in uno o più giornali indicati nel provvedimento che la applica.

- **OMESSA INFORMAZIONE O ESIBIZIONE DI DOCUMENTI RICHIESTI DAL GARANTE** (art. 164).

  - **Pena applicabile**: **sanzione amministrativa** consistente nel pagamento di una somma da Euro 4.000 a Euro 24.000.

Occorre, infine, rilevare che, ai sensi dell'art. 165 del Codice, nei casi di cui agli articoli 161, 162 e 164, può essere applicata la **sanzione amministrativa accessoria** della **pubblicazione dell'ordinanza-ingiunzione**, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica. La suddetta previsione non riguarda, tuttavia, la fattispecie dell'omessa o incompleta notificazione (art. 163), ove la sanzione accessoria è già prevista come obbligatoria.