

**Relazione 2007 - 16 luglio 2008
Parte II - L'attività svolta dal Garante**[Indice generale](#)**10. Le attività economiche e i rapporti di lavoro**

L'Autorità ha continuato ad estendere il ventaglio delle aree di intervento ai diversi ambiti delle attività economiche e produttive. Tenuto conto dell'elevato numero di segnalazioni e reclami che continuano a pervenire, anche nel corso del 2007 si è preferito, ove possibile, considerare congiuntamente le segnalazioni aventi profili in comune formulando, specie in settori che coinvolgono larghe fasce della popolazione, linee-guida suscettibili di ampia applicazione, fornendo con esse indicazioni agli operatori economici. Tale è stato il caso dei trattamenti relativi al rapporto banca-clientela e quello del trattamento di dati personali nel contesto lavorativo mediante l'uso di risorse elettroniche (*e-mail* e Internet).

In pari tempo, l'Autorità ha fatto ulteriori passi avanti nella ricerca di forme di esonero o semplificazione nell'adempimento degli obblighi connessi alla protezione dei dati personali, individuando misure comunque atte ad assicurare la tutela dei dati personali: a tale proposito possono essere richiamati sinteticamente i provvedimenti correlati all'informativa da rendere nell'ambito della *cd.* "catena assicurativa", in occasione delle operazioni di cartolarizzazione o, ancora, dell'esecuzione di servizi di informazione al pubblico resi telefonicamente. Più in generale, con particolare riferimento alle piccole e medie imprese (comprese le attività artigianali), è stata predisposta una "Guida pratica" per facilitare gli operatori dei vari settori nell'adempimento degli obblighi che la normativa sulla *privacy* impone.

10.1. Settore bancario

Tra i settori nei quali più intensa è stata l'attività del Garante nel 2007 deve essere menzionato anche quello bancario: ciò, in relazione sia alla verifica del rispetto della disciplina di protezione dei dati e di decisioni adottate in passato dall'Autorità, sia alla formulazione di "Linee-guida", utili ad orientare l'attività degli operatori bancari e a fornire, rispetto ai profili di protezione dei dati, indicazioni alla clientela; la vicenda Swift (*v. infra*) ha focalizzato l'attenzione dell'Autorità anche in un'area sinora poco esplorata, quella del trattamento dei dati personali nell'ambito dei sistemi di pagamento.

Le "Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario" (*Prov. 25 ottobre 2007*, in *G.U.* del 23 novembre 2007 n. 273, [doc. web n. [1457247](#)]) sono state adottate al fine di fissare le garanzie per il corretto uso dei dati personali dei clienti da parte degli istituti bancari e degli operatori postali (quando operano nell'ambito bancario e finanziario) e introdurre alcune semplificazioni a vantaggio degli operatori (cioè, in particolare, in relazione alla cessione degli sportelli bancari).

**Linee-guida
per trattamenti
dati relativi
al rapporto
banca-clientela**

Oltre a ribadire la necessità di scrupoloso rispetto dei principi fondamentali in materia di protezione dei dati personali della clientela (pertinenza e non eccedenza, necessità e qualità e sicurezza dei dati), sono state evidenziate alcune modalità di trattamento che possono condurre ad accessi o utilizzazioni indebite: si pensi alla mancata adozione di idonee misure di sicurezza o, più semplicemente, all'inosservanza di "distanze di cortesia" nelle filiali bancarie, o, ancora, alla comunicazione di informazioni bancarie a terzi (compresi i familiari o il coniuge) non autorizzati dall'interessato a venirne a conoscenza.

Non pochi sono invece i casi, previsti dalla legge (che ne determina limiti e modalità) in cui la comunicazione di dati personali relativi a un cliente deve essere effettuata: ad esempio, la comunicazione in applicazione della disciplina in materia di anticiclaggio o di contrasto al terrorismo, quella a vantaggio della Centrale di allarme interbancaria (Cai) e della Centrale dei rischi della Banca d'Italia e, ancora, la comunicazione al creditore precedente nell'ambito di una procedura esecutiva (ai sensi degli artt. 543 ss. c.p.c.).

Permangono numerose le segnalazioni relative all'esercizio del diritto d'accesso da parte della clientela: il diritto previsto dall'art. 7 del Codice consente all'interessato di conoscere tutte le informazioni che lo riguardano detenute dalla banca (quali le operazioni bancarie effettuate), ma non il diritto di conoscere informazioni personali riferite a terzi ancorché coinvolti nell'operazione effettuata.

Anche nelle linee-guida il Garante ha ribadito, data la frequenza con la quale è dato assistere al ricorso indifferenziato ai rimedi previsti dal Codice, i caratteri distintivi tra il diritto di accesso ai dati personali detenuti da istituti di credito, disciplinato dagli artt. 7 ss. del Codice, e il diverso diritto di ottenere copia della documentazione bancaria (che può contenere o meno dati personali, peraltro riferiti sia all'interessato, sia a terzi) regolato dall'art. 119 d.lg. 1 settembre 2003, n. 385.

Nell'ambito delle linee-guida ha formato oggetto di trattazione anche la cessione di sportelli bancari, che comporta una comunicazione di dati personali relativi alla clientela (ma anche dei dati personali dei dipendenti degli sportelli ceduti) dalla banca cedente a quella cessionaria: a tale proposito l'Autorità ha dato ulteriore applicazione al principio del bilanciamento di interessi previsto dall'art. 24, comma 1, lett. *g*), del Codice (coerentemente al quadro normativo desumibile dalla disciplina di settore all'art. 58 del d.lg. 1 settembre 1993, n. 385), rendendo così lecita la comunicazione dei dati personali (diversi da quelli sensibili) oggetto della cessione degli sportelli bancari anche in assenza del consenso degli interessati. Con riguardo all'informativa cui sarebbe tenuta la banca cessionaria, sono stati ritenuti sussistenti i requisiti per esonerare dall'obbligo di rendere individualmente l'informativa agli interessati (art. 13, comma 5, lett. *c*), del Codice). Gli elementi indicati all'art. 13 del Codice dovranno pertanto essere resi noti agli interessati mediante la loro pubblicazione nella *Gazzetta Ufficiale* (come previsto, anche se a fini diversi, dal citato art. 58 del *Tub*) e (conformemente alla previsione contenuta nell'art. 13, comma 5, lett. *c*), del Codice) le banche che acquisiscono sportelli dovranno fornire ai soggetti ceduti l'informativa di cui all'art. 13, commi 1 e 2, del Codice alla prima occasione utile successiva all'avvenuta cessione (in armonia con quanto previsto dalle Istruzioni della Banca d'Italia).

Per verificare il rispetto delle prescrizioni impartite dal Garante nel *provvedimento* generale adottato il 27 ottobre 2005 [doc. web n. [1246675](#)] sul trattamento di immagini del volto e delle impronte digitali per accedere all'interno delle filiali (sul tema v. più ampiamente la *Relazione* 2005, p. 69), la Guardia di finanza, su incarico dell'Autorità, ha effettuato accertamenti nei confronti di sette banche (per complessive 34 filiali dislocate sul territorio nazionale, scelte in parte a campione, in parte a seguito di segnalazioni pervenute).

**Banche,
videosorveglianza
e registrazione
dell'immagine
delle
impronte digitali
presso
istituti bancari**

All'esito degli accertamenti, dai quali è emersa in molti casi una sostanziale legittimità dei trattamenti, il Garante ha adottato quattro provvedimenti contenenti prescrizioni per le banche presso le quali sono stati riscontrati profili di non conformità con la disciplina in materia (*Prov. 23* gennaio 2008 [doc. web nn. [1490533](#), [1490477](#), [1490463](#) e [1490382](#)]).

In particolare, nei confronti di un istituto di credito è emerso un utilizzo generalizzato dei sistemi biometrici (84 filiali su 92 presenti sul territorio nazionale, sono risultate infatti dotate di sistemi di rilevazione) in assenza di specifici elementi che, in base al *provvedimento* del 27 ottobre 2005, evidenziassero una concreta situazione di rischio per la banca (desumibile da alcuni indici, quali l'aver subito precedenti rapine, l'ubicazione in aree ad alta densità criminale o isolate o, comunque, poste nell'immediata prossimità di "vie di fuga"). Il Garante ha quindi prescritto a tale istituto bancario di rivalutare, alla luce della pertinente documentazione eventualmente acquisita presso le competenti autorità di pubblica sicurezza, l'effettiva necessità dei sistemi di rilevazione di impronte digitali e immagini della clientela.

In altri casi le prescrizioni impartite hanno riguardato la necessità di fornire alla clientela un'ideale informativa sulla presenza dei sistemi in parola, nonché di garantire l'accesso agli sportelli mediante modalità alternative (qualora il cliente non voglia o non possa rilasciare le proprie impronte).

Il Garante ha, infine, prescritto ad alcuni istituti bancari interessati dalle verifiche di adottare le misure necessarie, per limitare a una settimana dalla loro registrazione la conservazione delle informazioni raccolte.

Tra i profili oggetto di segnalazione si registra l'asserito accesso abusivo ad informazioni bancarie da parte di incaricati della banca (sovente con comunicazione dei dati a terzi).

**Accessi abusivi
a informazioni
personali
da parte
di incaricati**

L'accertamento può talora essere assai complesso: l'Autorità però ha dato corso a una segnalazione nella quale l'interessato, pur non essendo più cliente di una banca ormai da alcuni anni, era venuto a conoscenza dell'esistenza di accessi relativi al suo nominativo mediante il cd. "servizio di prima informazione" reso disponibile presso la Centrale dei rischi della Banca d'Italia e al sistema centralizzato di rilevazione dei rischi di importo contenuto gestito da Sia S.p.A.

In riscontro alla richiesta di informazioni inviata dal Garante, la banca ha ammesso (diversamente da quanto dichiarato in precedenza al segnalante), che dai controlli effettuati erano emersi accessi indebiti da parte di un dipendente per finalità di natura personale. Il Garante, con *provvedimento* dell'8 marzo 2007 [doc. web n. [1390872](#)], ha dichiarato illecito il trattamento di dati personali effettuato presso l'istituto di credito e ha prescritto al titolare del trattamento di adottare le misure di sicurezza atte a evitare accessi non autorizzati o trattamenti non conformi alle legittime finalità perseguite dall'istituto di credito; sono state inoltre prescritte misure idonee a consentire controlli più tempestivi ed efficaci sull'effettiva correlazione tra l'accesso ai predetti sistemi informativi e la documentabile necessità di trattare affari che lo giustificano. Il Garante ha pure invitato la banca ad assicurare un riscontro veritiero e tempestivo agli interessati che presentano richieste di accesso ai propri dati personali ai sensi dell'art. 7 del Codice (circostanza che non si era verificata nel caso di specie), disponendo altresì la trasmissione degli atti e di copia del *provvedimento* all'autorità giudiziaria per le valutazioni di competenza in ordine alla sussistenza di illeciti penalmente rilevanti eventualmente configurabili.

L'Autorità ha continuato a seguire, anche partecipando alle riunioni del sottogruppo stabilito nell'ambito del Gruppo dei Garanti europei, il "caso Swift" (v. *Relazione* 2006, p. 162). La vicenda, come noto, si riferisce a un programma di monitoraggio delle transazioni finanziarie che utilizzano il sistema fornito da Swift (Società per le telecomunicazioni finanziarie interbancarie mondiali stabilita in Belgio) da parte delle autorità statunitensi che, nell'ambito delle iniziative adottate per contrastare il terrorismo ("*Terrorism finance tracking programme*"), avrebbero avuto accesso, con tecniche di data *mining*, fin dall'autunno del 2001 ai dati personali di coloro che effettuano transazioni finanziarie internazionali.

La vicenda Swift

Nell'ambito dei negoziati condotti con le autorità Usa dal vice presidente della Commissione europea Franco Frattini per rinvenire una soluzione condivisa dei profili critici sollevati dal caso, le autorità di protezione europee riunite nel Gruppo art. 29 hanno evidenziato la necessità di soluzioni efficaci e non di una mera "legalizzazione" dell'esistente, individuando le garanzie necessarie affinché lo scambio di informazioni con le autorità statunitensi si possa svolgere nel rispetto della disciplina contenuta nella direttiva 95/46/Ce.

In relazione ai profili critici affrontati nel parere del Gruppo (n. 10/2006 del 22 novembre 2006, WP 128) (in particolare riguardo all'inosservanza della disciplina sul flusso transfrontaliero dei dati personali trattati attraverso *SwiftNet* e temporaneamente memorizzati in un *mirror server* situato negli Stati Uniti d'America, oltre al mancato rispetto del principio di proporzionalità), la succursale americana di Swift (per rendere legittimo il trasferimento di dati verso gli Usa) ha chiesto e ottenuto dalle autorità statunitensi di poter aderire al cd. "*Safe Harbor*" (v. *Relazione* 2002, p. 129) incrementando in pari tempo la trasparenza delle operazioni di trattamento effettuate grazie alla predisposizione di una informativa per le banche e gli altri organismi clienti.

Inoltre, in una prospettiva di medio termine (entro la fine del 2009), Swift provvederà a modificare l'architettura del proprio sistema, conservando nel *mirror server* situato negli Usa solo le transazioni dirette verso quel Paese e parte delle restanti transazioni (riferite ad altri Paesi che scegliessero di far capo ad esso); il *mirroring* dell'intero *database* sarebbe collocato in un Paese europeo. Nel frattempo le autorità americane potranno continuare ad attingere, con le modalità in uso, all'intero *database*.

Nel contesto nazionale, il Garante -nell'ambito di un'attività concordata con le autorità di protezione degli altri Paesi europei- ha richiesto notizie utili oltre a Swift Italia, anche al Ministero dell'economia e delle finanze, all'Abi e alla Banca d'Italia.

Si è così appurato che le banche si limitano a comunicare a Swift i dati forniti dalla clientela solo per le operazioni bancarie richieste dalla stessa; tramite l'associazione di categoria è stata messa in luce l'estraneità del sistema bancario rispetto alle decisioni assunte da Swift nella localizzazione di un proprio *mirror server* negli Stati Uniti. Con particolare riferimento all'informativa da rendersi alla clientela in ordine alla possibilità di un trasferimento dei dati verso gli Stati Uniti, con il conseguente rischio di accesso ai medesimi da parte delle

autorità statunitensi, Abi ha sottoposto all'Autorità un *fac-simile* di informativa inoltrato successivamente alle banche associate; da primi riscontri è emerso che, con modalità diverse, tale informativa viene resa alla clientela.

L'intera vicenda ha coinvolto anche le banche centrali, sia quella europea, sia quelle nazionali, mettendo in evidenza la necessità di una vigilanza più penetrante su Swift, società che non essendo né un sistema di pagamento, né un intermediario finanziario, non sarebbe allo stato sottoposta a vigilanza, ma a una (meno incisiva) forma di supervisione (*cd. "oversight"*) il cui coordinamento sarebbe rimesso alla Banca centrale del Belgio (*cd. "lead overseer"*). A seguito dell'accaduto, la Banca d'Italia ha rappresentato che le banche centrali del Sebco hanno avviato una riflessione comune, per giungere a un approccio condiviso che tenga conto del ruolo di Swift nel sistema dei pagamenti a livello globale, nonché nell'ambito del nuovo sistema unico europeo dei pagamenti (Sepa), nel quadro della direttiva 2007/64/Ce sui servizi di pagamento, da recepire entro il 1 novembre 2009.

Tra le iniziative volte alla realizzazione di un'area europea dei pagamenti (Sepa), l'Associazione bancaria italiana ha interessato l'Autorità sulle misure di aggiornamento "massivo" degli archivi del sistema bancario, al fine di sostituire le "vecchie" coordinate bancarie della clientela con un codice internazionale (*International banking account number - Iban*) che individui in modo univoco i conti correnti. L'*Iban* (il cui utilizzo per i bonifici transfrontalieri è previsto come obbligatorio dal 2003 già nel Regolamento n. 2560/2001 del Parlamento europeo e del Consiglio) è un codice alfanumerico composto da 27 caratteri: 23 dei quali sono le attuali coordinate bancarie alle quali vengono aggiunti ulteriori 4 caratteri: 2 individuano il codice del Paese presso il quale è detenuto il conto (*ad es.*, IT corrisponde a Italia) e due rappresentano un codice di controllo internazionale.

Iban
(**International banking account number**)

La procedura che l'Abi ha rappresentato al Garante per realizzare tale progetto prevede l'allineamento degli archivi tra imprese e banche per l'acquisizione delle autorizzazioni all'addebito rilasciate dal correntista e l'allineamento degli archivi tra Ministero dell'economia e finanze e banche (tramite la Banca d'Italia) per il pagamento di stipendi e pensioni domiciliati di dipendenti pubblici sui propri conti correnti bancari tramite bonifico.

All'esito degli approfondimenti svolti, l'Autorità ha ritenuto che la procedura elettronica configurasse un mero aggiornamento delle coordinate bancarie dei correntisti (già detenute dalle banche) e rientrasse quindi nell'ambito dell'esecuzione del rapporto contrattuale già in essere; si è ritenuta perciò sufficiente l'informativa resa già alla clientela prima dell'avvio della procedura, senza che fosse necessario provvedere a reiterarla (*Nota* 10 aprile 2007).

Si segnala, infine, la collaborazione con la Banca d'Italia in vista dell'attuazione della disciplina prevista dall'art. 53, comma 2-ter, del d.lg. 1 settembre 1993, n. 385 (introdotta dalla l. 23 febbraio 2007, n. 15, di conversione del decreto legge n. 27 dicembre 2006, n. 297, per il recepimento delle direttive 2006/48/Ce e 2006/49/Ce). La disposizione, da attuare con regolamento della Banca d'Italia previo parere dell'Autorità, prevede che i soggetti che rilasciano alle banche valutazioni del rischio di credito o sviluppano modelli per la valutazione dell'adeguatezza patrimoniale, possano conservare, per tale esclusiva finalità (anche in deroga alle altre vigenti disposizioni normative), i dati personali detenuti legittimamente per un periodo di osservazione ulteriore, che sia congruo secondo criteri dettati dalla Banca centrale.

Attuazione dell'art. 53, comma 2-ter, del d.lg. 1 settembre 1993, n. 385

Tale prolungata conservazione dovrà tuttavia avvenire secondo modalità che assicurano la non identificabilità delle informazioni; nonostante la collaborazione con la Banca d'Italia, emerge al riguardo la difficoltà di assicurare l'univocità delle informazioni riferite agli interessati e il necessario, progressivo aggiornamento delle stesse (necessari per dare effettiva attuazione alle previsioni contenute negli accordi di Basilea II) unitamente alla "non identificabilità" prescritta dal legislatore.

10.2. Settore assicurativo

Le compagnie di assicurazione più rappresentative in termini di quote di mercato sono state oggetto di una verifica congiunta a livello europeo relativa al rispetto dei principi in materia di protezione dati (*v. par.* 20.1).

L'informativa sul trattamento dei dati personali e la cd. "catena assicurativa"

A livello nazionale il settore assicurativo, tramite l'Associazione nazionale fra le imprese assicurative (Ania), aveva per altro già richiesto l'individuazione di modalità più snelle per l'adempimento dell'obbligo dell'informativa (ora previsto dall'art. 13 del Codice). In ragione della complessità delle attività connesse alla gestione del contratto assicurativo, con specifico riferimento alla pluralità di soggetti (persone fisiche e giuridiche, operanti in Italia e all'estero) che possono venire a conoscenza delle informazioni relative a una specifica posizione assicurativa, tale problematica, nota con la locuzione di "catena assicurativa", ha infine formato oggetto del *provvedimento* del 26 aprile 2007 [doc. web n. [1410057](#)].

Con esso, anche ai sensi dell'art. 13, comma 5, lett. c), del Codice, il Garante ha autorizzato le imprese assicurative stipulanti (titolari del trattamento) a rendere l'informativa alla clientela *una tantum*, in sede di conclusione del contratto di assicurazione, anche nell'interesse dei diversi soggetti che, in qualità di autonomi titolari del trattamento, utilizzano dati personali relativi al medesimo rischio assicurato.

L'Ania aveva sottolineato che l'informativa da parte di ciascun titolare del trattamento operante all'interno della catena assicurativa avrebbe comportato modalità complesse di realizzazione, oltre che costi e impegni amministrativi sproporzionati rispetto al diritto tutelato, considerato anche che, il più delle volte, i soggetti che a vario titolo partecipano alla catena assicurativa non hanno alcun contatto diretto con l'interessato e ricevono i dati dall'assicuratore. Anche per la clientela sarebbe stato preferibile conoscere mediante un'informativa fornita in un unico contesto i diversi ambiti di circolazione delle informazioni personali relative al medesimo rischio assicurato.

Di tali aspetti il Garante ha tenuto conto nell'adozione, ai sensi dell'art. 13, commi 3 e 5, del Codice (e tenendo in considerazione la previsione contenuta nell'art. 13 della direttiva 95/46/Ce oltre alle indicazioni formulate dalla Raccomandazione del Consiglio d'Europa R(2002)9, del 18 settembre 2002), del menzionato *provvedimento* del 26 aprile 2007 volto a semplificare, nel rispetto della disciplina di protezione dei dati personali, alcuni adempimenti gravanti sulle imprese del settore assicurativo.

Il Garante ha comunque precisato che l'informativa non deve essere resa da parte dei (numerosi) soggetti che, nelle *cd. "fasi assuntiva e liquidativa"*, vengono a operare quali "responsabili del trattamento". Anche alla luce di tale considerazione, le imprese di assicurazione devono però valutare con attenzione la funzione effettivamente svolta dai soggetti che vengono chiamati a cooperare (o ad operare) nell'ambito della catena assicurativa per dare esecuzione alla medesima prestazione.

Infatti, solo in presenza di un reale ed autonomo potere decisionale in ordine alle finalità del trattamento, soggetti appartenenti alla *cd.*

"catena assicurativa" opereranno quali "titolari del trattamento" ai sensi degli artt. 4, comma 1, lett. f) e 28 del Codice. Diversamente è appropriato ricorrere, con la necessaria designazione di tali ausiliari, a "responsabili del trattamento" (cfr. Provv. 19 dicembre 1998 [doc. web n. [41941](#)]): si pensi, ad esempio, a soggetti che operano nella fase precontrattuale senza effettiva autonomia decisionale in ordine alle finalità del trattamento, ad esempio produttori o agenti; o, ancora, a soggetti che operano quali ausiliari dell'assicurazione in sede di distribuzione dei prodotti assicurativi o che operano quali *outsourcers* per determinate operazioni (per assicurare taluni servizi informatici, di archiviazione, di liquidazione sinistri, di posta, di manutenzione, di tipografia, ecc.).

Come già chiarito in passato, l'informativa dovrà riferirsi a tutte le operazioni necessarie per la corretta esecuzione al rapporto contrattuale, nonché agli altri trattamenti che (talora anche in base a esplicite previsioni di legge) possono essere effettuati lecitamente (v. già Provv. 28 maggio 1997 [doc. web n. [40425](#)]); essa dovrà illustrare i flussi comunicativi e indicare con precisione le finalità in concreto perseguite dalla compagnia di assicurazione, i soggetti o le tipologie di soggetti ai quali i dati possono essere comunicati (in qualità di autonomi titolari del trattamento) o che possono venire a conoscenza quali "responsabili del trattamento".

Per evitare un impiego di mezzi sproporzionato rispetto al diritto tutelato (Prov. 26 novembre 1998 [doc. web n. [39624](#)]), con il provvedimento in esame il Garante ha individuato modalità semplificate affinché l'assicurazione stipulante possa fornire un'ideonea informativa anche nell'interesse degli altri titolari del trattamento (con particolare riferimento ai coassicuratori e ai riassicuratori), in relazione a un medesimo rischio assicurato: questi ultimi, ai sensi del predetto art. 13, comma 5, lett. c), sono così esonerati dall'obbligo di fornire un'autonoma informativa sul trattamento già reso noto all'interessato, a condizione che "i medesimi titolari del trattamento siano già individuati univocamente nell'informativa resa anche nel loro interesse dall'impresa assicuratrice stipulante o siano comunque individuabili presso quest'ultima" e che "l'informativa sia formulata in modo da esplicitare univocamente anche le eventuali finalità ulteriori rispetto alla sola gestione del rischio assicurato perseguite da detti titolari del trattamento".

Con il provvedimento il Garante ha altresì fornito ulteriori precisazioni in ordine alla modulistica, per le ipotesi in cui sia necessario il consenso dell'interessato. Salva infatti l'ipotesi in cui esso non è richiesto –quando i dati sono necessari (per instaurare o) per dare esecuzione a un contratto di assicurazione (art. 24, comma 1, lett. b), del Codice), oppure in quanto gli stessi sono trattati sulla base di uno dei presupposti di cui all'art. 24 del Codice nei casi in cui il consenso dell'interessato sia comunque necessario (ad es., per il trattamento dei dati sensibili)– l'impresa assicuratrice stipulante potrà limitare la formula di consenso ai soli trattamenti da essa effettuati, oppure formularla in modo da ricomprendere, nei limiti del medesimo rischio assicurato, anche gli specifici trattamenti ulteriori effettuati da altri "titolari" appartenenti alla catena assicurativa chiaramente individuabili nell'informativa resa.

Da ultimo, in considerazione del particolare ruolo svolto dai riassicuratori –che non instaurano un rapporto contrattuale con i soggetti coinvolti nel contratto di assicurazione– il Garante ha stabilito che l'eventuale comunicazione di dati (ad eccezione dei dati di natura sensibile) da parte della compagnia assicuratrice al riassicuratore rientra nell'ambito di applicazione dell'istituto del bilanciamento degli interessi tenuto conto del legittimo interesse dei titolari del trattamento coinvolti, e non richiede pertanto il consenso dell'interessato (art. 24, comma 1, lett. g), del Codice).

Interpellato dall'Ania, il Garante è tornato a occuparsi dell'esonero dall'obbligo di notificazione preventiva ai sensi dell'art. 37 del Codice da parte delle imprese assicuratrici (Nota 9 agosto 2007). Con specifico riferimento ai trattamenti di dati personali della clientela che nella fase precontrattuale comportino la profilazione del contraente, necessari in base alla nuova disciplina dell'offerta dei prodotti finanziari per garantire l'adeguatezza dell'offerta dei prodotti assicurativi, l'Autorità ha precisato che per tali trattamenti non è necessaria la notificazione ai sensi dell'art. 37, comma 1, lett. d) del Codice (art. 1, comma 1, lett. w-bis, 21, comma 1 e 25-bis del d.lg. 24 febbraio 1998, n. 58, testo unico delle disposizioni in materia di intermediazione finanziaria).

Prodotti finanziari emessi da imprese di assicurazione e notificazione del trattamento

Con deliberazione del Garante del 31 marzo 2004 (doc. web n. [852561](#)) l'Autorità aveva infatti stabilito che l'esenzione concerne i trattamenti dei dati personali "che non siano fondati unicamente su un trattamento automatizzato volto a definire il profilo di un investitore, effettuati esclusivamente per adempiere a specifici obblighi previsti dalla normativa in materia di intermediazione finanziaria".

10.3. Rapporti di lavoro e previdenza

10.3.1. Rapporto di lavoro in ambito pubblico

L'attività dedicata nel 2007 al trattamento di dati personali dei dipendenti da parte dei datori di lavoro pubblici è stata particolarmente intensa. L'esame di un consistente numero di segnalazioni, reclami, quesiti e richieste di parere, spesso di tenore similare, ha consentito di elaborare un documento di sintesi su problematiche sollevate di frequente da amministrazioni pubbliche, dipendenti e organizzazioni sindacali.

Con le "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (Prov. 14 giugno 2007 [doc. web n. [1417809](#)]), nel quadro della tendenziale uniformità dei principi applicabili al rapporto di lavoro, sono state evidenziate alcune specificità del trattamento effettuato da soggetti pubblici, in qualità di datori di lavoro, indicando le misure e gli accorgimenti cui essi devono attenersi nel trattamento dei dati personali di lavoratori.

Le Linee-guida del Garante

In termini generali il datore di lavoro pubblico può trattare lecitamente i dati personali dei lavoratori necessari per la corretta gestione del rapporto di lavoro, avendo cura di applicare le previsioni che riguardano le proprie funzioni istituzionali o il rapporto di lavoro, contenute in atti normativi o contrattuali, in modo da avvalersi in piena trasparenza di informazioni personali e modalità di trattamento proporzionate ai singoli scopi (artt. 3, 11, 13 e 18 Codice).

L'amministrazione deve adottare particolari cautele nella trasmissione –tra uffici del medesimo ente o verso soggetti esterni preposti al trattamento (artt. 29 e 30 del Codice)– di informazioni personali riferite ai propri dipendenti, selezionando quelle di volta in volta indispensabili, ed evitando, in linea di principio, i riferimenti puntuali a particolari condizioni personali, specie se riguardanti la salute (artt. 11 e 22 del Codice). Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'ente pubblico deve inoltre adottare forme di comunicazione con lo stesso dipendente protette e individualizzate: inoltrando le note in busta chiusa, inviandole all'e-mail personale o invitandolo a ritirare personalmente la documentazione.

Particolare attenzione deve essere posta nei rapporti con le organizzazioni sindacali, avendo cura che il rispetto degli obblighi di informativa, consultazione, concertazione e contrattazione sia ispirato ai principi di necessità e proporzionalità nella comunicazione di informazioni ai sindacati (artt. 3 e 11 del Codice). Salvi casi specifici in cui la normativa contrattuale preveda espressamente la comunicazione alle medesime organizzazioni di dati nominativi, le amministrazioni possono, infatti, fornire solo dati numerici o aggregati e non anche informazioni riferibili a uno o più lavoratori individuabili, per verificare la corretta attuazione di taluni atti organizzativi.

A parte quanto eventualmente previsto per specifiche categorie di atti, le amministrazioni, sulla base di apposite disposizioni normative, possono avvalersi delle potenzialità offerte dalle nuove tecnologie per mettere a disposizione del pubblico atti e documenti contenenti dati personali, purché ne assicurino l'esattezza, l'aggiornamento e la pertinenza, garantendo altresì agli interessati il "diritto all'oblio" (mediante forme adeguate di selezione delle informazioni che, trascorso un certo periodo dalla pubblicazione, non consentano di

rintracciare i loro dati personali tramite motori di ricerca esterni). È in ogni caso vietata la diffusione di informazioni sulla salute di lavoratori o familiari interessati.

Le nuove tecnologie possono facilitare anche le comunicazioni dell'amministrazione con gli interessati, come ad esempio in occasione di concorsi o selezioni pubbliche: in tali casi vanno riportati nelle graduatorie da pubblicare (indipendentemente dal mezzo utilizzato per la diffusione) soltanto dati pertinenti (elenchi nominativi abbinati ai risultati, elenchi di ammessi alle prove scritte o orali, con l'esclusione di altre informazioni quali recapiti telefonici, codice fiscale ecc.).

Anche nel pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare tali sistemi di rilevazione solo in presenza di esigenze che impongano l'adozione di elevati e specifici livelli di sicurezza (aree adibite alla sicurezza dello Stato, torri di controllo, conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, notificazione al Garante, esclusione di archivi centralizzati, codice cifrato dell'impronta memorizzato solo nel *badge* del dipendente, informativa specifica agli interessati).

Dati sensibili o giudiziari possono essere utilizzati per attuare la normativa in materia di instaurazione e gestione di rapporti di lavoro, nonché per finalità di formazione o per concedere benefici economici e altre agevolazioni (artt. 95, 68, 112 del Codice). Il loro trattamento va limitato alle sole informazioni e operazioni previste negli atti regolamentari conformi al parere del Garante applicabili a ciascuna amministrazione (artt. 20, 21 e 154 del Codice).

In particolare, nei casi di assenza per malattia, vanno consegnati all'amministrazione certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio pubblico deve astenersi dall'utilizzare queste informazioni e deve invitare a non produrre altri certificati con le stesse caratteristiche. Particolari cautele devono essere inoltre adottate dall'ente pubblico che tratti dati sulla salute dei dipendenti nei casi di visite medico legali, denunce di infortunio all'Inail, abilitazioni al porto d'armi e alla guida.

Le linee-guida sul pubblico impiego hanno reso possibile all'Ufficio fornire indicazioni e orientamenti di carattere generale in relazione a specifiche istanze pervenute.

L'Ufficio ha ad esempio interessato diversi organismi sanitari sulle garanzie da osservare nella trasmissione ai datori di lavoro pubblici dei verbali di visita relativi agli accertamenti di idoneità al servizio dei rispettivi dipendenti (v., *ad es.*, *Nota* 18 dicembre 2007). In particolare è stato evidenziato che il datore di lavoro può conoscere non le eventuali patologie accertate, ma la sola valutazione finale circa l'idoneità del dipendente allo svolgimento di date mansioni. I collegi medici devono quindi trasmettere all'amministrazione di appartenenza dell'interessato il verbale relativo all'accertamento con la sola indicazione del giudizio-medico legale di idoneità o inidoneità, anche parziale, al servizio. Il datore di lavoro, inoltre, qualora sia destinatario di atti di accertamento recanti ulteriori informazioni riferite al lavoratore, non può, comunque, utilizzarle ulteriormente (art. 11, comma 2, del Codice).

Con riferimento alla casistica individuale, l'Ufficio ha esaminato una segnalazione riguardante l'affissione in bacheca sindacale, senza il consenso degli interessati, di una missiva della rappresentanza sindacale unitaria dal contenuto apparentemente lesivo della riservatezza. Tale trattamento è in termini generali lecito nell'esercizio del diritto riconosciuto ai soggetti sindacali, individuati nel contratto collettivo applicabile, di affiggere "testi e comunicati inerenti a materie di interesse sindacale e del lavoro" negli appositi spazi predisposti dall'amministrazione in luoghi accessibili a tutto il personale all'interno dell'unità operativa (art. 25, l. 20 maggio 1970, n. 300; artt. 3 e 10, ccnq sulle modalità di utilizzo dei distacchi, aspettative e permessi, nonché delle altre prerogative sindacali del 7 agosto 1998).

Pubblicazione di corrispondenza in bacheca

I trattamenti di dati personali effettuati per tale finalità, rientrano tra quelli volti a concretizzare la libera manifestazione del pensiero (v. Cass. 24 maggio 2001, n. 7091; Cass. 22 ottobre 1998, n. 10511; Cass. 22 agosto 1997, n. 7884; Trib. Viterbo 19 dicembre 2005) e sono pertanto consentiti anche in assenza del consenso delle persone interessate, purché nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli interessati, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali (artt. 2 e 21 Cost.; artt. 2, 11 e 136 ss. del Codice). Secondo la giurisprudenza, inoltre, la qualificazione di un testo come inerente a "materie di interesse sindacale e del lavoro" deriva dalla circostanza che esso abbia formato oggetto di scelta da parte del sindacato, fermi restando i limiti della provenienza del materiale affisso dai soggetti legittimati, nonché quelli inerenti al rispetto del decoro, della reputazione e dell'onore degli interessati (art. 2 Cost.; Cass. 23 marzo 1994, n. 2808).

Prima di affiggere in bacheca un documento contenente dati personali i soggetti sindacali devono in particolare valutare la necessità, pertinenza e non eccedenza dei dati trattati (artt. 3 e 11 del Codice) rispetto alle finalità perseguite, garantendo agli interessati il "diritto all'oblio" trascorso un certo periodo di tempo dal verificarsi delle vicende dalle quali è originata l'affissione (*Nota* 23 gennaio 2008).

In un altro caso l'Ufficio è stato chiamato a valutare la liceità della comunicazione tra amministrazioni comunali limitrofe di informazioni sanitarie fornite a un comune per attestare la propria inidoneità fisica da un conducente di taxi, il quale, in un concorso successivamente bandito dallo stesso comune, era risultato socio di una società che svolgeva servizio di noleggio con conducente in comuni limitrofi.

Comunicazione di dati sensibili tra enti locali

Al riguardo è stato evidenziato che, in linea generale, ciascun ente comunale, anche per il tramite della Polizia municipale, è legittimato a verificare i requisiti previsti dalla legge e dal proprio regolamento per il rilascio di licenze e autorizzazioni per i servizi di taxi e noleggio con conducente (artt. 4 e 5 della legge l. 15 gennaio 1992, n. 21 e artt. 2, 16 e 32 del regolamento comunale applicabile). Tuttavia, la normativa in materia di trasporto di persone mediante autoservizi pubblici non di linea prevede che eventuali accertamenti relativi all'esercizio abusivo di tale attività vengano trasmessi soltanto a determinati soggetti tra i quali la Motorizzazione civile e non anche alle altre amministrazioni comunali limitrofe (artt. 4, comma 2, e 6, comma 5, l. 15 gennaio 1992, n. 21; artt. 5, c. 4, lett. b) e 12, l. regionale applicabile).

Dal momento che nel caso in esame il trattamento dei dati sanitari dell'interessato non trovava fondamento nella disciplina di settore, né in altra disposizione idonea a legittimarla (art. 20 del Codice, regolamento comunale sul trattamento dei dati sensibili e giudiziari), l'Ufficio ha rilevato che tali dati, ai sensi dell'art. 11, comma 2, del Codice non potevano più essere utilizzati dal comune (*Nota* 27 febbraio 2008). È stato pertanto considerato inibito ogni ulteriore trattamento dei dati riferiti all'interessato con l'eccezione della conservazione, in quanto presupposto essenziale dell'atto con cui era stata precedentemente autorizzata la cessione ad un altro soggetto della sua licenza per il servizio di taxi.

A seguito di una comunicazione ai sensi dell'art. 39, comma 1, lett. a), del Codice, l'Autorità è stata chiamata a valutare la conformità al Codice dell'iniziativa di una prefettura di costituire una rete socio-istituzionale per contrastare il lavoro irregolare nell'edilizia privata tramite un sistema informatico volto a consentire alle amministrazioni comunali, al comitato paritetico territoriale e agli organi di controllo e di vigilanza di condividere una serie di informazioni relative ai cantieri di lavori di edilizia privata.

Rete socio-istituzionale di contrasto al lavoro

irregolare

Al riguardo, l'Ufficio ha precisato che la prefettura può accedere al sistema informativo e utilizzare i dati ivi registrati con modalità e per finalità definite in autonomia, soltanto ove ravvisi, tra le sue finalità istituzionali, specifici profili di competenza in materia di indirizzo e coordinamento delle attività di contrasto del lavoro irregolare che non potrebbero essere altrimenti realizzati (artt. 3, 18 e 28 del Codice; art. 1 d.lg. 23 aprile 2004, n. 124; art. 13 l. 1 aprile 1981, n. 121). L'amministrazione, infatti, non può avvalersi di tale sistema per perseguire attività che la disciplina di settore conferisce specificamente ad altri soggetti coinvolti nell'iniziativa, ovvero agli organi di polizia (art. 14 l. 1 aprile 1981, n. 121; art. 5, comma 2, d.lg. 23 aprile 2004, n. 124). L'Ufficio non ha, invece, ravvisato alcun ostacolo in ordine alla possibilità che la prefettura svolga rispetto al sistema informativo le funzioni di amministratore di sistema, in qualità di "responsabile del trattamento" (art. 29 del Codice) (*Nota* 28 febbraio 2008).

In seguito a una segnalazione inoltrata da alcune organizzazioni sindacali, un'azienda sanitaria, su sollecitazione dell'Ufficio (*Nota* 12 dicembre 2007), ha provveduto a adottare opportune cautele nelle modalità di consegna ai propri dipendenti dei *cd.* "cedolini" dello stipendio inserendoli in busta chiusa. L'Ufficio ha ricordato che all'atto della consegna tali documenti andrebbero imbustati, ovvero piegati e spillati, o coperti nelle parti che non riportano informazioni di comune conoscenza, per limitare l'immediata accessibilità delle informazioni ivi contenute al solo interessato e agli incaricati del trattamento (*Parere* 31 dicembre 1998 [doc. web n. [39324](#)], *Prov. v.* 31 ottobre 2007 [doc. web n. [1459297](#)]).

**Modalità
di consegna
dei "cedolini"
dello stipendio**

Nel riscontrare taluni quesiti sull'applicabilità alle regioni, agli enti, alle agenzie o alle società a partecipazione regionale del regime di pubblicità degli incarichi e dei compensi conferiti dalle amministrazioni pubbliche (art. 1, comma 593, legge 27 dicembre 2006, n. 296), l'Ufficio ha richiamato le specifiche direttive fornite dalla Presidenza del Consiglio dei ministri (*Nota* 28 novembre 2007). In particolare, la Presidenza ha chiarito che sono estranei al campo di applicazione della suddetta disciplina gli enti di autonomia territoriale (per i quali vigono tuttavia gli specifici obblighi di pubblicità di cui all'art. 1, comma 725, della legge finanziaria 2007) e tutti gli enti non riconducibili all'apparato dello Stato, quali le aziende sanitarie locali (dir. P.C.m. del 16 marzo 2007 pubblicata in *G.U.* 3 luglio 2007, n. 152).

**Regime
di pubblicità
degli incarichi
e dei compensi
conferiti dalle
amministrazioni
pubbliche**

Per quanto riguarda richieste di accesso formulate da associazioni sindacali ad atti contenenti le informazioni relative ai predetti incarichi e compensi, è stato evidenziato che la disciplina in materia di protezione dei dati personali non pone ostacoli di fondo all'applicazione delle disposizioni in materia di accesso ai documenti amministrativi (art. 59 del Codice). Spetta a ciascuna amministrazione, destinataria di un'istanza di accesso, verificare, caso per caso, l'interesse e i motivi sottesi alla richiesta, nonché valutare la sussistenza di una delle ragioni per le quali i documenti possano eventualmente essere sottratti in tutto o in parte alla conoscibilità dell'istante, (artt. 22 ss. l. 7 agosto 1990, n. 241; art. 6 d.p.R. 12 aprile 2006, n. 184).

Nell'istruttoria preliminare di un reclamo, con il quale un dipendente comunale lamentava che l'amministrazione aveva affisso all'albo pretorio una delibera di concessione del patrocinio legale contenente alcune informazioni riguardanti la vicenda giudiziaria nella quale era coinvolto, l'Ufficio ha ribadito quanto precisato in più occasioni dall'Autorità circa l'applicazione delle previsioni normative sulla pubblicità delle deliberazioni degli enti locali (art. 124 d.lg. 18 agosto 2000, n. 267).

**Affissione
all'albo
di delibere
riferite
a dipendenti**

Nel ricordare che l'amministrazione deve selezionare le informazioni effettivamente necessarie per perseguire, nei singoli casi, le finalità di trasparenza dei propri organi, specie se si tratti di dati sensibili e giudiziari (artt. 11 e 22, commi 3 e 5, del Codice), l'Ufficio ha sottolineato che vanno rivalutate con estrema attenzione le stesse tecniche di redazione delle deliberazioni e dei loro allegati, menzionando ad esempio tali dati solo negli atti a disposizione degli uffici, adoperando espressioni di carattere generale o utilizzando, eventualmente, codici numerici (*cf.* *Prov. v.* 19 aprile 2007 [doc. web n. [1407101](#)]).

A seguito dell'intervento dell'Ufficio (*Nota* 12 ottobre 2007), l'ente locale ha affermato di aver adottato le misure suggerite dall'Autorità.

In un altro reclamo, riguardante la pubblicazione, all'albo di un consorzio, di deliberazioni commissariali relative a provvedimenti disciplinari emessi a carico del reclamante, l'Ufficio non ha invece rilevato generali profili di illiceità del trattamento dei dati dell'interessato effettuato dal consorzio (*Nota* 12 febbraio 2008) alla luce della pertinente disciplina del Codice (artt. 23 e 24, comma 1, lett. a)) sulla diffusione di dati comuni da parte di enti pubblici economici, e della vigente normativa in materia di adozione di provvedimenti disciplinari e di doverosa pubblicazione delle delibere degli organi consortili (art. 7 l. 20 maggio 1970, n. 300; art. 22 e art. 1, all. h), ccnl per i dirigenti dei consorzi di bonifica del 29 marzo 2006; art. 60 r.d. 13 febbraio 1933, n. 215; art. 57 dello statuto del consorzio).

Nel caso esaminato, infatti, non è stato ritenuto in contrasto con i principi di pertinenza e non eccedenza dei dati trattati la menzione, negli atti pubblicati all'albo, del numero di matricola dell'interessato in luogo dei suoi dati nominativi (art. 11 del Codice; *Prov. v.* 12 gennaio 2004 [doc. web n. [1053395](#)]; *Prov. v.* 23 novembre 2006 [doc. web n. [1364099](#)]).

Sono state completate le verifiche tecniche, avviate dalla Guardia di finanza su richiesta dell'Autorità, nell'ambito di un procedimento ai sensi dell'art. 154 del Codice, per accertare se i test utilizzati nell'ambito delle diverse procedure di reclutamento contengano riferimenti e informazioni relative a dati sensibili. Alla luce degli elementi acquisiti l'Autorità sta verificando la liceità dei questionari in uso in relazione al divieto di trattare informazioni sensibili nell'ambito di test psico-attitudinali volti a definire la personalità dell'interessato di cui all'art. 22, comma 10, del Codice.

**Forze armate
e di polizia**

A seguito di una segnalazione pervenuta all'Autorità sono state fornite indicazioni a una questura riguardo alla gestione dei certificati medici degli appartenenti alla polizia di stato. È stato precisato in particolare che l'amministrazione, anche nei casi in cui sia autorizzata a raccogliere documentazione medica recante l'indicazione della diagnosi, insieme a quella della prognosi, a giustificazione delle assenze per malattia (art. 61 d.P.R. 28 ottobre 1985, n. 782; decreto del Ministro dell'interno 21 giugno 2006, n. 244), deve rispettare anzitutto i principi di necessità e indispensabilità nel trattamento dei dati sulla salute (artt. 3 e 22 del Codice). Il trattamento di dati relativi alla diagnosi contenuti nei certificati medici prodotti dagli interessati va circoscritto ai soli uffici per i quali la conoscenza di tali dati risulti indispensabile e, segnatamente, a quelli sanitari. Gli uffici di appartenenza del dipendente devono astenersi dal raccogliere tali informazioni (*Nota* 4 aprile 2007).

10.3.2. Rapporto di lavoro in ambito privato

Tenuto conto delle segnalazioni pervenute negli anni e dei ricorsi presentati nel 2006 con riguardo alla delicata tematica del contemperamento, nel contesto del rapporto di lavoro, dei diritti fondamentali e della dignità dei lavoratori con le legittime prerogative datoriali, l'Autorità, come anticipato nella *Relazione* 2006, ha adottato proprie linee-guida dedicate al trattamento dei dati personali effettuato in corrispondenza dell'utilizzo della posta elettronica e di Internet ("*Linee-guida del Garante per posta elettronica e Internet*",

Prov. 1 marzo 2007 [doc. web n. [1387522](#)].

Nell'adozione delle "Linee-guida per posta elettronica ed Internet" si è tenuto conto di un quadro normativo che rischia talora di dover inseguire le evoluzioni tecnologiche del settore (profilo peraltro emerso nel corso degli incontri tecnici avvenuti con Abi e Confindustria a seguito dell'adozione delle linee-guida), nonché degli orientamenti espressi dal Ministero del lavoro (Parere 6 giugno 2006, relativo all'ammissibilità del controllo mediante l'utilizzo dei dati relativi al traffico telematico; Parere 28 novembre 2006, relativo all'ammissibilità di controlli a distanza mediante un *computer* telefonare); si sono inoltre considerate le decisioni delle massime giurisdizioni anche sopranazionali (v. in particolare Corte europea dei diritti dell'uomo, *Halford v. United Kingdom*, del 25 giugno 1997 e *Copland v. United Kingdom*, del 3 aprile 2007) e, infine, le indicazioni del Gruppo art. 29 (in particolare "Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro" del 29 maggio 2002 - WP 55).

Ciò premesso, le linee-guida evidenziano che l'utilizzo della posta elettronica e di Internet rappresenta una potenziale fonte di informazioni anche sensibili di lavoratori o di terzi, non necessariamente legate all'attività lavorativa.

In tale quadro, l'eventuale trattamento di dati personali riferiti ai lavoratori deve rispettare le legislazioni di settore (in particolar modo quella sui controlli a distanza dell'attività lavorativa) e la disciplina di protezione dei dati personali (in particolare, i principi di necessità, di correttezza e di pertinenza e non eccedenza, per il perseguimento di finalità determinate, esplicite e legittime).

A tal fine, i datori di lavoro sono tenuti a indicare chiaramente le modalità di utilizzo degli strumenti messi a disposizione dei lavoratori (*ad es.*, i comportamenti eventualmente "tollerati" rispetto alla navigazione in Internet o alla tenuta di *file* nella rete interna, le soluzioni volte a garantire la continuità dell'attività lavorativa in caso di assenza del lavoratore, ecc.) e di eventuali controlli (precisando le ragioni che ne giustificerebbero l'espletamento), anche a mezzo di un apposito disciplinare interno.

I lavoratori devono essere informati in ordine alle principali caratteristiche dei trattamenti, ai soggetti presso cui rivolgersi per esercitare i propri diritti, all'eventualità di controlli sull'impiego di Internet e della posta elettronica; il datore di lavoro, al fine di prevenire l'utilizzo indebito di dati, è chiamato ad adottare opportune misure organizzative e tecnologiche (valutando anche l'impatto sui diritti dei lavoratori dell'eventuale installazione di apparecchiature suscettibili di consentire il controllo a distanza).

Vanno inoltre adottate misure tecnologiche per minimizzare l'uso di dati identificativi dei lavoratori, eventualmente differenziate in funzione della tecnologia impiegata (individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa, configurazione dei sistemi o utilizzo di filtri che prevenivano determinate operazioni reputate inconferenti con l'attività lavorativa, trattamento di dati in forma anonima o aggregata, ecc.).

Parimenti, per quanto concerne l'utilizzo della posta elettronica, i datori di lavoro devono contemperare le esigenze di ordinato svolgimento dell'attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori (*ad es.*, indirizzi di posta elettronica condivisi tra più lavoratori, funzionalità di sistema che consentano l'invio di messaggi automatici in caso di assenza, messaggi di risposta contenenti "coordinate", anche elettroniche o telefoniche, di altro soggetto, ovvero altre utili modalità di contatto della struttura, ecc.).

I sistemi *software* devono cancellare periodicamente e automaticamente i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria. In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all'uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata, nonché limitata al tempo necessario a raggiungerla. Un eventuale prolungamento dei tempi di conservazione può aver luogo solo in riferimento a ipotesi specifiche (*ad es.*, in relazione all'esercizio o alla difesa di un diritto in sede giudiziaria, ovvero all'obbligo di custodire o consegnare i dati su specifica richiesta dell'autorità giudiziaria o della polizia giudiziaria). Il trattamento deve essere comunque limitato alle sole informazioni indispensabili ed essere effettuato con logiche strettamente correlate agli obblighi, compiti e finalità già esplicitati.

Eventuali controlli datoriali devono essere effettuati nella misura meno invasiva possibile e nel rispetto delle previste normative di settore (segnatamente, dell'art. 4 della legge 20 maggio 1970, n. 300). Non risulta ad esempio legittimo il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza dell'attività di lavoratori (lettura e registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori; riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore; lettura e registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo; ecc.). Eventuali controlli legittimi, nel rispetto del predetto art. 4, possono essere effettuati evitando interferenze ingiustificate sui diritti e le libertà fondamentali di lavoratori e terzi, nel rispetto dei principi di pertinenza e di non eccedenza. Per quanto possibile, devono essere preferiti controlli effettuati su dati aggregati, riferiti all'intera struttura lavorativa o a sue aree; in caso di eventuali anomalie, le stesse potranno essere "formalizzate" in comunicazioni dirette alla generalità dei lavoratori della struttura o dell'area. In mancanza di ulteriori anomalie, eventuali controlli su base individuale non risultano, di regola, giustificati; va in ogni caso esclusa l'ammissibilità di controlli prolungati, costanti o indiscriminati.

Il datore di lavoro, in qualità di titolare del trattamento, è tenuto ad adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità di sistemi informativi e di dati; lo stesso può ritenere utile la designazione facoltativa di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità. In caso di interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l'accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti. I predetti soggetti, in ogni caso, potranno svolgere le sole operazioni strettamente necessarie al perseguimento delle previste finalità.

Particolare cura andrebbe prestata nella formazione del personale e in particolare, dei soggetti che operano quali amministratori di sistema o figure analoghe, non solo per i profili tecnico-gestionali e di sicurezza delle reti, ma anche in relazione ai principi di protezione dei dati personali e correlati al segreto nelle comunicazioni.

L'immediata attività di divulgazione delle indicazioni e degli orientamenti espressi dall'Autorità con tale documento ha consentito di dare risposta, già nell'anno in esame, ad alcune istanze, in particolare in materia di controllo a distanza dell'attività dei lavoratori.

Con riferimento a una segnalazione volta ad ottenere una pronuncia del Garante in relazione alla soppressione, alterazione e falsificazione di corrispondenza telematica, si è specificato che l'accertamento di profili attinenti a eventuali condotte penalmente rilevanti dei datori di lavoro resta demandato all'autorità giudiziaria ordinaria (*Nota* 11 dicembre 2007).

Non illegittima è risultata l'irrogazione di un provvedimento disciplinare a un dipendente che aveva utilizzato la posta elettronica per comunicazioni con altri lavoratori non attinenti all'attività lavorativa. La società era venuta a conoscenza della trasmissione delle predette comunicazioni non già attraverso un controllo a distanza della casella di posta elettronica in uso al segnalante (in violazione, quindi, dell'art. 4 della legge 20 maggio 1970, n. 300), bensì dalle numerose lamentele ricevute dagli stessi destinatari delle comunicazioni. Alla luce delle dichiarazioni rese dalla società - e a prescindere, in ogni caso, dal merito dell'intimata sanzione - non sono dunque emersi, in relazione alla vicenda segnalata, elementi atti a giustificare un intervento da parte dell'Autorità (*Nota* 28 novembre 2007).

Alcune segnalazioni hanno riguardato il trattamento effettuato con strumenti di localizzazione dei veicoli dati in dotazione ai lavoratori. Nel fornire un preliminare riscontro agli interessati, in attesa degli ulteriori opportuni approfondimenti, si è fatto in termini generali richiamo, per quanto applicabile, al *provvedimento* generale del 1 marzo 2007 (Linee-guida in materia di posta elettronica e Internet, *cit.*) e si sono altresì trasmessi due provvedimenti del Ministero del lavoro relativi a strumenti che consentono la localizzazione dei dipendenti – uno specificamente riferito all'utilizzo del *Gps* su autoveicoli– nei quali si è ritenuto applicabile l'art. 4 dello Statuto dei lavoratori (con riguardo alla possibilità di un controllo a distanza dei medesimi). In un caso specifico, inoltre, questa Autorità ha ritenuto legittima l'installazione di un sistema di localizzazione satellitare *Gps* su mezzi aziendali, stante la sussistenza, nel caso di specie, di un provvedimento autorizzatorio appositamente emesso dalla direzione provinciale del lavoro territorialmente competente (*Nota* 27 dicembre 2007).

Strumenti di localizzazione satellitare dei lavoratori

L'Autorità sta valutando la necessità di adottare anche in questo contesto un proprio provvedimento.

Dalla documentazione trasmessa con segnalazioni, o a seguito di accertamenti preliminari svolti dall'Autorità, è sovente emerso che l'installazione di sistemi di rilevazione di dati biometrici dei lavoratori è legata a finalità di accertamento delle presenze dei dipendenti sui luoghi di lavoro. Sull'argomento, il Garante (*cf.* *Prov.* 21 luglio 2005 [doc. *web* n. [1150679](#)]) anche con le anzidette linee-guida in materia di rapporto di lavoro, ha precisato che l'utilizzo di dati biometrici dei lavoratori può essere giustificato solo in casi particolari e, in relazione ai luoghi di lavoro, per presidiare accessi ad "aree sensibili" (processi produttivi pericolosi, locali destinati a custodia di beni, documenti riservati). Non si è ritenuto invece ammissibile il trattamento di dati biometrici per finalità di ordinaria gestione del rapporto di lavoro (accertamento delle presenze, commisurazione dei tempi di lavoro, *ecc.*).

Biometria e luoghi di lavoro

Questa Autorità ha fatto inoltre presente che, ai fini dell'installazione dei predetti sistemi, restano salve le previsioni di cui all'art. 4 della legge 20 maggio 1970, n. 300 in ordine all'eventuale controllo a distanza dell'attività dei lavoratori che ne potrebbe derivare.

Questa Autorità è stata chiamata da alcune segnalazioni a esaminare fattispecie relative al recapito in busta "aperta" di cedolini paga dei dipendenti, con conseguente agevole accessibilità alle informazioni ivi contenute da parte di soggetti diversi dal destinatario.

Buste paga

Al riguardo, si è già avuto modo di chiarire, mediante le linee-guida sopra richiamate, che il datore di lavoro, salvi i casi in cui sia la legge stessa a prevedere specifiche modalità di divulgazione dei dati, è tenuto a utilizzare forme di comunicazione individualizzata con il lavoratore, adottando misure opportune per prevenire un'indebita comunicazione di dati personali a terzi diversi dal destinatario (tale è, appunto, la consegna in busta chiusa del cedolino dello stipendio). Tali cautele risultano ancor più necessarie quando dalle suddette comunicazioni sia possibile desumere vicende personali del lavoratore (*ad es.*, alcune diciture riportate sulle buste paga, come la voce "pignoramento").

Nel richiamare detti principi, questa Autorità ha fornito specifiche indicazioni sulla corretta applicazione della disciplina di protezione dei dati in ordine alle vicende segnalate, invitando in un caso il titolare del trattamento a fornire idoneo riscontro circa le misure adottate per conformarsi alle indicazioni rese (*Nota* 30 novembre 2007).

Con riferimento a una fattispecie di divulgazione a mezzo posta elettronica di dati personali dei dipendenti relativi a ferie e permessi non fruiti, questa Autorità ha invitato il titolare del trattamento ad attenersi scrupolosamente alle indicazioni contenute nelle citate linee-guida in materia di rapporto di lavoro, ribadendo che la conoscenza da parte di terzi dei dati personali dei lavoratori, in assenza degli specifici presupposti normativi, è ammessa solo se l'interessato vi acconsente. In proposito, la società interessata ha dichiarato che la vicenda segnalata è stata frutto di un'iniziativa individuale e che sono state comunque adottate soluzioni idonee a evitare il ripetersi di accadimenti simili. L'Autorità ne ha preso atto, rinnovando l'invito alla società a valutare attentamente l'adeguatezza delle istruzioni fornite ai propri incaricati, al fine di garantire modalità di comunicazione con i lavoratori conformi alla disciplina di protezione dei dati (*Nota* 5 febbraio 2008).

Ferie e permessi

Nel corso dell'anno sono inoltre pervenute alcune segnalazioni in ordine alla conformità alla disciplina di protezione dei dati personali di normative settoriali che, per finalità di elusione del lavoro sommerso, impongono ai datori di lavoro di far indossare ai propri dipendenti tesserini identificativi contenenti taluni dati personali agli stessi riferiti (in particolare, fotografia e generalità). Tale obbligo di diffusione presenta profili di criticità in relazione a talune figure professionali (e segnatamente, dalle segnalazioni pervenute, le guardie giurate), che si ritengono esposte al rischio di incolumità personale in ragione dell'agevole conoscibilità, da parte di terzi, di informazioni personali alle medesime riconducibili. La problematica segnalata, considerate le rilevanti implicazioni che la diffusione può comportare sul piano della sicurezza e dell'incolumità individuale, è al vaglio dell'Autorità.

Tesserini identificativi dei dipendenti

Ulteriori ipotesi di diffusione di dati personali dei dipendenti si sono registrate in relazione ad alcune segnalazioni aventi per oggetto la divulgazione di provvedimenti disciplinari. In particolare, una segnalazione lamentava l'affissione nella bacheca aziendale di una delibera contenente il nominativo di un dipendente associato al *provvedimento* sanzionatorio irrogato, contestando l'illegittimità del trattamento effettuato.

Sanzioni disciplinari

Al riguardo si è già avuto modo di ribadire che, in termini generali, la diffusione di dati personali riferiti ai lavoratori, in assenza di specifiche disposizioni o comunque di altro presupposto ai sensi dell'art. 24 del Codice, può avvenire solo se necessaria per dare esecuzione a obblighi derivanti dal contratto di lavoro (art. 24, comma 1, lett. *b*)). Quindi, non è di regola lecito dare diffusione a informazioni personali riferite a singoli lavoratori, anche attraverso la loro pubblicazione in bacheche aziendali o in comunicazioni interne destinate alla collettività dei lavoratori, specie se non correlate all'esecuzione di obblighi lavorativi. In tali casi, tra l'altro, la diffusione si pone anche in violazione dei principi di finalità e pertinenza stabiliti dall'art. 11 del Codice.

Al riguardo, l'associazione interessata, fornendo chiarimenti in ordine alla vicenda segnalata, ha confermato l'accaduto, addebitandolo tuttavia a un episodio isolato e asserendo di voler introdurre opportuni correttivi per adeguarsi alla normativa vigente. L'Autorità ne ha preso atto e ha inoltrato copia del *provvedimento* generale in materia di rapporto di lavoro al fine di consentire alla stessa una più compiuta attuazione della disciplina di protezione dei dati (*Nota* 21 dicembre 2007).

È risultata invece legittima, alla luce della documentazione trasmessa, la diffusione di dati relativi alla sanzione disciplinare riferita a un dipendente operante presso una società di trasporto pubblico locale. Nel caso di specie, considerata la sia pur risalente normativa di settore –che impone al datore di lavoro di portare a conoscenza del personale, tra l'altro, le sanzioni disciplinari irrogate nei confronti dei dipendenti– non sono stati ravvisati profili di violazione della disciplina di protezione dei dati personali.

Alcune segnalazioni hanno lamentato l'illegittimità di comportamenti datoriali volti ad acquisire numeri telefonici

dei medici curanti al fine di "approfondire" le cause di assenza per malattia dei dipendenti. Nel fornire riscontro agli interessati si è precisato che il datore di lavoro, come già chiarito dalle linee-guida in materia di rapporto di lavoro (cfr. par. 6.2.), può conoscere solo la "prognosi" e non la "diagnosi" della patologia denunciata dal lavoratore (fatte salve alcune limitate fattispecie, come in caso di denuncia all'Inail di infortuni sul lavoro o malattie professionali). Si è ricordato, peraltro, che il datore di lavoro può servirsi degli "ordinari" strumenti previsti dall'ordinamento (contestazioni dirette al solo interessato, visite fiscali, denunce di ipotetico reato), ma nel rispetto della disciplina in materia di protezione dei dati personali (per un caso simile, cfr. *Prov. 24 settembre 2001* [doc. web n. [39460](#)]).

**Assenze
per malattia
e controlli
datoriali**

In un caso, tra l'altro, si è riscontrato l'invio a terzi (nella fattispecie, i medici curanti), ad opera del datore di lavoro, di comunicazioni contenenti dati personali di una dipendente per finalità di contestazione della prolungata e ininterrotta assenza dal servizio della dipendente medesima. Nell'invitare il titolare del trattamento a conformarsi ai principi di protezione dei dati e al *provvedimento* generale in materia di rapporto di lavoro, questa Autorità ha confermato che simili trattamenti non rispondono ai principi di pertinenza, non eccedenza e proporzionalità (*Nota 18 ottobre 2007*).

Con specifico riferimento a un'ipotesi di diffusione di dati sensibili dei lavoratori (nella fattispecie, l'iscrizione di alcuni dipendenti a una organizzazione sindacale), questa Autorità ha ricordato al titolare del trattamento che la diffusione di dati sensibili dei dipendenti non è ammissibile, in assenza dei presupposti di equipollenza del consenso legislativamente previsti (art. 26, comma 4, del Codice), senza il consenso scritto degli interessati (art. 26, comma 1, del Codice). Chiamata a fornire chiarimenti la società interessata ha dichiarato, ai sensi e per gli effetti di cui all'art. 168 del Codice, di non aver diffuso dati personali sensibili dei lavoratori, producendo documentazione fotografica comprovante le proprie deduzioni. Preso atto delle dichiarazioni rese, si è nondimeno provveduto a richiamare la società al più rigoroso rispetto delle misure di sicurezza adottate (*Nota 24 gennaio 2008*).

**Iscrizioni
sindacali**

In un caso, questa Autorità è stata interpellata sulla conformità alla disciplina di protezione dei dati personali di un contratto di somministrazione stipulato per ragioni sostitutive e che recava il nominativo del lavoratore temporaneamente sostituito. Alla luce delle dichiarazioni rese dall'agenzia di lavoro presso il quale il contratto era stato stipulato –secondo cui le procedure in essere prevederebbero da tempo l'indicazione del solo numero di matricola del dipendente temporaneamente sostituito in luogo del nominativo al medesimo riferito–, si è ritenuto che, allo stato, non sussistessero i presupposti per un intervento da parte del Garante (*Nota 15 febbraio 2008*).

**Contratto di
somministrazione**

Di particolare rilevanza, considerata la delicatezza della materia sotto il profilo della protezione dei dati personali, sono alcune segnalazioni pervenute all'Autorità aventi per oggetto l'adozione di procedure societarie interne di "segnalazione" di illeciti commessi da propri dipendenti (cd. "whistleblowing"). Trattandosi di materia attualmente priva di qualsiasi disciplina legale, questa Autorità, per i profili di propria competenza, sta valutando quali iniziative intraprendere e quali determinazioni adottare.

**Procedure
societarie
di "segnalazione"
di illeciti
commessi
da propri
dipendenti (cd.
"whistleblowing")**

Nonostante le linee-guida in materia di rapporto di lavoro abbiano fornito significativi chiarimenti in merito (v. in particolare il punto 9.5.), diverse segnalazioni hanno avuto per oggetto molteplici tipologie di informazioni e documenti (rilevanza delle presenze, corrispondenza intercorsa, giornate di malattia, schede di valutazione, ecc.) trattati dai datori di lavoro.

**Accesso
ai dati trattati
dal datore
di lavoro**

In proposito, si è ricordato che l'art. 7 del Codice riconosce agli interessati il diritto di accedere alle informazioni personali a sé riferite, ivi comprese quelle di carattere valutativo (alle condizioni e nei limiti di cui all'art. 8, comma 5, del Codice). L'esercizio di tale diritto consente di ottenere, ai sensi dell'art. 10 del Codice, solo la comunicazione dei dati personali relativi al richiedente detenuti dal titolare del trattamento; non permette, invece, di richiedere il diretto e illimitato accesso a documenti e a intere tipologie di atti, ovvero di ottenere, sempre e necessariamente, copia dei documenti detenuti. In altra occasione si è precisato che il titolare del trattamento è tenuto a comunicare i dati richiesti ed effettivamente detenuti, non già a ricercare o raccogliere altri dati che non siano nella sua disponibilità e non siano oggetto, in alcuna forma, di attuale trattamento.

Uno studio di consulenza ha chiesto di essere autorizzato a adottare, quale credenziale di autenticazione per l'utilizzo del *personal computer* in dotazione, una caratteristica biometrica dei propri dipendenti, onde elevare il livello di sicurezza in ordine agli accessi ai dati personali sensibili ivi contenuti, assicurando espressamente che il sistema non è preordinato alla rilevazione della presenza dei lavoratori e che non verrebbe costituito alcun archivio centralizzato contenente le impronte dei lavoratori. Con specifico riferimento alla fattispecie evidenziata, si è ritenuto che, allo stato degli atti, non fosse necessaria una verifica preliminare da parte dell'Autorità, tenuto conto delle circostanze sopra evidenziate e della circoscritta finalità perseguita in conformità all'Allegato b) al Codice in materia di protezione dei dati personali [doc. web n. [488497](#)], che prevede, quale credenziale di autenticazione, anche l'utilizzo di "una caratteristica biometrica dell'incaricato eventualmente associata a un codice identificativo o a una parola chiave" (regola 2 dell'All. b) cit.; *Nota 4 gennaio 2008*).

**Credenziali
biometriche**

Un segnalante lamentava l'illegittima sottrazione di documenti (tra cui corrispondenza privata e ricette mediche) da un cassetto della scrivania di lavoro assegnatagli. Non sono però emersi elementi atti a giustificare un intervento del Garante, anche in considerazione della riconducibilità al medesimo segnalante dei documenti sottratti e della loro volontaria dislocazione, per scelte personali, in ambiti di pertinenza aziendale (*Nota 23 gennaio 2008*).

**Documenti
personali
in ambito
di pertinenza
aziendale**

È pervenuta a questa Autorità una segnalazione avente per oggetto un patto di non concorrenza sottoscritto dalla segnalante con la sua pregressa società di appartenenza. L'interessata, contattata dalla società che chiedeva informazioni in ordine alla sua "nuova" attività professionale al fine di verificare il rispetto di quanto pattiziamente convenuto, chiedeva delucidazioni all'Autorità in ordine a tale richiesta. Dalla documentazione in atti non sono emersi profili di violazione della disciplina di protezione dei dati, considerato che nel patto di non concorrenza stipulato dalla segnalante figurava una clausola con cui la medesima segnalante si impegnavano a comunicare alla società le attività svolte durante la vigenza del patto stesso (*Nota 14 dicembre 2007*).

**Patto di non
concorrenza**

10.3.3. Previdenza

L'Istituto nazionale della previdenza sociale, recependo le valutazioni effettuate a suo tempo dall'Ufficio, nell'ambito dell'istruttoria preliminare di una segnalazione, ha riformulato la modulistica utilizzata per le richieste di astensione obbligatoria e facoltativa per maternità, con particolare riferimento al rispetto dei principi di necessità, indispensabilità, pertinenza e non eccedenza dei dati trattati e alla correttezza dell'informativa sul trattamento dei dati personali (artt. 3, 11, 13 e 22 del Codice). È stata eliminata l'indicazione relativa ad alcune informazioni sulla gestazione della lavoratrice, quali la data dell'ultimo ciclo mestruale, quella dei primi movimenti del feto e dei fenomeni connessi alla gravidanza, nonché i rilievi obiettivi per la diagnosi risultanti dall'esame clinico. Nell'informativa, che è stata aggiornata al Codice, sono stati inoltre espunti i riferimenti al consenso al trattamento dei dati da parte delle lavoratrici, in quanto i soggetti pubblici non devono richiedere il consenso dell'interessato (art. 18 del Codice).

**Rivisitazione
della
modulistica Inps**

Su impulso dell'Ufficio, al quale è pervenuta una segnalazione circostanziata, l'Inps sta avviando specifici approfondimenti in merito alle istruzioni fornite alle proprie articolazioni organizzative con la circolare n. 90 del 23 maggio 2007. La circolare prevede che i richiedenti i permessi per l'assistenza ai propri familiari disabili (art. 33 legge 5 febbraio 1992, n. 104), che lavorano o risiedono in luoghi distanti da quello del familiare, presentino all'atto della richiesta, un "Programma di assistenza" a firma congiunta del lavoratore e del familiare interessato (Nota 15 novembre 2007). All'esito di tali approfondimenti, l'Autorità verificherà il rispetto dei principi di pertinenza, non eccedenza e indispensabilità dei dati trattati dall'Istituto –specie se riferiti a terzi non direttamente interessati alle prestazioni da svolgere– in rapporto alle finalità di rilevante interesse pubblico perseguite (artt. 11, 20, 22, commi 3 e 5, 68 e 86, comma 1, lett. c), del Codice).

**Permessi per
l'assistenza
a familiari
disabili**

A seguito della segnalazione di una lavoratrice, che lamentava che il datore di lavoro aveva ricevuto un plico anonimo contenente il suo estratto conto contributivo, sono state verificate le modalità adottate dall'Inps per il rilascio di tali documenti, con particolare riferimento all'individuazione dei soggetti, diversi dal lavoratore interessato, che possono venire legittimamente a conoscenza dei dati personali, e alle modalità eventualmente adottate per prevenire l'indebita conoscenza di tali dati da parte di terzi non legittimati (artt. 19, 31 e 33 ss. del Codice). Sono stati inoltre richiesti specifici elementi riguardo al funzionamento di talune apparecchiature *self-service* per l'emissione degli estratti contributivi che, all'esito dei primi approfondimenti, risultavano essere installate presso alcune sedi dell'Istituto e funzionare mediante l'inserimento del tesserino magnetico del codice fiscale non necessariamente appartenente all'interessato (Note 5 novembre 2007 e 21 dicembre 2007).

**Modalità
di rilascio
dell'estratto
conto
contributivo
relativo
ai lavoratori**

Dagli elementi acquisiti all'esito dell'istruttoria preliminare, le modalità adottate dall'Istituto non sono state ritenute in contrasto con la disciplina sulla protezione dei dati personali anche in considerazione della circostanza che l'evoluzione tecnologica ha determinato la riduzione dell'uso tali apparecchiature, le quali non risultano attualmente più attive.

10.4. Attività di marketing e fidelizzazione

Il fenomeno delle carte e dei programmi di fidelizzazione (nei settori più vari, della grande distribuzione, telefonia, trasporti, viaggi) ha formato oggetto di accertamenti sulla conformità dei trattamenti al *provvedimento* generale in materia di fidelizzazione della clientela adottato il 24 febbraio 2005 [doc. web n. [1103045](#)].

**Programmi di
fidelizzazione**

È così emerso che le prescrizioni contenute nel *provvedimento* sono state recepite solo in parte dagli operatori. Nel dettaglio, il Garante ha vietato a quattro società l'uso di dati personali trattati in modo illecito: alcune società raccoglievano, oltre ai dati anagrafici e ai recapiti degli interessati (necessari per attribuire *bonus* connessi all'uso della carta), ulteriori informazioni quali il titolo di studio, la professione e il numero dei componenti del nucleo familiare; dati ritenuti nei casi esaminati non pertinenti ed eccedenti dal Garante che ha ordinato ai titolari dei relativi trattamenti di cancellarli o di renderli anonimi (Prov. 15 novembre 2007 [doc. web nn. [1466930](#) e [1466898](#)]).

Altre irregolarità sono state riscontrate nella scarsa chiarezza o nella mancanza degli elementi indicati nell'art. 13 del Codice con cui vengono fornite le informative (comprese quelle rese *on-line*) ai consumatori e talora anche nella loro incompletezza, nonché nelle modalità di raccolta del consenso degli interessati (Prov. 15 novembre 2007 [doc. web nn. [1466971](#) e [1466985](#)]).

L'Autorità ha ribadito la necessità di mettere il consumatore nelle condizione di poter scegliere liberamente se e quali trattamenti di dati autorizzare, chiarendo agli interessati che il consenso per l'utilizzo dei dati per finalità ulteriori rispetto a quelle connesse alla mera consegna dei premi e vantaggi previsti dal programma di fidelizzazione deve essere prestato liberamente: è quindi necessaria l'autonoma decisione del consumatore per l'utilizzo dei dati anche per finalità ulteriori, quale quella di *marketing* e di profilazione della clientela (Provvedimenti 15 novembre 2007 [doc. web nn. [1466956](#) e [1466898](#)]).

Infine, in relazione all'uso di dati il cui conferimento era facoltativo a fini statistici, il Garante ha prescritto alle società di adottare opportuni accorgimenti che impediscano di ricondurre i dati all'interessato fin dal momento della raccolta (Prov. 15 novembre 2007 [doc. web n. [1466956](#)]).

Verifiche sono state svolte nell'ambito del trattamento di dati personali (dati anagrafici, recapiti e opinioni espresse dagli interessati) per l'effettuazione di sondaggi telefonici di natura politico-elettorale finalizzati a rilevare il grado di soddisfazione dei residenti in un comune in vista delle consultazioni amministrative del 2006. Nel corso degli accertamenti è emerso che dalle risposte ai quesiti posti agli interessati era possibile risalire alle opinioni politiche degli intervistati (art. 4, comma 1, lett. d), del Codice).

**Sondaggi
in materia
elettorale**

Nella vicenda in parola, la disciplina in materia di protezione dei dati personali è stata violata sotto più profili (Prov. 13 settembre 2007 [doc. web n. [1523633](#)]): non è risultato acquisito, limitatamente ai dati sensibili trattati, il consenso degli interessati in forma scritta (risultando, in base alle attestazioni fornite dalla società, la sua acquisizione solo telefonica); non sono state rispettate le condizioni previste dall'*autorizzazione generale* n. 5 del 21 dicembre 2005 (all'epoca applicabile e ora sostituita dall'analoga *autorizzazione generale* n. 5/2007) in materia di trattamento dei dati sensibili nello svolgimento di sondaggi e ricerche (Capo II); i trattamenti effettuati non erano stati notificati al Garante (art. 37, comma 1, lett. e), del Codice, relativo all'obbligo di notificazione di dati sensibili utilizzati per sondaggi d'opinione).

A ciò si aggiunga che i dati personali trattati (in particolare, quelli identificativi) erano sicuramente eccedenti, atteso che, per l'esecuzione del sondaggio, non è necessario registrare e conservare la valutazione espressa dagli interessati unitamente ai dati identificativi degli stessi (come invece avvenuto nel caso di specie).

Inoltre, anche in relazione ai dati diversi da quelli sensibili, il Garante ha ritenuto che, una volta consegnati gli elaborati delle interviste al committente, non sussistessero più le ragioni per la loro ulteriore conservazione presso la società che aveva eseguito il sondaggio (art.

11, comma 1, lett. e), del Codice): esaurita l'elaborazione delle informazioni personali consentita nella misura indispensabile, infatti, la società avrebbe dovuto procedere alla cancellazione o anonimizzazione dei dati personali relativi agli interessati.

Il Garante ha dunque prescritto alla società, titolare del trattamento la cancellazione o l'anonimizzazione dei dati personali raccolti illecitamente. È stato altresì prescritto che prima dell'effettuazione dei sondaggi vengano fornite all'interessato, anche ricorrendo a formulazioni sintetiche ma chiare, le informazioni contenute nell'art. 13 del Codice (anzitutto indicando chiaramente la finalità, mentre nel caso di specie si era operato un riferimento generico alla rilevazione della qualità della vita e dell'ambiente nell'area interessata).

Con *deliberazione* del 25 luglio 2007 [doc. web n. [1428567](#)], adottata al termine di una procedura di cooperazione con l'Autorità per l'energia elettrica e il gas, il Garante ha fornito una serie di indicazioni sulle offerte commerciali formulate da soggetti operanti nel mercato libero elettrico, per garantire una corretta informazione degli utenti e un giusto utilizzo dei loro dati.

**Le proposte
commerciali
nel mercato
dell'energia
elettrica**

La disciplina sulla liberalizzazione dell'energia (d.l. 18 giugno 2007, n. 73) prevede infatti che, a partire dal 1 luglio 2007, i clienti domestici possano scegliere un fornitore diverso. L'Autorità per l'energia elettrica e il gas ha quindi rappresentato la necessità che, per un periodo transitorio, le società che vendono energia possano acquisire dai distributori alcune informazioni di base relative agli utenti del mercato energetico per formulare proposte commerciali.

In questa cornice, l'Autorità per l'energia elettrica e il gas ha approvato con la deliberazione del 27 giugno 2007 n. 157 una prima parte della "*Disciplina in materia di accesso ai dati di base per la formulazione di proposte commerciali inerenti la fornitura di energia elettrica e/o di gas naturale*", e ha interpellato il Garante sul trattamento dei dati personali degli utenti. Al riguardo l'Autorità ha stabilito che le società distributrici dovranno informare la clientela prima di comunicare i dati personali dati (generalità, consumi, potenza impegnata ecc.): per agevolare tale compito il Garante ha curato la predisposizione di un modello (allegato alla citata delibera). L'informativa dovrà preferibilmente essere recapitata unitamente alla corrispondenza inviata ordinariamente alla clientela (*ad es.*, con la bolletta) e dovrà essere messa a disposizione anche sul sito Internet delle società o attraverso i servizi di assistenza e informazione al pubblico.

I venditori dovranno utilizzare i dati solo con modalità strettamente correlate all'invio delle proposte cartacee e non dovranno conservare i dati relativi a clienti che, decorso un congruo termine non superiore a sei mesi, non abbiano aderito alla proposta; ciò, ferma restando la possibilità di utilizzare i dati di base ottenuti dai distributori fino al raggiungimento di un adeguato grado di concorrenza dei mercati dell'energia elettrica e del gas naturale sulla base di valutazioni della competente Autorità e, comunque, non oltre il 31 dicembre 2010. Decorso tale termine tutti i dati personali forniti dai distributori in relazione ai quali non si sia instaurato un rapporto di fornitura dovranno essere cancellati.

10.5. Altre attività imprenditoriali

Nel corso degli anni è emerso, anche tramite associazioni di categoria, che alcuni adempimenti contenuti nella disciplina di protezione dei dati personali vengono reputati talvolta onerosi per l'ordinaria attività di impresa.

**Attività
di impresa e
semplificazioni.
La "Guida
pratica"
per le piccole
e medie
imprese**

Considerato però che una giusta protezione dei dati personali può rappresentare una risorsa per l'impresa, rendendone più efficiente l'attività e incrementando la fiducia di consumatori e utenti, il Garante ha messo a punto una "Guida pratica" pubblicata nella *Gazzetta Ufficiale* 21 giugno 2007, n. 142 [doc. web n. [1412271](#)], per facilitare le piccole e medie imprese, ivi compresi gli artigiani, nell'assolvimento degli obblighi imposti dalla normativa sulla protezione dei dati personali.

La "*Guida pratica e misure di semplificazione per le piccole e medie imprese*" fornisce soluzioni semplificate per un corretto trattamento dei dati personali: dall'individuazione del titolare del trattamento e dei suoi obblighi alle verifiche sui soggetti che possono effettuare il trattamento (incaricati e responsabili); all'indicazione dei casi in cui l'imprenditore non è tenuto ad effettuare la notificazione al Garante o a rendere l'informativa agli interessati, o comunque può renderla in forma semplificata (art. 13, commi 2 e 3); chiarimenti sono espressi anche in relazione ai casi nei quali non è necessario richiedere il consenso dell'interessato (si tratta dei casi che comprendono larga parte dei trattamenti effettuati ordinariamente dall'impresa e che sono indicati nelle lettere a)-d) dell'art. 24, comma 1, del Codice); ai doveri del titolare per soddisfare le richieste di accesso nel caso di esercizio dei diritti e alla sempre maggiore necessità di trasferire dati personali all'estero.

La Guida è stata integrata con un questionario che dovrebbe agevolare un'immediata verifica da parte degli imprenditori di eventuali criticità rispetto all'osservanza dei principi di protezione dei dati.

All'inizio del 2007 (*Prov. 18 gennaio 2007* [doc. web n. [1392461](#)]) l'Autorità si è pronunciata in materia di operazioni di cartolarizzazione, regolate dalla l. 30 aprile 1999, n. 130, e di altre operazioni che presentavano caratteristiche omogenee. L'Autorità aveva già individuato modalità alternative (rispetto a quella individuale) per rendere l'informativa ai debitori ceduti da parte del cessionario (da ultimo *Prov. 4 aprile 2001* [doc. web n. [40763](#)]), disponendo che l'informativa fosse resa dal cessionario mediante pubblicazione sulla *Gazzetta Ufficiale* e con annunci pubblicati su almeno due quotidiani nazionali e uno locale.

Cartolarizzazioni

Nel corso dell'attività di controllo volta ad accertare l'adozione delle menzionate misure da parte di tutte le società cessionarie che nel tempo avevano inviato al Garante apposita istanza di esonero dall'informativa in vista dell'esecuzione di operazioni di cartolarizzazione, sono emerse ampie aree di omessa o inidonea informativa rispetto alle indicazioni contenute nel *provvedimento* del 2001.

L'intervento dell'Autorità in tale settore è stato ritenuto necessario anche alla luce di alcune innovazioni normative contenute nel Codice (entrato in vigore successivamente all'adozione del menzionato *provvedimento* del Garante). In particolare, l'art. 13, comma 5, lett. c), del Codice prevede ora espressamente che, in casi determinati, il titolare del trattamento sia esonerato dall'obbligo di fornire l'informativa all'interessato, rimettendo al Garante l'eventuale individuazione di "*misure appropriate*" per consentire comunque adeguata pubblicità al trattamento effettuato. L'art. 2 del Codice, con disposizione assente nel quadro normativo previgente, dispone, tra l'altro, la semplificazione degli adempimenti richiesti dalla disciplina in materia di protezione dei dati personali ai titolari del trattamento, pur assicurando un elevato livello di tutela dei diritti e delle libertà fondamentali dell'interessato nell'ambito di operazioni di trattamento (*cf.* art. 2, comma 2, del Codice; considerando n. 49 direttiva 95/46/Ce). L'esigenza di un nuovo intervento dell'Autorità nel settore è

derivata anche dalla crescente complessità di talune operazioni di cartolarizzazione, attuate mediante la conclusione di "contratti cornice" tra cedente e cessionario del credito funzionali a regolamentare una pluralità di operazioni di cessione di crediti, nonché l'attribuzione di compiti ulteriori, con particolare riferimento alla gestione dei crediti per conto del cessionario (abituamente denominato "società veicolo" o *special purpose vehicle*), non di rado posta in capo alla stessa società cedente i crediti (cd. "originator").

Pertanto, muovendo anche dalla considerazione che l'informativa effettuata singolarmente a ciascun debitore comporterebbe costi manifestamente sproporzionati rispetto al diritto tutelato, con il nuovo *provvedimento* il Garante ha individuato chiaramente le operazioni di cessione in blocco dei crediti che determinano la comunicazione dal cedente al cessionario di dati personali relativi al debitore ceduto ("interessato"), precisandone l'ambito di applicazione con riguardo sia alle operazioni di cessione in blocco a titolo oneroso di portafogli di crediti pecuniari, anche futuri, di cui alla l. 30 aprile 1999, n. 130 (recante disposizioni sulla cartolarizzazione di crediti) sia alle operazioni di cessione dei crediti disciplinate all'art. 58 del d.lg. 1 settembre 1993, n. 385 (*Testo unico delle leggi in materia bancaria e creditizia*), sia alle operazioni di cessione dei crediti futuri e di crediti in massa, disciplinate dalla l. 21 febbraio 1991, n. 52, in materia di cessione di crediti d'impresa (cd. "legge sul factoring").

Ai sensi dell'art. 13, comma 5, lett. c) del Codice, il Garante ha, dunque, esonerato, in via generale, i cessionari di crediti in blocco rientranti nell'ambito di applicazione del *provvedimento* dall'obbligo di rendere l'informativa, senza che debba essere presentata apposita istanza di autorizzazione al Garante. In applicazione del principio di semplificazione, inoltre, ha disposto la pubblicazione dell'informativa contenente gli elementi previsti dall'art. 13, commi 1 e 2, del Codice sulla sola *Gazzetta Ufficiale*, eliminando alcuni degli adempimenti che, alla luce delle verifiche effettuate, erano risultati inefficaci sotto il profilo della effettiva conoscibilità da parte degli interessati o troppo onerosi per le imprese. In particolare, non è più richiesta la pubblicazione dell'informativa sulle testate giornalistiche, e quella resa mediante l'affissione nei locali della cessionaria.

Si è provveduto comunque a individuare, quale misura appropriata a garanzia degli interessati, l'invio dell'informativa individuale nei confronti del singolo debitore ceduto alla prima occasione utile (*ad es.*, in sede di invio dell'estratto conto o della prima richiesta di pagamento, se del caso anche tramite la società incaricata dei servizi di *servicing*).

L'esigenza di semplificazione è emersa anche in relazione ai servizi telefonici di assistenza e di informazione al pubblico utilizzati da numerosi soggetti nello svolgimento della propria attività (pubblica o privata) per una vasta gamma di funzioni: tra le più ricorrenti, possono evidenziarsi quelle di informazione e/o di assistenza alla clientela (cd. "*customer care*"), con riferimento all'instaurazione e all'esecuzione di rapporti contrattuali in vari contesti (quali *preNotazione* di servizi a sovrapprezzo di tipo sociale-informativo, di assistenza, di consulenza e di intrattenimento), ma anche quelle svolte a vantaggio della collettività da parte di amministrazioni pubbliche.

**Adempimenti
semplificati
per i servizi
telefonici
di assistenza
e di informazione
al pubblico**

Tenendo conto delle dimensioni assunte dal fenomeno, e con riguardo anche alle sollecitazioni provenienti da un'associazione di categoria rappresentativa delle società di *call center* operanti in *outsourcing*, l'Autorità ha ritenuto opportuno intervenire in materia con un *provvedimento* generale del 15 novembre 2007 (doc. *web* n. [1462788](#)), soffermandosi in particolare sulle attività prestate in modalità "*inbound*" (ossia a seguito di chiamate degli utenti, effettuate anche attraverso canali completamente automatizzati).

In attuazione del principio di semplificazione contenuto nel Codice (art. 1, comma 2 e più in particolare art. 13, commi 2 e 3) il Garante ha precisato che in molti casi (specie per servizi meramente informativi), non essendo trattati dati personali, la disciplina di protezione dei dati personali (e i correlativi adempimenti) non trova applicazione.

Nei casi in cui l'informativa non sia già stata fornita in precedenza (si pensi ai cd. "servizi *post-vendita* resi telefonicamente), può rendersi necessario fornire all'interessato gli elementi previsti all'art. 13 del Codice: anche per questa ipotesi, tuttavia, il Garante ha precisato (al fine di prevenire una scorretta interpretazione della disciplina e l'introduzione di prassi inutilmente burocratiche) che gli operatori qui presi in considerazione possono non fornire "gli elementi già noti" all'interessato (art. 13, comma 2).

Ogni altro ulteriore elemento, in base al principio di cui all'art. 2 del Codice, può essere comunque fornito con formule sintetiche, purché chiare e di immediata comprensione, ad esempio utilizzando messaggi preregistrati nel corso di eventuali tempi di attesa.

Coloro che prestano i servizi in esame sono stati autorizzati (senza rivolgere al Garante alcuna richiesta), dopo aver rappresentato in modo semplificato agli utenti gli eventuali elementi dell'informativa che risulti necessario fornire, a indicare la modalità attraverso la quale l'interessato può prendere conoscenza integrale dell'informativa, anche tramite un messaggio ascoltabile digitando una cifra sulla tastiera del telefono. Apposita istanza deve essere invece formulata solo per situazioni meritevoli di specifico esame.

Per quanto riguarda i servizi abilitati in base alla legge a ricevere chiamate d'emergenza (d.m. Min. comunicazioni 27 aprile 2006 sul servizio "112" quale numero unico europeo d'emergenza; v. anche *Parere* 6 aprile 2006, [doc. *web* n. [1269343](#)]) il Garante ha stabilito che, attesa la loro peculiare natura, i titolari del trattamento possono rendere l'informativa agli interessati (se dovuta in base al Codice: *cf.* art. 53) inserendola nei siti *web* di riferimento.

Nel *provvedimento* l'Autorità ha inoltre invitato le società che operano nella gestione dei servizi telefonici a considerare la natura dei dati trattati, che talora possono essere di natura sensibile (si pensi alle informazioni raccolte nell'ambito di servizi prestati da strutture sanitarie); ad assicurare elevati livelli di professionalità nel trattamento dei dati, nonché ad adottare adeguate soluzioni tecnico-organizzative anche in ordine alla sicurezza dei dati e dei sistemi.

In tal senso, il contratto di fornitura del servizio di assistenza telefonica al pubblico deve contenere concrete modalità operative idonee ad assicurare condizioni di trasparente e corretto svolgimento delle relazioni con l'utenza, indicando altresì le misure di sicurezza che dovranno essere adottate, anche al fine di prevenire commistioni tra distinti archivi gestiti dal medesimo responsabile del trattamento.

L'Autorità ha inoltre precisato che le informazioni raccolte devono essere utilizzate solo per scopi determinati, espliciti e legittimi, senza l'utilizzo di dati di abbonati e di utenti non necessari.

I soggetti privati devono di regola sollecitare il consenso informato qualora intendano utilizzare i dati per finalità diverse e compatibili, come nel caso del *marketing* o della creazione di profili relativi all'utenza (artt. 23 e 24 del Codice), mentre i soggetti pubblici devono operare pur sempre per dichiarate finalità istituzionali, nell'osservanza delle pertinenti disposizioni del Codice (*cf.* artt. 18 ss. del Codice).

Infine, eventuali registrazioni legittime del contenuto delle comunicazioni, effettuate con l'operatore o per il tramite di dispositivi automatici, possono essere conservate solo per un periodo di tempo necessario al corretto assolvimento delle operazioni richieste dagli utenti o alle eventuali esigenze di fatturazione, nei casi di servizi a pagamento, salva l'osservanza di specifici obblighi di legge che ne legittimino l'ulteriore conservazione.

10.6. Attività di impresa e controlli

Nell'ambito di verifiche sull'osservanza della disciplina in materia protezione dei dati personali nella compilazione della *cd. "schede albergo"* e di "altri trattamenti dei dati personali dei clienti" è stato ribadito, in particolare, che il trattamento effettuato per finalità diverse da quelle di esecuzione del contratto alberghiero richiede il consenso libero, specifico e informato dell'interessato (art. 23, comma 3, del Codice) (*Nota* 9 agosto 2007). Nel modello di informativa in uso presso la struttura alberghiera interessata dagli accertamenti, il consenso era richiesto con un'unica formula onnicomprensiva. Come già rilevato in passato dal Garante, la capacità di autodeterminazione dell'interessato non è assicurata quando si sollecita il consenso in modo indifferenziato per perseguire anche la finalità di marketing, mediante "*l'invio di mailing*" o la "*comunicazione di offerte speciali*" alla clientela (tra i tanti, *Prov. 24 febbraio 2005*, punto 7 [*doc. web n. 1103045*]).

**Accertamenti
in ambito
alberghiero**

Con riferimento all'enunciazione delle diverse finalità del trattamento (art. 13, comma 1, lett. *a*) del Codice), l'Autorità ha messo in luce l'opportunità che gli elementi individuati all'art. 13 del Codice "*compaiano in un unico messaggio*" (*cf.*, sul punto, *Prov. 13 gennaio 2000* [*doc. web n. 42276*]) in modo da risultare agevolmente individuabili, ponendo in distinta e specifica evidenza le caratteristiche dell'eventuale attività di profilazione e/o di *marketing*, come pure l'intenzione di cedere a terzi specificamente individuati i dati per finalità da indicare puntualmente (*cf.* *Prov. 24 febbraio 2005* [*doc. web n. 1103045*]).

Attesa la scarsa chiarezza del modello di informativa attualmente distribuita alla clientela, la società è stata invitata a predisporre un nuovo modello di informativa riformulato, alla luce delle prescrizioni già fornite in via generale dal Garante con i richiamati provvedimenti, al fine di rendere la medesima trasparente e di agevole comprensione per gli interessati e collocando, altresì, le pertinenti informazioni in un'unica sede.

A seguito di talune alcune segnalazioni pervenute nel tempo, sono stati svolti accertamenti presso alcuni esercizi commerciali sulla conformità alla disciplina in materia di protezione dei dati personali delle operazioni di trattamento poste in essere da una società che acquista *pro-soluto* crediti vantati da parte di esercizi commerciali convenzionati sorti in occasione di vendite pagate con assegni bancari.

**Trattamenti
di dati
per il servizio
garanzia assegni**

Con *provvedimento* del 17 maggio 2007 (*doc. web n. 1409251*) il Garante ha fornito prescrizioni ai sensi dell'art. 154, comma 1, lett. *c*) del Codice e fissato un termine entro il quale la società ha provveduto a rendere il complessivo trattamento dei dati personali strumentale alla gestione del servizio conforme alla disciplina del Codice.

Nel corso dell'attività istruttoria era emerso che, in particolare, dati identificativi del traente (nome, cognome, indirizzo, tipologia e numero del documento di identità, recapito telefonico) e dati idonei a identificare l'assegno (codice Abi e Cab della banca, conto corrente e numero dell'assegno) erano conservati per un periodo "indefinito"; venivano utilizzati per valutare se procedere all'acquisto del credito nei confronti degli esercizi convenzionati; venivano trattati unitamente a dati eventualmente provenienti da archivi pubblici o privati (quali la Centrale d'allarme interbancaria o società esterne che forniscono dati relativi a protesti o pregiudizievoli).

A tale proposito il *provvedimento* ha ribadito la necessità di identificare tempi massimi di conservazione dei dati trattati alla luce delle finalità in concreto perseguite, salva la necessità che i dati personali siano conservati in conformità a puntuali disposizioni normative (*ad es.*, quelle sulle scritture contabili). Le informazioni necessarie alla gestione del servizio possono essere trattate, infatti, per il tempo strettamente necessario allo svolgimento dello stesso e, comunque, non oltre i termini di prescrizione delle azioni eventualmente esercitabili a tutela del credito (art. 11, comma 1, lett. *e*), del Codice).

Il Garante ha poi prescritto alla società, in qualità di titolare del trattamento, di effettuare le verifiche previste dall'art. 30 del Codice impartendo le dovute istruzioni, anche mediante controlli periodici, ancorché a campione, a mezzo di propri incaricati, sull'adempimento da parte del personale operante presso gli esercizi commerciali dell'obbligo di rendere l'informativa ai sensi dell'art. 13 del Codice.

Con il *provvedimento* in esame il Garante ha dichiarato inidonea l'informativa in quanto nel testo predisposto non risultava presente la circostanza che dati personali riferiti all'interessato potessero essere raccolti dalla società anche presso terzi (nel caso di specie, banche dati pubbliche e private), e ha conseguentemente prescritto di integrarla.

Da ultimo, con riferimento alla designazione degli esercizi commerciali convenzionati e/o dei rappresentanti legali dei punti vendita quali "incaricati del trattamento", l'Autorità ha sottolineato che sono tali solo le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile e in quanto operanti "*sotto la diretta autorità*" di questi, in presenza di un atto scritto di designazione e tenuti comunque ad attenersi alle istruzioni dai medesimi impartite (art. 4, lett. *h*) e 30 del Codice) (*cf.* *Prov. 8 giugno 1999* [*doc. web n. 42260*]). Con riferimento alla designazione del personale addetto alle vendite all'interno dei punti vendita convenzionati come "incaricati", inoltre, il Garante ha osservato che il rapporto di dipendenza o di collaborazione che tali soggetti hanno con l'esercizio commerciale convenzionato appare incompatibile con la qualifica di incaricati della società. Ciò non toglie che tali soggetti possono comunque porre in essere operazioni di trattamento anche a vantaggio della società, ma quali incaricati di tali operazioni di trattamento da parte del proprio datore di lavoro (previamente designato "responsabile del trattamento" dalla società).

L'Autorità ha quindi fissato un termine, correttamente osservato dalla società per l'attuazione delle prescrizioni formulate.

Nell'ambito del programma di ispezioni nei confronti di alcuni settori e categorie professionali, è emerso che un'agenzia immobiliare raccoglieva, oltre ai dati necessari per adempiere al proprio mandato (dati anagrafici, indirizzo, numero di telefono, ecc.), anche i dati sensibili delle persone che la contattavano per la compravendita o la locazione di una casa in quanto alcuni proprietari non avrebbero gradito stipulare contratti di locazione con extracomunitari, omosessuali o con persone di fede religiosa islamica.

**Trattamento
di dati
personali
presso agenzie di
intermediazione
immobiliare**

Con il *provvedimento* dell'11 gennaio 2007 [*doc. web n. 1381620*], accertata l'illiceità del trattamento, il Garante ha vietato all'agenzia immobiliare di utilizzare tali informazioni personali, in quanto discriminatorie e lesive della dignità delle persone, e in contrasto con quanto stabilito dal Codice e dalle autorizzazioni generali in materia di trattamento di dati sensibili (art. 2, 11, 26, 40 e 41 del Codice), oltre che in violazione delle norme sulla parità di trattamento tra le persone (art. 29, comma 1, lett. *d*), punto 9 l. n. 39/2002; art. 3, comma 1, lett. *i*) d.lg. n. 215/2003).

Il Garante ha inoltre prescritto all'agenzia di riformulare l'informativa, in particolare quella resa *on-line*, specificando chiaramente le finalità di utilizzo dei dati personali raccolti; si è inoltre rilevato che l'agenzia è tenuta inoltre a fornire indicazioni agli interessati circa la facoltà di rifiutare sin dall'inizio (oltre che in occasione di successive comunicazioni) l'utilizzo dell'indirizzo di posta elettronica per finalità di *marketing* (art. 130, comma 4, del Codice; in merito v. pure *Prov. 3 novembre 2005*, punto 3.2. [*doc. web n. 1195215*]).

È stata invece considerata lecita dal Garante la raccolta di informazioni relative ad *handicap* o patologie invalidanti in quanto effettuata dall'agenzia per escludere dalle trattative immobili con barriere architettoniche o privi di ascensore.

Nel 2007 il Garante ha avviato e concluso accertamenti sullo svolgimento dell'attività di recupero dei crediti, al fine di verificare l'osservanza delle prescrizioni contenute nel *provvedimento* generale del 30 novembre 2005 [doc. *web* n. [1213644](#)], a suo tempo trasmesso a tutte le società interessate dall'istruttoria.

**Recupero
crediti**

La maggior parte delle società interessate ha dichiarato nella sostanza di aver adeguato le proprie procedure interne alle prescrizioni del Garante.

Tuttavia, in considerazione di ulteriori segnalazioni pervenute, è emerso che persistevano prassi finalizzate al recupero stragiudiziale dei crediti caratterizzate da modalità di ricerca e di presa di contatto del debitore invasive e, talora, lesive della riservatezza e della dignità personale.

L'Autorità ha così provveduto –anche avvalendosi dell'ausilio della Guardia di finanza– a inviare richieste più analitiche di informazioni ai sensi dell'art. 157 del Codice nei confronti di sette società che, a vario titolo, effettuano il recupero stragiudiziale del credito.

Dalle risultanze ispettive è emerso che, complessivamente, le società operanti nel settore hanno rispettato le prescrizioni del Garante contenute nel *provvedimento* del 30 novembre 2005.

Un profilo di criticità, emerso anche nel corso di un incontro con l'associazione di categoria (Unirec-Unione nazionale imprese recupero crediti e informazioni commerciali), attiene alla qualificazione soggettiva delle società di recupero crediti quando operano quali mandatarie nell'attività di riscossione. In particolare, talvolta esse vengono designate quali "responsabili del trattamento"; talora, invece, appaiono assumere il ruolo di "titolari del trattamento" (pur operando quali mandatarie del creditore o, comunque, nell'ambito dell'appalto di servizi nell'attività di recupero dei crediti e salva ogni ulteriore verifica in ordine al consenso prestato dalla clientela a tale comunicazione a terzi).

Una società ha chiesto chiarimenti sulla parte del *provvedimento* nella quale si prevede che integri un illecito trattamento il ricorso a comunicazioni telefoniche preregistrate volte a sollecitare i pagamenti dovuti.

**Trattamento
di dati
personali
in sede
di recupero
credito
mediante
sistemi
automatizzati
di chiamata**

Con *Nota* 1 giugno 2007 l'Autorità ha precisato che non deve ritenersi precluso l'utilizzo di comunicazioni telefoniche senza l'intervento di un operatore per sollecitare pagamenti, ma che l'impiego di tale modalità –proprio in considerazione delle specifiche caratteristiche del mezzo usato, oltre che del contenuto del messaggio trasmesso– implica il rischio di comunicare a soggetti diversi dall'interessato, in assenza di sua espressa autorizzazione (art. 4, comma 1, lett. *l*) del Codice), dati personali riferiti al debitore e, in particolare, il suo asserito inadempimento.

Pertanto, in questi casi è necessario che il trattamento delle informazioni riferite ai debitori con le modalità anzidette si svolga nel pieno rispetto della disciplina in materia di protezione dei dati personali e in presenza dei presupposti di liceità del trattamento previsti dal Codice.

A questo riguardo sono state fornite ulteriori indicazioni ricordando che, in generale, la società che intenda avvalersi del meccanismo di chiamate preregistrate, anche senza l'ausilio di un operatore, è tenuta a dotarsi di idonei meccanismi a tutela della riservatezza degli interessati.

A tal fine potrebbe essere fornito al cliente, in sede di conclusione del contratto, un codice identificativo personale (di agevole memorizzazione) da digitare sull'apparecchio telefonico per ascoltare eventuali comunicazioni preregistrate a lui dirette, sì da scongiurare che comunicazione di dati personali riferiti al debitore siano resi noti a terzi che, per le ragioni più varie, utilizzino la medesima utenza telefonica.

Diversamente, ove si adottino modalità di trattamento di dati personali suscettibili di determinare una comunicazione a terzi di dati personali (non necessaria ai fini dell'esecuzione del contratto), è indispensabile, in assenza di altri presupposti di liceità del trattamento (artt. 24 e 25 del Codice), che i committenti, in qualità di titolari del trattamento (artt. 4, comma 1, lett. *f*) e 28 del Codice), acquisiscano uno specifico consenso informato dell'interessato alla comunicazione di dati a terzi (nel caso di specie, da individuarsi nei soggetti che potrebbero far uso dell'utenza telefonica attribuita al debitore) (artt. 13 e 23 del Codice).

Si è infine richiamata l'attenzione sul generale obbligo di informativa, in sede di raccolta delle informazioni personali della clientela: in tale occasione, con riferimento all'attività di recupero crediti, devono essere chiarite le "*modalità del trattamento cui sono destinati i dati*" (art. 13, comma 1, lett. *a*) del Codice), nonché indicati i "*soggetti o le categorie di soggetti ai quali i dati possono essere comunicati*" (art. 13, comma 1, lett. *d*) (nell'ipotesi indicata al punto 4, i soggetti che possono rispondere all'utenza telefonica del debitore) o che "*possono venire a conoscenza in qualità di responsabili o incaricati e l'ambito di diffusione degli stessi*" (dipendenti, collaboratori, anche società di recupero crediti, se nominate responsabili).

Per quanto concerne l'impiego di dispositivi atti a consentire l'ascolto di conversazioni a soggetti diversi dagli utenti, è pervenuta all'Autorità una segnalazione con cui si contestava un utilizzo indebito del cd. "viva voce" da parte di una società di gestione del credito. L'Autorità, nell'invitare quest'ultima a fornire chiarimenti, ha ricordato che l'art. 131, comma 3, del Codice impone all'utente di informare l'altro utente "*quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti*". Tale obbligo discende direttamente dal più generale principio di lealtà e correttezza che deve informare ogni trattamento di dati personali (art. 11, comma 1, lett. *a*) del Codice). All'esito degli accertamenti preliminari effettuati, nel prendere atto delle dichiarazioni rese dalla società ai sensi e per gli effetti di cui all'art. 168 del Codice non si sono ravvisati elementi per adottare un provvedimento (*Nota* 29 febbraio 2008).

Vivavoce

stampa

chiudi