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'abito dei sistemi di pagamento.

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

Le "Linee-guida in materia di trattamento di dati personali della clientela in ambito bancario" (*Provv.* 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 (ciò, in particolare, in relazione alla cessione degli sportelli bancari).

Oltre a ribadire la necessità di scrupoloso rispetto dei princìpi 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 antiriciclaggio 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 procedente 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).

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

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).

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 (*Provv.* 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'idonea 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.

Accessi abusivi a informazioni personali da parte di incaricati

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).

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 2008 [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 giustifichino. 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.

La vicenda Swift

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.

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 *SwifiNet* 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 versi 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 Sebc 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.

Iban (International banking account number)

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.

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).

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

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 conforme 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.

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*

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

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 princìpi in materia di protezione dati (*v. par.* 20.1).

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 venirne a conoscenza quali "responsabili del trattamento".

Per evitare un impiego di mezzi sproporzionato rispetto al diritto tutelato (*Provv.* 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'idonea informativa anche nell'interesse degli altri titolari del tratta-

mento (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).

Prodotti finanziari emessi da imprese di assicurazione e notificazione del trattamento

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).

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.

Le Linee-guida del Garante

Con le "Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico" (*Provv.* 14 giugno 2007 [doc. *web* n. 1417809]), nel quadro della tendenziale uniformità dei princìpi 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.

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, 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 princìpi 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'oblìo" (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).

Pubblicazione di corrispondenza in bacheca

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).

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'oblìo" trascorso un certo periodo di tempo dal verificarsi delle vicende dalle quali è originata l'affissione (*Nota* 23 gennaio 2008).

Comunicazione di dati sensibili tra enti locali

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.

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.

Rete socio-istituzionale di contrasto al lavoro irregolare

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.

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).

Modalità di consegna dei "cedolini" dello stipendio

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], *Provv.* 31 ottobre 2007 [doc. *web* n. 1459297]).

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

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).

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).

Affissione all'albo di delibere riferite a dipendenti

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).

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 (*cfr. Provv.* 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 tratta-

mento 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 princìpi 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; *Provv.* 12 gennaio 2004 [doc. *web* n. 1053395]; *Provv.* 23 novembre 2006 [doc. *web* n. 1364099]).

Forze armate e di polizia

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.

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 princìpi 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"*, *Provv.* 1 marzo 2007 [doc. *web* n. 1387522]).

Internet e posta elettronica

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 telefonico; Parere 28 novembre 2006, relativo all'ammissibilità di controlli a distanza mediante un *computer* palmare); si sono inoltre considerate le decisioni delle mas-

sime 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 princìpi 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 giustificherebbero 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 prevengano 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 princìpi 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 princìpi 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).

Strumenti di localizzazione satellitare dei lavoratori

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).

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

Biometria e luoghi di lavoro

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 (*cfr. Provv.* 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 presenza, commisurazione dei tempi di lavoro, *ecc.*).

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.

Buste paga

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.

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 princìpi, 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).

Ferie e permessi

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 propo-

sito, 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).

Tesserini identificativi dei dipendenti

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.

Sanzioni disciplinari

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.

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 princìpi 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.

Assenze per malattia e controlli datoriali

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 "dia-