RELAZIONE PER L'ANNO 2005

Diritto alla protezione dei dati personali: garanzie per i cittadini e sicurezza dei sistemi

PAGINA BIANCA

I. STATO DI ATTUAZIONE DEL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

1. Il quadro normativo

II. L'ATTIVITÀ SVOLTA DAL GARANTE

2. Trattamenti effettuati in ambito pubblico

3. Sanità

4. Dati genetici

5. Ricerca statistica e scientifica

6. Attività di polizia

Unione europea

57. Miglioramento della cooperazione di polizia, con particolare riferimento ai confini interni (modifica della Convenzione di applicazione Schengen)
58. Decisione sull'istituzione del Sistema informativo Schengen di seconda generazione (Sis II)
59. Regolamento sull'istituzione del Sistema informativo Schengen di seconda generazione (Sis II)
60. Accesso al Sistema informativo Schengen di seconda generazione (Sis II) per l'emissione delle carte di circolazione dei veicoli
61. Protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale
62. Scambio di informazioni in virtù del principio di disponibilità
63. Formato uniforme per i permessi di soggiorno dei cittadini di Paesi terzi

Consiglio dell'Unione europea

64. Requisiti minimi comuni di sicurezza per le carte di identità nazionali
65. Convenzione di Prüm sulla lotta al terrorismo, al crimine transfrontaliero e all'immigrazione clandestina

Gruppo art. 29

66. Livello di protezione garantito in Canada ai fini della trasmissione, da parte delle compagnie aeree, dei dati sui viaggiatori
67. Questioni di protezione dati relative ai diritti di proprietà intellettuale
68. Protezione dati e tecnologie *Rfid*
69. Notificazione dei trattamenti di dati e ruolo dei *privacy officer*
70. Trasferimento all'estero di dati e "regole vincolanti nell'impresa"
71. Modello di richiesta ai fini dell'approvazione di "regole vincolanti nell'impresa"
72. Sistema di informazione visti (Vis) e scambio di dati sui visti per soggiorni di breve durata
73. Caratteristiche di sicurezza ed elementi biometrici nei passaporti e nei documenti di viaggio
74. Conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica
75. Trasferimento all'estero dei dati e adeguatezza: linee di interpretazione armonizzata
76. Uso di dati relativi all'ubicazione al fine di fornire servizi a valore aggiunto
77. Istituzione del Sis II e accesso per il rilascio delle carte di circolazione
78. Linee guida per i *terminated merchant database*
79. Rapporto annuale per il 2004

Elenco delle abbreviazioni

La presente Relazione è riferita al 2005 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 15 giugno 2005, relative a sviluppi che si è ritenuto opportuno menzionare.

ad es.	ad esempio
art.	articolo
Bollettino	Bollettino del Garante per la protezione dei dati personali "Cittadini e Società dell'Informazione"
c.c.	codice civile
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cd.	cosiddetto/a
cfr.	confronta
Cost.	Costituzione
d.l.	decreto legge
d.lg.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.G.p.	decreto del Presidente della Giunta provinciale
d.P.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
P.a.	Pubblica amministrazione
par.	paragrafo
Provv.	provvedimento
Relazione	Relazione del Garante per la protezione dei dati personali
r.d.	regio decreto
reg.	regolamento
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

PAGINA BIANCA

I - Stato di attuazione del Codice in materia di protezione dei dati personali

1 Il quadro normativo

1.1. *Il Codice e la "stabilizzazione" delle regole per la protezione dei dati*

Nella *Relazione* del Garante per l'anno 2004 si è già ampiamente evidenziato come il Codice in materia di protezione dei dati personali entrato in vigore il 1° gennaio di tale anno (d.lg. 30 giugno 2003, n. 196) abbia consolidato il quadro di rafforzate garanzie per i diritti fondamentali della persona che sono state introdotte negli anni scorsi rispetto al trattamento dei dati personali. In particolare, si è richiamata l'attenzione sull'importante e solenne riconoscimento del diritto alla protezione dei dati personali, affermato già nell'art. 1 del Codice, diritto già contemplato nella Carta dei diritti fondamentali dell'Unione europea e nel Trattato per la Costituzione europea.

Nella stessa *Relazione* (p. 3) si erano tuttavia posti in luce alcuni interventi modificativi del Codice che erano stati avviati nel 2004 in alcuni settori di rilievo, da analizzare con cura stante l'esigenza di evitare possibili passi in parziale controtendenza rispetto al processo di consolidamento e di "stabilizzazione" delle garanzie dei cittadini che nel Codice aveva trovato ampia esplicazione. In questa prospettiva ci si era riferiti, in particolare, alle modifiche normative sulla conservazione dei dati del traffico telefonico e all'ambito sanitario (d.l. 24 dicembre 2003, n. 354, convertito dalla l. 26 febbraio 2004, n. 45; d.l. 29 marzo 2004, n. 81, convertito dalla l. 26 maggio 2004, n. 138), nonché alle diverse proroghe dei termini per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili delle pubbliche amministrazioni.

Analoghi interventi normativi si sono registrati anche nel corso del 2005, interventi dei quali viene effettuata di seguito una sintesi.

1.2. *Le modifiche apportate*

Specifico rilievo hanno assunto, anzitutto, le ulteriori modifiche apportate al Codice (art. 132) e ad alcune disposizioni ad esso collegate, relativamente alla disciplina della conservazione dei dati di traffico telefonico e telematico per finalità di accertamento e di repressione dei reati (d.l. 27 luglio 2005, n. 144, convertito, con modificazioni, dalla l. 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale: art. 6).

Dati di traffico

Le modifiche introdotte hanno riguardato, in particolare, la tipologia dei dati personali oggetto di necessaria conservazione, la durata di tale conservazione e le modalità di acquisizione, accesso ed utilizzazione dei dati medesimi. In questo quadro:

a) la conservazione dei dati di traffico telefonico per finalità di accertamento e repressione dei reati è stata estesa ai dati concernenti le "chiamate senza risposta";

b) è stato introdotto l'obbligo per i fornitori di servizi di comunicazione elettronica di conservare anche i dati relativi al "traffico telematico", esclusi i contenuti delle comunicazioni, per un periodo di sei mesi, nonché per ulteriori sei mesi per esclusive finalità di accertamento e repressione di delitti di particolare gravità (indicati all'art. 407, comma 2, lett. a), c.p.p. o commessi in danno di sistemi informatici o telematici) (art. 132, commi 1 e 2, del Codice, come modificato dall'art. 6, comma 2, d.l. n. 144/2005);

c) è stata sospesa fino al 31 dicembre 2007 l'applicazione di tutte le disposizioni normative o amministrative che prescrivano o consentano la cancellazione dei dati del traffico telefonico o telematico; questi debbono essere quindi conservati fino alla medesima data del 31 dicembre 2007 limitatamente, per quanto riguarda i dati di traffico telematico, alle "informazioni che consentono la tracciabilità degli accessi, nonché qualora disponibili, dei servizi", rimanendo del pari esclusa la conservazione dei contenuti delle conversazioni (art. 6, comma 1, d.l. n. 144/2005).

Il d.l. n. 144/2005 ha previsto, altresì, che le modalità e i tempi di attuazione delle predette modifiche all'art. 132 del Codice siano individuati con regolamento governativo, adottato previo parere del Garante (art. 6, comma 4, d.l. n. 144/2005). A tale regolamento si aggiunge –e, per certi versi, potrebbe in parte "sovrapporsi"– il provvedimento che l'Autorità dovrà adottare, in base al medesimo articolo 132 del Codice, per disciplinare le modalità di trattamento presso i fornitori e di accesso ai dati conservati per le finalità accertamento e repressione dei reati, nonché per individuare ulteriori e più incisive misure di sicurezza necessarie a garantire maggiormente che la conservazione di tale categoria delicata di dati sia effettuata nel pieno rispetto dei diritti fondamentali della persona.

La piena attuazione di tali modalità e misure protettive si è affiancata al dibattito relativo all'ampliamento dei tempi di conservazione e delle categorie di dati da conservare anche relativamente alle comunicazioni telematiche. Sebbene le modifiche apportate abbiano in parte un'efficacia temporale limitata, resta sul tappeto il rapporto tra la predetta conservazione e il principio relativo alle finalità per le quali i dati sono o dovrebbero essere trattati dai fornitori, nonché il tema della proporzionalità rispetto alle finalità di polizia e di giustizia da perseguire. In materia dovranno essere peraltro effettuate a breve nuove valutazioni di carattere anche normativo, per effetto del prossimo recepimento della direttiva 2006/24/Ce del Parlamento e dal Consiglio dell'Unione europea approvata il 15 marzo 2006 sempre in tema di *data retention*, direttiva la quale prevede un periodo di conservazione dei dati (compreso fra i sei mesi e i due anni) che, oltre ad essere più breve rispetto a quello attualmente previsto in Italia, è stato oggetto di rilievi critici nel parere espresso preventivamente dalle autorità europee per la protezione dei dati personali (parere elaborato da un sottogruppo che è stato coordinato dall'Autorità italiana: parere del Gruppo art. 29 WP 113, 21 ottobre 2005).

Esercizi di telefonia ed Internet point

Il d.l. n. 144/2005 ha introdotto altre disposizioni di rilievo per la protezione dei dati personali.

Per finalità di lotta al terrorismo, sono stati ad esempio previsti, nei confronti

di titolari e gestori di esercizi pubblici di telefonia e Internet, alcuni obblighi orientati ad un maggiore controllo delle comunicazioni effettuate con strumenti telematici o telefonici, come l'identificazione del cliente, il monitoraggio delle operazioni dell'utente e l'archiviazione dei relativi dati (art. 7 d.l. n. 144/2005). In relazione a tali obblighi, il Ministero dell'interno, sentito il Garante, ha poi adottato il previsto decreto di attuazione recante la disciplina delle misure che il gestore è tenuto ad osservare, nonché delle modalità di trattamento dei dati (*v.* anche par. 21.2).

Dna dell'indagato e banca di dati

A parziale modifica dell'art. 349 c.p.p., sono stati previsti, con il d.l. n. 144/2005, nuovi poteri per la polizia giudiziaria al fine di identificare la persona nei cui confronti vengono svolte indagini, prevedendo che si possa procedere, previa autorizzazione del pubblico ministero, al prelievo coattivo di capelli o saliva anche senza il consenso dell'interessato. Nel corso dei lavori di conversione del decreto, il Governo ha accettato un ordine del giorno parlamentare che lo impegna ad istituire una banca dati nella quale raccogliere i dati relativi al Dna acquisiti ai sensi del predetto art. 349 c.p.p., ovvero attraverso altri accertamenti effettuati da reparti di polizia scientifica. Secondo l'o.d.g., tale banca dati dovrebbe operare sotto la vigilanza del Garante, il quale potrebbe fissare limiti e condizioni alla consultazione dei dati relativi a soggetti per i quali non sia già intervenuta una sentenza di condanna. Appare evidente che si tratta di una tematica particolarmente delicata in relazione alla quale ogni iniziativa richiederà un'attenta valutazione delle diverse implicazioni che, anche sul piano costituzionale, potrebbero derivarne per i diritti fondamentali della persona e, in particolare, per la riservatezza e la dignità degli interessati.

Adozione delle misure minime di sicurezza

Le altre modifiche apportate al Codice hanno riguardato la reiterazione di proroghe, già disposte nel corso del 2004, con le quali erano stati differiti i termini per adempiere a pur importanti obblighi posti a garanzia dell'interessato, in relazione all'applicazione delle "nuove" misure minime di sicurezza e all'adozione dei regolamenti in materia di dati sensibili e giudiziari da parte dei soggetti pubblici.

Per quanto riguarda le misure minime di sicurezza, la scadenza originariamente fissata al 30 giugno 2004 (art. 180, comma 1, del Codice), era stata prorogata due volte già nel corso del 2004, inizialmente al 31 dicembre 2004 (d.l. 24 giugno 2004, n. 158, convertito, con modificazioni, dalla l. 27 luglio 2004, n. 188) e, quindi, al 30 giugno 2005 (d.l. 9 novembre 2004, n. 266, convertito, con modificazioni, dalla l. 27 dicembre 2004, n. 306). Con successivi interventi adottati sempre in via d'urgenza nel 2005, il termine è stato ulteriormente prorogato, una prima volta al 31 dicembre 2005 (d.l. 30 dicembre 2004, n. 314, convertito, con modificazioni, dalla l. 1° marzo 2005, n. 26) e, da ultimo, al 31 marzo 2006 (d.l. 30 dicembre 2005, n. 273, convertito, con modificazioni, dalla l. 23 febbraio 2006, n. 51). Analogamente, è stato prorogato anche il termine per adottare le misure di sicurezza da parte dei soggetti che, alla data di entrata in vigore del Codice, disponevano di strumenti elettronici "obsoleti": prima al 31 marzo 2005, poi al 30 settembre 2005, quindi al 31 marzo 2006 e, da ultimo, al 30 giugno 2006 (d.l. n. 273/2005 cit.).

Adozione dei regolamenti sul trattamento dei dati sensibili e giudiziari

Il già citato d.l. n. 158/2004 aveva, inoltre, prorogato al 31 dicembre 2005 il termine per l'adozione e pubblicazione, da parte delle pubbliche amministrazioni, dei regolamenti in materia di dati sensibili e giudiziari, originariamente fissato dal Codice alla data del 31 dicembre 2004 (art. 181, comma 1, lett. *a*)). La citata l. 23 febbraio 2006, n. 51, di conversione del d.l. n. 273/2005, ha poi prorogato ulteriormente il termine in questione al 15 maggio 2006 (da ultimo prorogato ancora al 31 luglio 2006 con d.l. 12 maggio 2006, n. 173).

1.3. *Il monitoraggio delle leggi regionali*

Nel quadro normativo di riferimento dell'attività di monitoraggio sugli atti delle regioni e degli enti locali, si deve evidenziare il testo di legge costituzionale recante modifiche alla Parte II della Costituzione approvato dal Parlamento, pubblicato sulla *Gazzetta Ufficiale* 18 novembre 2005, n. 269, e sottoposto a *referendum* confermativo ai sensi dell'art. 138 Cost. (*v.* anche par. 1.3). Per quanto attiene ai rapporti tra Stato e regioni (capo V del testo, artt. 37-50), non vi sono particolari innovazioni rispetto a quanto statuito dalla Corte costituzionale con l'importante sentenza n. 271/2005 (sulla quale v. anche par. 21.3), circa la titolarità esclusiva dello Stato a legiferare in materia della protezione di dati personali in quanto "*essenzialmente riferibile, all'interno delle materie legislative di cui all'art. 117 Cost., alla categoria dell'ordinamento civile*".

La pronuncia della Corte è intervenuta su una questione complessa e dibattuta anche in sede parlamentare successivamente alla modifica del titolo V della Costituzione. La materia in esame, ha affermato la Corte, rientra tra le situazioni nella titolarità esclusiva del potere legislativo da parte dello Stato. L'adozione da parte delle regioni, nell'esercizio della loro potestà legislativa esclusiva o concorrente, di norme attinenti direttamente alla protezione dei dati personali, se può apparire giustificata e legittimata dalla natura "trasversale" della normativa sulla *privacy* e in ragione del suo vasto e articolato ambito di applicazione, deve tuttavia limitarsi a meglio specificare i principi o le norme generali già contenuti nella legislazione statale.

Su questi presupposti, anche nel 2005 l'Autorità ha proseguito l'attività di monitoraggio svolta anche in passato con finalità essenzialmente conoscitive e di ricognizione di nodi problematici, imperniata anche sulla verifica della conformità degli atti normativi e regolamentari delle regioni alla normativa statale sulla protezione dei dati personali.

I profili tematici e problematici emersi dall'esame dei numerosi testi normativi effettuato nel 2005 sono, in gran parte, sostanzialmente analoghi a quelli già evidenziati nella *Relazione* 2004; particolare attenzione è stata rivolta all'applicazione del principio di pertinenza e non eccedenza, specialmente per quanto riguarda il trattamento di dati sensibili da parte di soggetti pubblici.

Per assicurare il rispetto della ripartizione costituzionale di competenze, si è tra gli altri criteri utilizzato frequentemente, nei casi dubbi, quello proposto anche in dottrina, consistente nel verificare se le norme regionali definiscano le posizioni soggettive e i rapporti giuridici dei soggetti coinvolti in termini diversi rispetto a quelli stabiliti dal legislatore nazionale, attribuendosi in tal caso alle stesse una valenza privatistica che le ascriverebbe alla materia dell'ordinamento civile, sottratta quindi alla competenza regionale.

In questo quadro è emersa, come rilevato dal presidente del Garante nel corso di un'audizione svoltasi il 26 maggio 2005 presso la Commissione affari costituzionali del Senato della Repubblica, l'opportunità di prevedere e, comunque, di realizzare adeguate modalità di raccordo e scambio di valutazioni anche fra il Garante e le regioni; meritano una citazione, come momento di raccordo, le collaborazioni informali con gli organismi rappresentativi delle autonomie locali e territoriali in vista del parere sullo schema tipo di regolamento sul trattamento dei dati sensibili e giudiziari, di cui più dettagliatamente si riferisce in altra parte di questa *Relazione* (*v.* par. 2.2.1).

1.4. *Altre novità normative con riflessi in materia di protezione di dati personali*

Nel corso dell'anno sono stati approvati altri provvedimenti normativi riguardanti la materia del trattamento dei dati personali e l'attività del Garante.

In proposito, vanno ricordati, in particolare:

Costituzione

a) la predetta legge costituzionale di modifica della Parte II della Costituzione, che menziona espressamente le autorità indipendenti nella Carta costituzionale. Il nuovo art. 98-*bis* Cost. prevede infatti che, per lo svolgimento di attività di garanzia o di vigilanza in materia di diritti di libertà garantiti dalla Costituzione e su materie di competenza dello Stato, si possano istituire con legge apposite autorità indipendenti, stabilendone la durata del mandato, i requisiti di eleggibilità e le condizioni di indipendenza. Le autorità riferiscono alle Camere sui risultati delle attività svolte. La legge costituzionale, approvata a maggioranza assoluta, ma inferiore ai due terzi dei componenti di ciascuna Camera, e pubblicata nella *G.U.* 18 novembre 2005, n. 269, è come è noto in procinto di essere sottoposta a *referendum* popolare confermativo ai sensi dell'art. 138 Cost.;

"Dematerializzazione" della corrispondenza nella pubblica amministrazione

b) la l. 23 dicembre 2005, n 266 (legge finanziaria per il 2006), la quale reca una delicata previsione che consente una "dematerializzazione" della corrispondenza delle pubbliche amministrazioni (art. 1, comma 51). La disposizione mira a collocarsi nel solco del processo di informatizzazione della pubblica amministrazione e, in particolare, dell'automatizzazione delle procedure, mediante la formazione dei documenti in formato elettronico, il trasferimento su supporto digitale della documentazione cartacea, l'utilizzo del protocollo informatico e dei sistemi di classificazione e di fascicolazione elettronica. Peraltro, il "Codice dell'amministrazione digitale" contiene già una norma sulla dematerializzazione dei documenti delle pubbliche amministrazioni, in base alla quale le amministrazioni sono tenute a valutare in termini di rapporto costi-benefici il recupero su supporto informatico dei documenti cartacei dei quali sia necessaria o opportuna la conservazione, predisponendo i conseguenti piani di sostituzione degli archivi cartacei con archivi informatici (art. 42 d.lg. n. 82/2005). La disposizione contenuta nella legge finanziaria sembra andare oltre tale previsione, consentendo alle pubbliche amministrazioni anche di stipulare convenzioni con soggetti pubblici o privati per il trasferimento su supporto informatico degli invii di corrispondenza da e per gli uffici pubblici, ed individuando nel concessionario del servizio pubblico universale un soggetto abilitato a tale dematerializzazione. La norma richiede altresì che le pubbliche amministrazioni si avvalgano, in ogni caso, di servizi informatici e telematici che assicurino l'integrità del messaggio nella fase di trasmissione informatica, attraverso la certificazione tramite firma digitale o altri strumenti che garantiscano l'integrità legale del contenuto, la marca temporale e l'identità dell'ente certificatore che presidia il processo. Il concessionario del servizio postale viene obbligato, poi, ad individuare i dirigenti preposti alla certificazione di conformità del documento informatico riproduttivo del documento originale cartaceo. È di tutta evidenza la particolare delicatezza di questi processi, che richiedono approfondite valutazioni per contemperare le esigenze di potenziamento dell'efficienza delle P.a. con una rigorosa serie di cautele volte a prevenire la dispersione o l'utilizzo di dati per finalità non consentite o comunque indebito, considerato anche l'incisivo ruolo previsto per soggetti esterni alla P.a.;

Tecniche di comunicazione a distanza

c) il d.l. 30 dicembre 2005, n. 273 (cui si è fatto già riferimento a proposito delle proroghe dei termini in materia di misure di sicurezza e di regolamenti sui dati sensibili e giudiziari, al par. 1.1), convertito, con modificazioni, dalla l. n. 51/2006, il cui art. 19-*bis* modifica l'art. 58, comma 2, del "Codice del consumo" (d.lg. 6 settembre 2005, n. 206), prevedendo che le disposizioni che individuano i limiti di utilizzo di tecniche di comunicazione per la conclusione di contratti a distanza si applichino anche in deroga alle norme previste dal Codice;

Attività delle autorità indipendenti in materia di tutela del risparmio

d) la l. 28 dicembre 2005, n. 262, recante "*Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari*", la quale prevede (art. 21) forme di collaborazione tra la Banca d'Italia, la Commissione nazionale per la società e la borsa (Consob), l'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (Isvap), la Commissione di vigilanza sui fondi pensione (Covip) e l'Autorità garante della concorrenza e del mercato, anche mediante scambio di informazioni, al fine di agevolare l'esercizio delle rispettive funzioni. D'interesse per il Garante appaiono, in particolare, le disposizioni generali sui procedimenti di competenza delle autorità e, in particolare, l'articolo 23, il quale disciplina i procedimenti per l'adozione di atti regolamentari e generali da parte delle citate autorità indipendenti;

Nuova disciplina delle attività trasfusionali

e) la l. 21 ottobre 2005, n. 219, recante nuove norme in materia di attività trasfusionali e di produzione degli emoderivati, la quale disciplina le attività trasfusionali comportanti la raccolta, oltre che del sangue e degli emocomponenti, anche delle cellule staminali. La legge prevede l'istituzione di un sistema informativo dei servizi trasfusionali, le cui caratteristiche saranno definite con decreto del Ministro della salute, al quale è demandata anche l'individuazione di un sistema di codifica che, *"nel rispetto delle norme sulla tutela e riservatezza dei dati sensibili"*, identifichi il donatore e il ricevente, nonché gli emocomponenti e le strutture trasfusionali. Il Garante dovrà fornire indicazioni sulle garanzie e cautele da adottare nel trattamento di tali dati in occasione dell'espressione del parere sullo schema di decreto, previsto ai sensi dell'articolo 154, comma 4, del Codice;

Misure di contrasto all'evasione fiscale

f) il d.l. 30 settembre 2005, n. 203 (*cd.* "collegato" alla manovra finanziaria per il 2006), convertito, con modificazioni, dalla l. 2 dicembre 2005, n. 248, recante misure di contrasto dell'evasione fiscale. Il decreto ha introdotto alcune disposizioni volte ad agevolare l'accesso dei comuni a banche di dati, nonché quello dei "concessionari" a dati personali utili ai fini della riscossione dei tributi. Il Garante, nel corso della discussione parlamentare del decreto e nell'esercizio del proprio compito di segnalazione al Parlamento, ha richiamato l'attenzione della Commissione finanze del Senato sull'esigenza di coordinare tali disposizioni con quelle previste dal Codice, in particolare per quanto riguarda il principio di pertinenza e non eccedenza dei dati accessibili per finalità istituzionali, e per ciò che attiene all'obbligo per i "concessionari" di informare i debitori ai sensi dell'articolo 13 del Codice. La necessità di procedere ad un'idonea informativa degli interessati è stata richiamata dal Garante anche con un *provvedimento* generale del 25 maggio 2005 [doc. *web* n. 1131826] riguardante alcune disposizioni della legge finanziaria del 2005 –che hanno aumentato il patrimonio informativo a disposizione degli organi preposti alla riscossione dei tributi– al fine di assicurare che le esigenze di riscossione dei crediti pubblici possano essere soddisfatte, ma rispettando pienamente, al tempo stesso, le garanzie e i diritti fondamentali dei soggetti interessati (sul punto *v.*, *amplius*, il par. 2.9);