

10 Libere professioni

10.1. *Attività forense. Ordini e collegi professionali*

Nell'ottica del rafforzamento dell'attenzione del Garante e dell'incidenza della sua azione nel mondo delle libere professioni, con particolare riferimento all'attività forense, e nel variegato ambito di operatività dei concessionari di pubblici servizi, l'Autorità ha istituito con deliberazione del 15 dicembre 2005 un'apposita unità organizzativa di primo livello denominata "Unità attività forense, ordini professionali e pubblici servizi", con decorrenza operativa dal 1° gennaio 2006. A tale unità è stato assegnato il compito di curare l'applicazione del Codice rispetto ai trattamenti di dati personali relativi all'attività degli ordini professionali e all'attività forense, nonché a quelli inerenti ai concessionari di pubblici servizi.

Tra i primi obiettivi che l'Autorità intende raggiungere in proposito a partire dal 2006 vi è quello di riavviare i lavori del codice di deontologia e buona condotta previsto dall'art. 135 del Codice, relativo ai trattamenti di dati personali effettuati da investigatori privati e liberi professionisti, in relazione ad investigazioni difensive e a trattamenti effettuati per far valere o difendere un diritto in giudizio.

11 Concessionari di pubblici servizi

11.1. Servizi di riscossione tributi

Dichiarazione stragiudiziale

Negli anni passati, intervenendo a seguito di numerosi quesiti, segnalazioni e ricorsi, l'Autorità aveva giudicato illecita la prassi, propria di alcune società concessionarie del servizio per la riscossione dei tributi, consistente nel richiedere a terzi informazioni personali sul contribuente, in modo da ottenere dichiarazioni stragiudiziali attestanti l'esistenza di crediti del contribuente su cui rivalersi; ciò, in quanto nessuna previsione legislativa o regolamentare attribuiva alle società concessionarie il potere di effettuare questo tipo di trattamento.

La legge finanziaria 2005 ha introdotto, in materia, l'istituto della "dichiarazione stragiudiziale" (art. 1, comma 425, l. n. 311/2004), sulla base della quale il concessionario del servizio di riscossione dei tributi risulta ora legittimato a chiedere ai debitori del soggetto iscritto a ruolo di indicare, per iscritto, le cose e le somme da essi dovute allo stesso soggetto, anche solo in modo generico. Nel più volte richiamato *provvedimento* del 25 maggio 2005 [doc. *web* n. 1131826], il Garante ha affermato al riguardo la necessità di verificare il rispetto del principio di pertinenza e non eccedenza e di assicurare che la competente amministrazione impartisca ai concessionari idonee istruzioni, a norma di legge, per i casi in cui si ritenga di dover ricorrere a tale strumento, prevedendo che il concessionario — oltre ad informare l'interessato sul trattamento dei dati — fornisca allo stesso una comunicazione preventiva della possibilità che, in caso di mancato pagamento, verrà acquisita una dichiarazione stragiudiziale prima di procedere al pignoramento presso terzi, utilizzando tale strumento solo dopo aver documentato l'impossibilità di procedere altrimenti alla riscossione del credito. Dovrà essere altresì verificato su base casistica, anche in relazione all'importo dovuto, se le cose e le somme dovute dai debitori del soggetto iscritto a ruolo debbano essere indicate dal terzo in modo generico oppure puntuale, indicando chiaramente nella richiesta il dettaglio delle informazioni richieste e la facoltatività o meno della risposta.

Relativamente a questo aspetto sarà peraltro necessario prendere in considerazione la riforma in materia di servizio nazionale della riscossione introdotta dalla legge finanziaria per il 2006 (l. n. 266/2005, in *G.U.* 29 dicembre 2005, n. 302, *S.O.* n. 211), che ha previsto la costituzione, da parte dell'Agenzia delle entrate e dell'Inps, della società Riscossione S.p.A.

Tarsu

L'Autorità è intervenuta, a seguito di una segnalazione, per valutare la liceità del trattamento di dati personali previsto ai fini del controllo del pagamento della tassa sui rifiuti solidi urbani (Tarsu). Al riguardo, il Garante ha osservato che la normativa di settore riconosce ai comuni, al fine di accertare e controllare il pagamento della citata tassa, la possibilità di invitare direttamente il contribuente ad esibire o trasmettere atti e documenti e di inviare questionari relativi a dati e notizie di carattere specifico, con invito a restituirli compilati e firmati (art. 11, comma 3, d.lg. 30 dicembre 1992, n. 504; art. 73, comma 1, d.lg. 15 novembre 1993, n. 507). Per lo svolgimento di tale attività, i comuni possono peraltro avvalersi legittimamente, in conformità alle disposizioni in materia di protezione dei dati personali, della collaborazione di soggetti privati (*Nota* 6 dicembre 2005).

12

Rapporto di lavoro e previdenza

12.1. Rapporti di lavoro in ambito pubblico

L'Autorità è intervenuta in numerose occasioni rispetto all'esercizio del diritto di accesso dei lavoratori ai propri dati personali.

Nell'esaminare due ricorsi concernenti richieste volte a conoscere i dati personali conservati in qualsiasi forma dal datore di lavoro, il Garante ha nuovamente precisato che l'esercizio del diritto di accesso consente all'interessato di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione in forma intelligibile dei dati personali detenuti dal titolare del trattamento; non permette, invece, l'accesso diretto e indiscriminato a documenti ed intere tipologie di atti, ovvero la creazione di documenti inesistenti negli archivi, oppure la loro aggregazione innovativa secondo specifiche modalità prospettate dall'interessato o, ancora, di ottenere, sempre e necessariamente, copia (fotostatica o autenticata) dei documenti detenuti (*Prov. 16 giugno 2005 [doc. web n. 1149999]*).

Nel fornire riscontro alla richiesta, il titolare del trattamento deve comunicare solo i dati personali richiesti ed effettivamente detenuti e non è tenuto, invece, a ricercare o raccogliere altri dati che, seppure originariamente trattati, non siano nella propria disponibilità e non siano oggetto in alcuna forma di un attuale trattamento.

In particolare, in uno dei casi sottoposti all'esame del Garante (*Prov. 21 dicembre 2005 [doc. web n. 1217532]*), concernente il riscontro a varie istanze di accesso rivolte da una dipendente all'azienda ospedaliera di appartenenza, si è evidenziato che tale riscontro non può avere ad oggetto i dati relativi a terzi, anche di natura sensibile, contenuti nelle richieste di diagnosi e cura sottoscritte dalla ricorrente. Il riscontro può riguardare legittimamente i dati relativi all'interessata consistenti nel suo nome e cognome, nei casi in cui nelle medesime richieste figurino (o vi sia associata) una sottoscrizione intelligibile di quest'ultima, ma non obbliga comunque il titolare del trattamento a fornire copia di tutti i supporti cartacei che li contengano, né tanto meno ad indicare quali e quanti siano tali documenti nel caso in cui i dati siano estrapolati e comunicati nei modi previsti dal Codice (art. 10, comma 4).

In risposta ad un quesito presentato da un dirigente statale, cui l'amministrazione di appartenenza aveva negato l'accesso ai documenti concernenti la valutazione dei propri colleghi, effettuata ai fini dell'assegnazione del premio di risultato, è stato ribadito che le informazioni di tipo valutativo, ivi compresi i giudizi, le valutazioni e gli altri elementi sui quali si basa eventualmente il giudizio sintetico espresso in occasione della valutazione dei dirigenti, sono dati personali e, in quanto tali, soggetti alla disciplina del Codice (*v. in particolare, l'art. 8, comma 4, del Codice*). Per questo motivo, tali informazioni, ove detenute da una pubblica amministrazione, possono essere rese conoscibili a soggetti privati diversi dalla persona cui si riferiscono, soltanto in base ad una previsione legislativa o regolamentare (art. 19, comma 3, del Codice).

Le disposizioni sull'accesso ai documenti amministrativi, applicabili anche al procedimento di valutazione dei dirigenti per espressa indicazione dell'art. 1, comma 5, d.lg. 30 luglio 1999, n. 286, rappresentano peraltro un'idonea base normativa per la comunicazione a terzi dei dati personali, eventualmente contenuti negli atti cui è rivolta l'istanza di accesso. In questo caso, spetta all'amministrazione destinataria del-

**Accesso
ai dati personali
in ambito lavorativo**

**Valutazione
dei dirigenti**

Tutela della dignità
e riservatezza
dei dipendenti

l'istanza di accesso verificare, di volta in volta, l'accogliibilità, o meno, di singole istanze di accesso alla documentazione valutativa, appurando i presupposti legittimanti l'accesso del richiedente, nonché le ragioni in base alle quali tali documenti debbano essere sottratti alla sua conoscibilità (*Nota* 7 febbraio 2005).

A seguito di una segnalazione il Garante è intervenuto a tutela della dignità e della riservatezza di una lavoratrice i cui dati personali, riguardanti la sua inidoneità al servizio dichiarata da "una commissione medica", erano stati riportati su alcuni atti interni concernenti lo svolgimento di una riunione svoltasi tra alcuni dipendenti, e successivamente affissi all'albo dell'ufficio.

Al riguardo, è stato accertato che le informazioni riportate nel materiale affisso, pur non fornendo alcuna specifica indicazione sui motivi di salute ritenuti all'origine dell'inidoneità della lavoratrice, facevano indirettamente riferimento alle condizioni di salute dell'interessata ed erano perciò da ritenersi "sensibili", in quanto il riscontro dell'inidoneità al servizio era derivato dal pronunciamento di una commissione medica, del quale negli atti affissi si faceva espressa menzione.

L'Autorità ha inoltre rilevato che, nel caso di specie, la diffusione non poteva ritenersi lecita, ponendosi in contrasto con i principi di proporzionalità, indispensabilità, pertinenza e non eccedenza, nonché con le cautele di cui all'art. 22 del Codice. In conformità a tali principi, l'esigenza di rendere noti ai colleghi non presenti alla riunione gli argomenti affrontati avrebbe potuto essere, infatti, utilmente soddisfatta mediante altre modalità di messa a disposizione delle informazioni, maggiormente rispettose della dignità e della riservatezza dell'interessata, come, ad esempio, la consegna in plico chiuso ai colleghi dei documenti affissi all'albo (*Nota* 23 novembre 2005).

Personale
delle forze armate
e di polizia

Con riferimento al trattamento di dati personali nell'ambito della gestione del personale delle forze armate e di polizia, l'Autorità ha esaminato due casi di opposizione al trattamento posto in essere dalla Guardia di finanza ai fini dell'accertamento della responsabilità disciplinare del personale.

In un primo caso, il Garante ha rilevato che, nell'ambito di tali attività, può essere lecitamente comunicata, ai superiori di un finanziere, la richiesta di archiviazione avanzata da un pubblico ministero in ordine ad una denuncia presentata dall'interessato nei confronti di altri componenti del Corpo, al fine di verificare eventuali violazioni delle disposizioni del regolamento di disciplina militare (in particolare, dell'art. 52, comma 5, lett. *b*), d.P.R. n. 545/1986, il quale prevede che il militare sia tenuto a comunicare al proprio comando gli "eventi in cui fosse rimasto coinvolto e che possono avere riflessi sul servizio") ed avviare, se necessario, il procedimento di contestazione di una infrazione disciplinare (*Prov. 28 settembre 2005* [doc. *web* n. 1180099]).

In un altro caso è stata ritenuta lecita la comunicazione alle superiori gerarchie del Corpo di vicende riguardanti l'interessato, che lo avevano indotto ad inoltrare una comunicazione di notizia di reato alle competenti autorità giudiziarie militari. Tali informazioni facevano infatti riferimento ad accadimenti di interesse, sia sotto il profilo amministrativo, sia, eventualmente, sotto quello disciplinare, verificatisi nella caserma presso cui l'interessato prestava servizio; non costituivano, nella specie, una violazione delle disposizioni sul segreto nelle indagini preliminari (art. 329 c.p.p.), dal momento che non contenevano alcun riferimento ad atti di indagine (*Prov. 3 novembre 2005* [doc. *web* n. 1198494]).

Immigrazione

Per quanto riguarda l'attività connessa con l'ingresso e la regolarizzazione dei cittadini extracomunitari, il Garante è intervenuto in riferimento alla predisposizione della modulistica utilizzata per le esigenze dello Sportello unico per l'immigrazione. Il Ministero dell'interno ha chiesto infatti il parere all'Autorità in merito ad un

decreto relativo alla modulistica necessaria al rilascio di provvedimenti di nulla osta in materia di assunzione di lavoratori stranieri o di ricongiungimento familiare.

Il Garante ha evidenziato la necessità di perfezionare l'informativa da rendere all'interessato e di individuare correttamente il titolare di trattamento; è stata inoltre richiamata l'esigenza di rispettare i principi di necessità, pertinenza e non eccedenza nel trattamento dei dati raccolti con la modulistica rispetto alle finalità perseguite, con particolare riguardo ai dati idonei a rivelare lo stato di salute del datore di lavoro in caso di lavoro domestico per assistenza (*Prov. 25 maggio 2005* [doc. web n. 1131847]).

12.2. Previdenza

La legge finanziaria 2005 ha stabilito che, a decorrere dal 1° giugno 2005, nei casi di infermità comportante incapacità lavorativa, il medico curante debba trasmettere all'Inps, per via telematica, il certificato di diagnosi sull'inizio e sulla durata presunta della malattia. La definizione delle specifiche tecniche e delle modalità procedurali è demandata ad un apposito decreto interministeriale di iniziativa del Ministero del lavoro e della previdenza sociale (art. 1, comma 149, l. n. 311/2004). Con il più volte richiamato *provvedimento* del 25 maggio 2005 il Garante — che dovrà essere comunque chiamato ad esprimere un parere su tale decreto — ha richiesto preventivamente che vengano individuate in tale sede soluzioni efficaci e rispettose dei principi in materia di protezione dei dati personali.

Su specifica richiesta dell'Inps, l'Autorità ha inoltre esaminato uno schema di protocollo volto a consentire ai patronati la consultazione delle posizioni relative agli assicurati contenute nelle banche dati dell'istituto previdenziale e, in particolare, nel Casellario centrale delle posizioni previdenziali (l. 23 agosto 2004, n. 243; d.m. 4 febbraio 2005, in *G.U.* 29 marzo 2005, n. 72).

Le modalità previste nello schema di protocollo sono state ritenute, allo stato, conformi alle disposizioni in materia di protezione dei dati personali, in attesa che vengano stabilite con decreto del Ministro del lavoro e delle politiche sociali le linee-guida per apposite convenzioni da stipularsi tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni, e ferme restando le possibili indicazioni che il Garante potrà impartire nel parere previsto sul medesimo decreto. Il protocollo prevede infatti che i patronati possano accedere alle banche dati dell'istituto, ma nell'ambito del mandato conferito dall'interessato e sulla base del consenso manifestato in relazione a tipi di dati individuati specificamente (art. 116 del Codice).

La circostanza che le disposizioni sul Casellario centrale delle posizioni previdenziali non menzionino espressamente i patronati tra i soggetti legittimati ad accedervi non è stata, peraltro, ritenuta ostativa della possibilità di consentire ai patronati stessi la consultazione delle informazioni contenute nella banca dati, nella misura in cui ciò avvenga alle condizioni e per le sole finalità previste dall'art. 116 del Codice (*Nota* 8 febbraio 2006).

L'Ufficio del Garante ha fornito altresì la propria collaborazione per l'elaborazione, su iniziativa di un gruppo di rappresentanti di alcuni istituti di patronato e di assistenza sociale, di un modello di informativa da fornire agli interessati che decidano di farsi assistere e rappresentare da tali enti nello svolgimento di pratiche relative a prestazioni in materia di previdenza, assistenza sociale e sanitaria.

A seguito della segnalazione inoltrata da un'associazione, l'Ufficio si è pronunciato circa il trattamento di dati personali effettuato da un istituto previdenziale, ai fini del riconoscimento di prestazioni sociali agevolate nei confronti di soggetti con

**Trasmissione
telematica
dei certificati
di malattia all'Inps**

**Accesso dei patronati
a banche dati
previdenziali**

**Informativa
rilasciata agli assistiti
da istituti di patronato**

**Prestazioni sociali
agevolate**

Incaricati
del trattamento
di dati previdenziali

handicap permanente grave e di soggetti ultra-sessantacinquenni non autosufficienti. La normativa di settore demanda ad un apposito decreto del Presidente del Consiglio dei ministri l'individuazione delle informazioni da dichiarare, in modo da evidenziare la situazione economica del solo assistito (art. 3, comma 2-ter, d.lg. n. 109/1998). Pur nella persistente mancanza di tale decreto attuativo, su cui l'Autorità dovrà essere chiamata ad esprimere il proprio parere, si è ritenuto che il rispetto dei principi di indispensabilità, pertinenza e non eccedenza dei dati raccolti rispetto alle finalità perseguite, imponga all'istituto di raccogliere soltanto le informazioni personali relative alla situazione economica degli interessati, e non anche quelle relative ai componenti del nucleo familiare di appartenenza (*Nota* 24 marzo 2006).

L'Autorità è intervenuta in un caso riguardante il trattamento di dati personali relativi all'estratto della posizione contributiva dell'interessato, acquisiti presso gli archivi di un istituto previdenziale e successivamente utilizzati dal coniuge — dipendente di una sede provinciale del medesimo istituto — nel giudizio di separazione legale. In seguito alle lamentele dell'interessato, l'istituto aveva, nel frattempo, oscurato la sua posizione contributiva in modo da evitare ulteriori accessi non autorizzati.

L'Ufficio ha rilevato che spetta all'istituto impartire adeguate istruzioni ai propri dipendenti in merito all'accesso e all'utilizzo delle informazioni da essi conoscibili ed assicurare la corretta applicazione della disciplina sulla protezione e sulla sicurezza dei dati, anche in riferimento a possibili trattamenti illeciti o non conformi alle finalità della raccolta, ascrivibili anche alla condotta di singoli dipendenti (artt. 31-36 del Codice). La sede interessata è stata pertanto invitata a far conoscere le iniziative e gli accorgimenti assunti per rendere il trattamento conforme alle disposizioni sulla sicurezza e per ripristinare, nei casi e nei modi consentiti, l'accesso dell'interessato ai dati personali relativi alla sua posizione contributiva.

Quanto all'utilizzo dei dati dell'interessato nel giudizio di separazione legale è stato precisato che la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nei procedimenti giudiziari basati sul trattamento, e quindi anche sulla eventuale raccolta illecita di dati personali, restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale (art. 11, comma 2, e 160, comma 6, del Codice) (*Nota* 11 novembre 2005).

13

Videosorveglianza

Anche nel corso del 2005, il Garante ha avuto occasione di occuparsi delle tematiche relative all'impianto ed all'utilizzo di sistemi di videosorveglianza.

Con riferimento all'installazione di impianti di videosorveglianza presso abitazioni, è stato nuovamente ribadito in una decisione adottata su ricorso che le disposizioni del Codice non risultano applicabili al trattamento di dati effettuato per fini personali, pur restando ferma l'osservanza degli obblighi in materia di sicurezza e di risarcimento dell'eventuale danno, nonché la facoltà dei soggetti che ritengono di aver subito un danno per effetto del trattamento dei dati di far valere i propri diritti in ordine alla liceità e correttezza della raccolta e dell'utilizzazione delle immagini (*Prov. 27 ottobre 2005 [doc. web n. 1193121]*).

Abitazioni private

13.1. Videosorveglianza in ambito pubblico

In relazione all'ambito pubblicistico molteplici segnalazioni e quesiti hanno evidenziato come, nonostante i ripetuti interventi del Garante, a due anni dall'adozione del *provvedimento* generale del 29 aprile 2004 [doc. web n. 1003482], lo stato di attuazione della disciplina in materia di videosorveglianza non risulti ancora del tutto soddisfacente, essendo emerse situazioni diffuse caratterizzate dall'omessa o inidonea applicazione delle regole fissate. Anche per questo, sono risultate numerose le occasioni per ribadire le indicazioni per un corretto utilizzo di telecamere da parte di soggetti pubblici in specifici settori.

Con riferimento all'installazione di sistemi di videosorveglianza presso istituti scolastici l'Autorità ha riaffermato la vigenza delle prescrizioni fornite con il *provvedimento* generale. In ordine all'attivazione di telecamere all'interno dell'edificio di un istituto anche durante l'orario delle lezioni, è stata ad esempio rappresentata la necessità di limitarla ai casi di stretta indispensabilità, come ad esempio, a causa di ripetuti atti vandalici e comunque al di fuori dell'orario scolastico, quando gli edifici sono chiusi, anche in ragione del fatto che possono essere altrimenti raccolti indebitamente dati riguardanti minori di età e di lavoratori (*Nota 26 aprile 2005*). Nella predetta circostanza l'Ufficio ha invitato l'istituto a produrre ogni documento utile a sostegno delle iniziative assunte al fine di rendere il trattamento dei dati effettuato conforme al quadro di garanzie delineato nel *provvedimento* generale, ricevendo un riscontro sul quale sono in corso ulteriori accertamenti.

In un diverso ambito il Garante ha fornito riscontro ad una richiesta pervenuta in merito all'utilizzo, da parte di alcuni comuni, di telecamere mobili installate su automezzi e posizionate temporaneamente in siti prestabiliti individuati di volta in volta in base a contingenti esigenze di sicurezza. In proposito, l'Autorità ha ribadito il necessario rispetto del principio di proporzionalità tra i mezzi impiegati e i fini perseguiti; in particolare, secondo tale principio, impianti di videosorveglianza possono essere attivati solo quando altre misure siano ponderatamente ritenute insufficienti o inattuabili. Tale valutazione deve essere, poi, effettuata specificamente anche in riferimento alla dislocazione, all'angolo visuale e alle tipologie –fisse o mobili– delle apparecchiature installate. Anche per le telecamere di tipo mobile

INFORMATICA E TELECOMUNICAZIONI

Scuole

INFORMATICA E TELECOMUNICAZIONI

Telecamere mobili

**Presupposti
per la videosorveglianza
da parte dei comuni**

restano valide le indicazioni specifiche relative all'installazione di sistemi di videosorveglianza presso, ad esempio, luoghi di culto o di sepoltura o per il controllo di aree abusivamente impiegate come discariche di materiali e di sostanze pericolose (*Nota* 8 novembre 2005).

In diverse occasioni sono stati forniti altri chiarimenti circa la possibilità, per i comuni, di attivare sistemi di videosorveglianza. In particolare è stato evidenziato che l'utilizzo di sistemi di videosorveglianza può essere giustificato solo ed esclusivamente dallo svolgimento di funzioni istituzionali che la stessa amministrazione è tenuta ad individuare ed esplicitare con esattezza e di cui essa sia effettivamente titolare in base all'ordinamento di riferimento (*Note* 16 e 22 febbraio 2005, 7 e 22 aprile 2005, 21 ottobre 2005 e 12 dicembre 2005).

È stata richiamata inoltre, in proposito, l'opportuna attenzione sul necessario rispetto di tutte le prescrizioni contenute nel *provvedimento* generale del 29 aprile 2004, ivi comprese la designazione dei responsabili o incaricati del trattamento, la predisposizione dell'informativa da rendere agli interessati (utilizzando eventualmente il modello semplificato messo a disposizione dal Garante in allegato al citato provvedimento) e l'adozione delle misure minime di sicurezza.

**Discariche abusive
e orario di deposito
dei rifiuti urbani**

Sono state nuovamente confermate le indicazioni già fornite a proposito dell'utilizzo di sistemi di videosorveglianza presso aree abusivamente impiegate come discariche di materiali, ricordando che tale utilizzo è lecito solo qualora risultino inefficaci o inattuabili altre misure; per converso, non risulta lecito un controllo video al solo scopo di accertare infrazioni amministrative rispetto a disposizioni concernenti le modalità e l'orario di deposito dei sacchetti dei rifiuti dentro gli appositi contenitori (*Note* 29 dicembre 2004 e 22 febbraio 2005). In un caso, a seguito della segnalazione pervenuta da un'associazione di risparmiatori e consumatori, l'Ufficio del Garante ha invitato a conformarsi alle citate prescrizioni un comune che intendeva "monitorare" le operazioni di smaltimento dei rifiuti per verificare il rispetto delle disposizioni sulla raccolta differenziata. L'ente locale ha comunicato di aver disattivato il sistema di registrazione e di aver cancellato tutte le immagini registrate (*cfr. Newsletter* 21-27 febbraio 2005).

**Accesso
ai centri storici e Ztl**

L'Autorità è stata nuovamente interpellata in riferimento all'installazione di sistemi di rilevazione degli accessi dei veicoli ai centri storici e alle zone a traffico limitato. Si è confermato che i comuni devono richiedere una specifica autorizzazione amministrativa e limitare la rilevazione delle immagini ai soli casi di infrazione (art. 3 d.P.R. 22 giugno 1999, n. 250). I dati così trattati possono essere conservati solo per il periodo necessario per contestare le infrazioni e per definire il relativo contenzioso; alle informazioni si può accedere solo a fini di polizia giudiziaria o di indagine penale (*Note* 22 febbraio 2005).

Strutture sanitarie

Rigorose e specifiche cautele sono state richiamate anche in relazione all'attivazione di impianti di videosorveglianza in alcune aree di un *campus* ospedaliero e presso gli ingressi di una sede di un'azienda sanitaria (*Note* 22 febbraio 2005 e 12 aprile 2005). In particolare, nel rappresentare che l'impiego di un sistema di videosorveglianza all'interno di una struttura sanitaria per finalità di sicurezza può evidenziare anche profili inerenti alle condizioni di salute dei pazienti, è stato confermato che l'eventuale controllo di ambienti sanitari e il monitoraggio di pazienti ricoverati in particolari reparti o ambienti (*ad es.*, unità di rianimazione) devono essere limitati a casi di stretta indispensabilità, circoscrivendo le riprese solo a determinati locali e a precise fasce orarie e adottando tutti gli accorgimenti necessari per garantire un elevato livello di tutela della riservatezza e della dignità delle persone malate. Nelle stesse occasioni è stato fatto nuovamente presente che possono accedere alle immagini solo i soggetti specificamente autorizzati (*ad es.*, personale

medico ed infermieristico), non potendo le stesse essere visionate da estranei (*ad es.*, visitatori), e che le immagini idonee a rivelare lo stato di salute non devono essere comunque diffuse, a pena di sanzione penale (artt. 22, comma 8, e 167 del Codice).

Per quanto riguarda l'installazione di impianti video nei luoghi di lavoro è stato ricordato ad una prefettura e ad una direzione provinciale di un istituto previdenziale, come già rilevato in precedenti provvedimenti dell'Autorità, che detta installazione potrebbe coinvolgere anche i lavoratori dipendenti e configurare pertanto un controllo a distanza nei confronti dei lavoratori. A tale proposito è stata nuovamente richiamata l'attenzione sulle garanzie previste per i rapporti di lavoro anche quando gli impianti sono utilizzati per esigenze organizzative e dei processi produttivi, ovvero sono richiesti per la sicurezza del lavoro, con particolare riferimento al principio contenuto nell'art. 4 dello Statuto dei lavoratori che sancisce il divieto di controllo a distanza dell'attività dei lavoratori (*Note* 8 e 22 febbraio 2005). Non è stata invece rinvenuta lesiva del citato principio la condotta di un ente di ricerca che aveva installato alcune telecamere a tutela della sede di una segreteria ove veniva esplicata una delicata funzione di sicurezza (*Nota* 2 febbraio 2006).

L'Autorità è stata chiamata a pronunciarsi anche a proposito dell'attivazione di sistemi di videosorveglianza presso impianti sportivi di capienza superiore alle diecimila unità, in occasione di competizioni calcistiche.

In particolare, il Garante ha espresso parere riguardo a due schemi di decreto, predisposti dal Ministero dell'interno in attuazione di un decreto-legge (n. 28/2003) che prevede, tra le misure contro la violenza negli stadi, oltre al rilascio di biglietti numerati, anche l'introduzione di telecamere fisse. Al riguardo, l'Autorità ha stabilito che il controllo svolto mediante videosorveglianza, basandosi su un idoneo fondamento normativo, risulta rispettoso del principio di liceità (art. 11, comma 1, lett. *a*), del Codice) ed è altresì giustificato alla luce del principio di necessità e proporzionalità nel trattamento dei dati, anche in ragione dei reiterati disordini e degli episodi di violenza verificatisi. Sono state poi considerate, in termini generali, proporzionate, alcune disposizioni in materia di conservazione dei dati, di modalità di ripresa e di tipologia di informazioni rilevabili, risultando trattati dati pertinenti e non eccedenti rispetto alle finalità di tutela dell'ordine pubblico e della sicurezza e di accertamento di reati.

Il Garante ha chiesto di limitare l'ambito applicativo ai soli impianti sportivi di capienza superiore alle diecimila unità e ad eventi in occasione di competizioni calcistiche, derivando questi limiti direttamente dalla norma di legge, e di espungere riferimenti ad altri ambiti applicativi non previsti da tale norma (*Parere* 4 maggio 2005 [doc. *web* n. 1120732]).

Accanto a diverse altre indicazioni (delimitazione dell'ambito geografico di alcune riprese alle "immediate vicinanze degli impianti"; registrazioni audio del solo evento calcistico in generale; individuazione del soggetto che dovrebbe prescrivere misure di sicurezza; modalità di previsione dell'obbligo di porre dati e supporti a disposizione dell'autorità o della polizia giudiziaria), il Garante ha affrontato analiticamente la questione della previsione di biglietti nominativi di accesso agli stadi, aggiuntiva rispetto a quella dei biglietti numerati.

L'Autorità ha richiamato l'attenzione sulle misure di controllo di altro tipo introdotte in altri Paesi constatando che il decreto-legge introduce solo l'obbligo di numerare i biglietti e sollecitando quindi una verifica circa la possibilità di introdurre questo ulteriore vincolo con un provvedimento amministrativo. Rilevato poi che la nominatività dei biglietti comporta la creazione di grandi banche dati relative a diverse centinaia di migliaia di interessati, il Garante ha rilevato che a sostegno della richiesta di parere non erano stati allegati specifici elementi che potessero per-

Luoghi di lavoro

Impianti sportivi

mettergli di ritenere allo stato proporzionata “una misura delicata di cui, a fronte degli innumerevoli dati personali che dovrebbero essere trattati, dovrà essere valutata attentamente la proporzione e l’effettiva utilità in rapporto alle finalità perseguite e alle più frequenti modalità con cui si svolgono incidenti negli stadi. Ciò, tenendo anche conto che potrebbero essere attivati altri controlli di sicurezza per identificare tifosi violenti ed escluderli dagli stadi...valutando infine la circostanza che i biglietti nominativi non risultano utilizzati diffusamente in altri Paesi dell’Unione europea (a parte i titoli di abbonamento, rilasciati per altre finalità”.

Sulla videosorveglianza in generale, allo scopo di verificare la conformità alle indicazioni contenute nel provvedimento generale sulla videosorveglianza, è stata sviluppata un’intensa attività ispettiva che ha evidenziato in più occasioni un rispetto non ancora rigoroso della disciplina, con particolare riferimento alla liceità dei sistemi installati, all’idoneità della necessaria informativa all’utenza, alle modalità di raccolta dei dati e ai tempi di conservazione delle immagini raccolte.

13.1.1. *Richieste di verifica preliminare*

In casi frequenti, il riscontro alle richieste di chiarimenti in materia di videosorveglianza ha fornito al Garante l’occasione per precisare che l’installazione di sistemi di videosorveglianza non deve essere generalmente sottoposta all’esame preventivo dell’Autorità e che non può per converso desumersi, dal mancato riscontro, alcuna approvazione implicita dalla trasmissione al Garante di comunicazioni o progetti relativi alla intenzione di installare sistemi di videosorveglianza. Non è del resto stabilito alcun termine decorso il quale i progetti sottoposti alla verifica dell’Autorità possano ritenersi dalla stessa autorizzati, non applicandosi neanche il principio del silenzio-assenso; deve ritenersi, invece, che il *provvedimento* 29 aprile 2004 abbia individuato espressamente le specifiche ipotesi in cui i titolari del trattamento sono tenuti a sottoporre alla verifica preliminare i sistemi di videosorveglianza che si intendono attivare.

14

Altre iniziative nel settore pubblico

14.1. *Utilizzo di dati biometrici*

In ambito pubblico sono pervenute numerose segnalazioni, nonché specifiche richieste di parere da parte di comuni, in merito all'utilizzo di sistemi di rilevazione automatica delle presenze mediante il riconoscimento delle impronte digitali. L'Autorità ha avviato nuove istruttorie in merito alla liceità dell'utilizzo di tali sistemi per il controllo dell'accesso al luogo di lavoro da parte dei dipendenti.

14.2. *Ulteriori iniziative dell'Ufficio*

L'Unità di crisi del Ministero degli affari esteri ha sottoposto all'esame del Garante un progetto denominato *“Dove siamo nel mondo”* per una valutazione preliminare in ordine alla sua compatibilità con la normativa in materia di protezione dei dati personali. Il progetto, nell'ambito dell'ottimizzazione della gestione di situazioni di crisi internazionali legate a calamità naturali, attentati terroristici ed altre emergenze, è volto a consentire ai cittadini italiani di segnalare al Ministero degli esteri, su base volontaria, i propri recapiti ed itinerari, al fine di facilitare la localizzazione, l'invio di eventuali avvisi o l'intervento di soccorso in caso di emergenze.

L'Ufficio del Garante ha indicato al Ministero le necessarie cautele da adottare nella realizzazione del progetto, con particolare riferimento alle tipologie di dati richiesti, alla loro gestione e conservazione, nonché all'informativa da fornire all'interessato e all'eventuale coinvolgimento di terzi.

La versione definitiva del progetto prevede la creazione di un apposito sito Internet attraverso il quale i cittadini, previa idonea informativa, possono inserire su base volontaria le proprie generalità ed informazioni sul viaggio (*ad es.*, paese di destinazione, date di partenza e di rientro, località di permanenza, dettagli dell'itinerario e recapiti); i dati registrati saranno automaticamente cancellati trascorse quarantotto ore dalla data di rientro. Il titolare del trattamento è il Ministero degli esteri e la banca dati è gestita unicamente dall'Unità di crisi. I dati raccolti sono utilizzati esclusivamente per lo studio e la realizzazione di piani di intervento per la sicurezza degli italiani all'estero in situazioni di crisi e potranno essere comunicati a determinati soggetti terzi al solo fine di assicurare assistenza in caso di emergenza.

PROGETTO DI LEGGE

Progetto***“Dove siamo nel mondo”***

15 Reti di comunicazione elettronica

15.1. *Conservazione dei dati di traffico*

Successivamente alle già ricordate modifiche apportate all'art. 132 del Codice dall'art. 3 del d.l. 24 dicembre 2003, n. 354, convertito, con modificazioni, dalla l. 26 febbraio 2004, n. 45 (*v. Relazione* 2004, p. 97), si è assistito, nel 2005, ad un nuovo, significativo intervento normativo, che ha ulteriormente innovato la disciplina della conservazione dei dati di traffico per finalità di accertamento e repressione dei reati (sul quale *v. par. 1.1*).

In tale contesto, il Garante, che aveva già avviato, conformemente alla previsione dell'art. 132, comma 5, del Codice, i lavori necessari per individuare le misure e gli accorgimenti al cui rispetto è subordinato il trattamento per le richiamate finalità di accertamento e repressione dei reati, ha esteso al traffico telematico l'ambito di verifica preliminare dei sistemi attualmente utilizzati dagli operatori, in vista della programmata predisposizione del provvedimento previsto dalla predetta disposizione.

15.2. *I nuovi elenchi telefonici*

Nella *Relazione* 2004 (p. 99) si era dato conto del provvedimento di carattere generale con il quale il Garante, ai sensi dell'art. 129, comma 2, del Codice, nonché in ragione delle modifiche introdotte nella disciplina degli elenchi telefonici, aveva individuato le modalità da osservare per il corretto inserimento e successivo utilizzo dei dati personali relativi ad abbonati (e utilizzatori di schede prepagate) nei nuovi elenchi telefonici (*cf. Provv. 15 luglio 2004 [doc. web n. 1032381]*).

Successivamente all'adozione del provvedimento il Garante ha fornito agli operatori prescrizioni integrative con riferimento ai moduli per l'informativa e la raccolta dei consensi predisposti dagli operatori, ed ha avviato altresì la campagna informativa prevista nel provvedimento stesso. L'Autorità ha, inoltre, avviato direttamente una prima campagna di informazione con un apposito *depliant* messo a disposizione degli operatori e attraverso una conferenza stampa tenutasi presso la sede dell'Autorità il 26 gennaio 2005.

Nel 2005 il Garante ha monitorato con attenzione, anche tramite varie richieste di informazioni agli operatori, il rispetto delle scadenze per l'attuazione della nuova disciplina indicate nel ricordato *provvedimento* del 15 luglio 2004 (*cf. l'allegato III del provvedimento*).

L'Ufficio, anche in risposta ad alcuni quesiti pervenuti in tema di utilizzabilità dei dati presenti nei nuovi elenchi telefonici da parte di soggetti operanti per finalità non di lucro, ha specificato che la nuova disciplina degli elenchi opera a prescindere dall'eventuale fine di profitto perseguito. Pertanto, ogni uso dei dati presenti nei nuovi elenchi diverso dalla comunicazione interpersonale, quali ad esempio le attività di carattere pubblicitario e promozionale, resta possibile solo con il consenso preventivo degli interessati. Il Garante ha altresì evidenziato come gli enti che perseguono finalità di carattere socio-assistenziale o di interesse collettivo o diffuso continuino, in ogni caso, a disporre di altre modalità per il reperimento dei dati perso-

nali dei potenziali sostenitori, in particolare tramite l'accesso alle liste elettorali (*cf.* art. 51, d.P.R. n. 223/1967, come modificato dall'art. 177 del Codice).

È stato inoltre rilevato che la nuova disciplina può non operare con riguardo ai dati personali estratti precedentemente dai vecchi elenchi e già effettivamente (e non elusivamente) registrati sempre in precedenza in una banca dati, eventualmente inseriti insieme ad altre informazioni tratte da ulteriori fonti. L'utilizzazione di questi dati è lecita solo se, al momento della loro registrazione, è stata fornita un'adeguata informativa agli interessati, instaurando così con gli stessi un "rapporto" nell'ambito del quale il titolare del trattamento è rimasto comunque obbligato a cancellare i dati di chi lo richieda. Se, però, la predetta informativa non è stata resa tempestivamente a norma di legge, il trattamento è stato ed è rimasto illecito; il titolare non può in alcun modo utilizzare i dati e deve necessariamente cancellarli per non incorrere in serie sanzioni. Per quanto concerne il necessario aggiornamento delle informazioni contenute nelle menzionate banche dati, è stato ribadito che lo stesso potrà avvenire soltanto sulla base delle nuove regole sull'uso degli elenchi telefonici.

15.3. Elenchi telefonici cd. "categorici"

Nel periodo di riferimento, il Garante ha valutato l'opportunità di intervenire in riferimento alla problematica degli elenchi telefonici organizzati per categorie merceologiche/professionali (*cd.* elenchi "categorici"). Tenendo conto del carattere commerciale e promozionale dei menzionati elenchi "categorici", che contengono informazioni relative allo svolgimento delle attività economiche ed equiparate dei soggetti interessati (in particolare aziende, professionisti, esercizi commerciali ed enti), nonché delle specifiche finalità degli stessi non riconducibili esclusivamente alla "mera ricerca dell'abbonato per comunicazioni interpersonali", il Garante ha individuato a favore degli editori di tali elenchi un particolare regime di semplificazione (*Prov. 14 luglio 2005 [doc. web n. 1151640]*).

Si è infatti chiarito che, per la formazione degli elenchi in questione, gli editori possono avvalersi della previsione del Codice che permette di prescindere dal consenso degli interessati quando il trattamento riguarda appunto "dati relativi allo svolgimento di attività economiche" (art. 24, comma 1, lett. *d*), del Codice). Devono essere comunque rispettati gli altri obblighi e diritti in materia di protezione dei dati personali: in particolare, deve essere garantita la completezza dei nominativi degli interessati riportati nelle diverse tipologie di elenchi pubblicati e, nel caso in cui i dati siano attinti dal nuovo "database unico", di cui all'allegato II del predetto provvedimento del 15 luglio 2004, non possono essere pubblicati gli estremi identificativi di coloro che abbiano eventualmente manifestato la volontà di non comparire negli elenchi telefonici "alfabetici".

L'Autorità, infine, ai sensi dell'art. 13, commi 4 e 5, lett. *c*), del Codice, ha autorizzato i suddetti titolari del trattamento a fornire a professionisti, esercenti, aziende ecc., che compariranno nell'elenco, un'informativa semplificata tramite la pubblicazione di appositi avvisi su quotidiani, nonché nella parte iniziale dell'elenco "categorico" cartaceo e di quello pubblicato *on-line*.

15.4. Spamming

Anche nel corso del 2005 si è mantenuta elevata l'attenzione dell'Autorità rispetto alla pratica dello *spamming* (invio di messaggi promozionali indesiderati

all'indirizzo di posta elettronica dei destinatari). Sono state, fra l'altro, intensificate le attività di controllo e verifica delle attività svolte da diversi operatori che, direttamente o per mezzo di soggetti specializzati, svolgono campagne pubblicitarie e di *direct marketing* utilizzando tale nuovo mezzo di comunicazione. Risulta, poi, in fase conclusiva l'istruttoria già avviata nei confronti di due importanti società operanti *on-line*, che utilizzano migliaia di indirizzi di posta elettronica per finalità promozionali e commerciali di prodotti e servizi propri e di altre aziende.

Particolare preoccupazione ha destato, tra l'altro, l'incremento delle segnalazioni che lamentano l'invio di *e-mail* riconducibili al fenomeno denominato "*phishing*", consistente nell'uso di messaggi di posta elettronica e nella creazione di pagine *web* progettate per simulare comunicazioni ufficiali da parte soprattutto di istituti di credito, con la finalità di aggirare gli utenti Internet per carpire dati personali o acquisire fraudolentemente informazioni riguardanti la carta di credito o il conto corrente bancario.

In ambito internazionale, nel periodo considerato, l'Autorità ha partecipato attivamente ai lavori del Cnsa (*Contact Network of Spam Authorities*) che si tengono presso la Commissione europea-Direzione generale società dell'informazione e media. Nei vari incontri, cui partecipano le istituzioni di settore di tutti i Paesi membri, si è proceduto a valutare vari strumenti di intervento per intensificare la lotta allo *spam*. È in corso la predisposizione di un documento comune, denominato *London Action Plan*, che definirà le procedure utili a facilitare le indagini sullo *spam* anche attraverso la semplificazione delle modalità di contatto tra le istituzioni partecipanti.

Tra le attività di carattere internazionale finalizzate a contrastare il fenomeno dello *spam* va ricordata anche la *task force* istituita presso l'Ocse, ai cui lavori ha partecipato anche l'Autorità, e che ha redatto nel 2005 una bozza di raccomandazione sulla "cooperazione transfrontaliera nel rafforzamento delle leggi contro lo *spam*" (sul punto, *u. par. 22.3*).

15.5. Videochiamate

I nuovi servizi telefonici disponibili attraverso l'impiego di telefoni mobili definiti "di terza generazione", tramite diverse tecnologie di rete, quali *Gprs*, *Edge* o *Umts*, sono stati già oggetto di attenzione da parte dell'Autorità (*cf. Relazione 2004*, pp. 100-101).

Rispetto al semplice utilizzo dei messaggi del tipo *Sms* e *Mms*, in ordine ai quali il Garante si è più volte pronunciato in passato, i "videotelefono" offrono nuove funzionalità. Questi apparecchi sono dotati di videocamere di dimensioni molto ridotte, orientabili in vario modo, e dispongono di diverse funzioni mediante le quali si possono agevolmente raccogliere, comunicare e diffondere immagini e suoni in tempo reale. Tali applicazioni, utili nell'ordinaria vita di relazione interpersonale, possono essere tuttavia utilizzate in modo da violare, anche involontariamente, i diritti delle persone interessate dalla comunicazione, come pure di terzi inconsapevoli della ripresa.

In ragione dei potenziali pericoli insiti nell'utilizzo di tali nuovi strumenti di telefonia, il Garante, all'esito di una consultazione pubblica attivata al fine di acquisire elementi di valutazione, ha individuato le modalità da osservare per un corretto utilizzo dei medesimi strumenti con riferimento al trattamento dei dati (*Prov. 20 gennaio 2005 [doc. web n. 1089812]*). In particolare, nell'evidenziare la generale liceità del loro utilizzo per fini esclusivamente personali, l'Autorità ha sottolineato che il Codice —ferme restando altre norme dell'ordinamento— non si applica se le

immagini rimangono nella disponibilità privata di chi ha effettuato le riprese o circolano solo tra un numero ristretto di persone. Si è indicata comunque la necessità che, anche in questi casi, il soggetto che utilizza l'apparecchio rispetti i diritti dei terzi anche in tema di diritto all'immagine e al ritratto, nonché gli obblighi previsti in materia di sicurezza dei dati, tenendo conto della possibilità di essere chiamati a risarcire eventuali danni anche morali cagionati a terzi.

È stata, poi, sottolineata l'illiceità di un'eventuale comunicazione sistematica attraverso il videotelefono o di una diffusione anche via Internet delle immagini, effettuata senza richiedere, quando è necessario, il consenso preventivo, libero e informato (manifestato per iscritto nel caso siano trattati dati sensibili). L'informativa ed il consenso possono riguardare in tal caso non solo i soggetti che si intende ritrarre direttamente, ma anche eventuali terzi, identificati o identificabili, eventualmente ripresi anch'essi nelle immagini.

Il Garante ha richiamato altresì l'attenzione sull'esigenza di verificare se, in determinati uffici pubblici, luoghi pubblici e privati o aperti al pubblico, l'uso dei videotelefonati sia eventualmente inibito: limiti e cautele (introdotti in alcuni Paesi anche con norme di legge) possono essere infatti prescritti legittimamente da soggetti pubblici e privati e, se non rispettati, possono rendere il trattamento dei dati illecito o non corretto. Garanzie analoghe sono state richiamate anche rispetto all'uso di immagini all'interno di forum *on-line*.

L'Autorità ha, infine, invitato imprese produttrici di apparecchi o impegnate nella realizzazione di *software* di valutare l'opportunità di dotare i cellulari di nuove funzioni, tra cui anche segnali luminosi, per rendere più evidente che il videotelefono è in funzione, come pure di sistemi per il blocco della trasmissione dell'immagine senza che venga interrotta la conversazione.

15.6. Chiamate in entrata

Il trattamento dei dati personali relativi alle comunicazioni telefoniche in entrata pone delicate implicazioni per la riservatezza delle persone cui gli stessi si riferiscono: oltre a riguardare gli abbonati o i titolari di una carta prepagata, le chiamate in entrata possono coinvolgere altri soggetti quali familiari, amici, membri di una comunità e dipendenti. Per questi motivi, relativamente a tali dati, il Codice non consente di regola agli interessati di rivolgere al fornitore di un servizio di comunicazione elettronica le istanze di cui all'art. 7. Solo in via di eccezione, le richieste di esercizio dei diritti possono essere presentate e riscontrate positivamente, qualora si compri che la risposta da parte del fornitore è necessaria per evitare "un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397" (art. 8, comma 2, lett. *f*), del Codice).

In tale contesto generale, il Garante (intervenuto già in passato sull'argomento in occasione dell'esame di ricorsi e segnalazioni) ha ritenuto necessario richiamare l'attenzione degli operatori telefonici sui limiti entro i quali i fornitori dei servizi di comunicazione elettronica accessibili al pubblico possono rispondere positivamente ad una richiesta *ex art. 7* del Codice, impartendo ad essi alcune prescrizioni con un apposito provvedimento di carattere generale (*Prov. 3 novembre 2005 [doc. web n. 1189488]*).

All'interno di quest'ultimo, è stato di nuovo posta in rilievo la disposizione codicistica che prevede che l'abbonato o il titolare di una carta prepagata possa conoscere i dati personali relativi al traffico telefonico in entrata, *Sms* ed *Mms* compresi, solo dimostrando l'indispensabilità dell'acquisizione di tali informazioni allo scopo

di tutelare i propri diritti in sede penale, in quanto la mancata conoscenza delle stesse determinerebbe un danno effettivo e concreto al diritto di difesa. I dati in tal modo conosciuti non possono essere utilizzati per altri scopi: a tal fine, il fornitore deve richiedere il rilascio di una dichiarazione, dall'interessato o dall'avvocato cui sia stato conferito mandato, che attesti la veridicità di quanto prospettato e manifesti l'impegno a non utilizzare i dati per altre finalità. Possono essere peraltro prese in considerazione solo le richieste corredate da una motivazione in cui sia specificata l'intenzione di utilizzare i dati nell'ambito di un procedimento penale, risultando pertanto escluse quelle riguardanti controversie civili e di volontaria giurisdizione.

È stato inoltre individuato in capo al fornitore del servizio l'obbligo di accertare con scrupolo l'identità e la legittimazione del richiedente, nonché quello di fornire un riscontro, seppur negativo, entro quindici giorni dal ricevimento dell'istanza. Non vi è, per converso, necessità di un'autorizzazione dell'autorità giudiziaria per comunicare i dati, né occorre che il richiedente documenti anche il numero di repertorio di un procedimento penale, in ragione del fatto che le indagini difensive possono essere avviate lecitamente anche prima di tale procedimento e per l'eventualità che esso sia instaurato (art. 391-*nonies* c.p.p.).

Sono stati infine specificati i dati che il fornitore potrà comunicare: si tratta del numero del chiamante, della data, dell'ora di inizio e della tipologia della comunicazione e della durata.

15.7. Intercettazioni

Nel mese di agosto del 2005, il Garante ha avviato un'indagine nei confronti dei principali gestori di telefonia fissa e mobile riguardo alle modalità con le quali essi adempiono alle richieste dell'autorità giudiziaria in materia di intercettazioni.

Gli accertamenti hanno messo in luce che i gestori, pur non venendo a conoscenza dei contenuti delle intercettazioni, raccolgono, selezionano, elaborano ed utilizzano una notevole quantità di dati personali riferibili agli indagati e ai terzi con i quali questi comunicano. Si tratta di dati personali particolarmente delicati che riguardano l'identità dei soggetti sottoposti ad intercettazione e l'arco temporale di svolgimento dell'intercettazione nonché i dati di traffico telefonico o telematico. In alcuni casi, tali dati sono integrati da informazioni aggiuntive relative alle chiamate in ingresso, ai tentativi di chiamata e alla localizzazione geografica dell'utenza intercettata.

È emerso, inoltre, che gli ulteriori servizi svolti dai fornitori a supporto dell'attività investigativa possono riguardare anche aspetti diversi dalle intercettazioni e comprendere interrogazioni anagrafiche, localizzazione dell'utenza, tracciamento e sospensione dei servizi agli utenti, documentazione del traffico storico. A differenza di quanto avviene con le conversazioni intercettate, i gestori hanno la possibilità di conoscere le informazioni derivanti dall'attivazione di questi servizi, essendo essi stessi ad estrarre i dati, a selezionarli secondo i criteri richiesti dall'autorità giudiziaria e ad organizzarli in tabulati. Infine, anche i servizi *Sms* ed *Mms* sono risultati compresi nell'attività di intercettazione.

All'esito dell'istruttoria e sulla base della documentazione pervenuta, l'Autorità ha prescritto ai gestori (*Prov. 15 dicembre 2005 [doc. web n. 1203890]*) di adottare alcuni accorgimenti e misure ulteriori nel proteggere i dati allorché adempiano alle menzionate richieste dell'autorità giudiziaria. Le misure riguardano sia gli aspetti organizzativi, sia la sicurezza dei flussi informativi diretti verso l'autorità giudiziaria, sia la protezione dei dati trattati a scopo di giustizia.