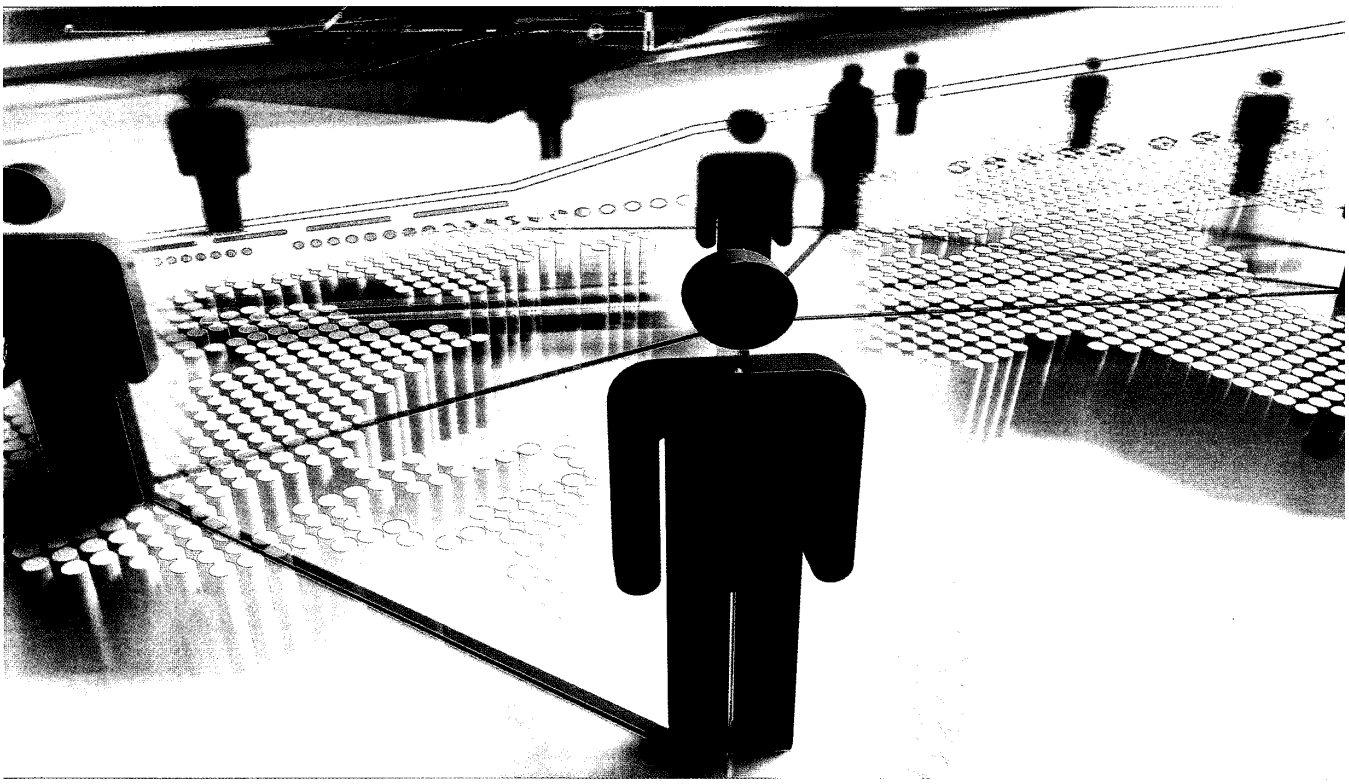

Stato di attuazione del Codice in materia di protezione dei dati personali

PAGINA BIANCA

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

1. Principali interventi dell'Autorità nel 2008

1.1. Provvedimenti più significativi

1.1.1. Trattamenti collegati allo svolgimento di funzioni di giustizia e di sicurezza pubblica

I trattamenti di dati effettuati per lo svolgimento di funzioni di giustizia e sicurezza pubblica hanno un considerevole impatto sulle persone interessate, come risulta dagli atti adottati nel 2008 dal Garante per assicurare il rispetto dei princìpi sulla protezione dati in questi delicati settori.

Con le *"Linee-guida in materia di trattamento di dati personali da parte dei consulenti tecnici e dei periti ausiliari del giudice e del pubblico ministero"* (*Provv.* 26 giugno 2008 [doc. *web* n. 1534086]) è stato individuato un quadro unitario di misure e di accorgimenti relativi ai trattamenti di consulenti tecnici e periti dell'Autorità giudiziaria. Tali trattamenti devono svolgersi nel rispetto dei princìpi di liceità e qualità dei dati (art. 11 del Codice), e devono essere adottate le necessarie misure di sicurezza (artt. 31 e ss. e disciplinare tecnico Allegato B. al Codice).

Il 27 ottobre 2008 è stato sottoscritto da parte delle associazioni rappresentative dell'avvocatura e degli investigatori privati il *"Codice di deontologia e di buona condotta per il trattamento di dati personali effettuato per svolgere le investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria"* (adottato con *Provv.* 6 novembre 2008, in *G.U.* 24 novembre 2008, n. 275 in vigore dal 1° gennaio 2009 [doc. *web* n. 1565171]).

Il codice per le indagini difensive, il cui rispetto costituisce condizione essenziale per la liceità e la correttezza dei trattamenti di dati personali (art. 12, comma 3, del Codice), disciplina in particolare i tempi di conservazione delle informazioni, i rapporti con i terzi

e la stampa e le modalità di trattamento dei dati personali, specie per quanto attiene all'essenzialità ed alla pertinenza dei dati trattati.

Con il *provvedimento* del 13 marzo 2008 sono state confermate le prescrizioni impartite l'8 maggio 2007 al Dipartimento di Pubblica sicurezza del Ministero dell'Interno sul trattamento dei dati da parte del Ced, con riferimento, in particolare, alla pertinenza e all'aggiornamento e ai tempi di conservazione dei dati, alle informazioni acquisite da soggetti pubblici, alla connessione con altre banche dati e all'esercizio dei diritti da parte degli interessati (*v. Relazione* 2007, *p.* 69).

Anche le prescrizioni impartite il 15 novembre 2007 al Tribunale ordinario di Roma, ai sensi dell'art. 160 del Codice, volte a rafforzare il livello di protezione dei dati personali trattati ai sensi dell'art. 47, comma 2, del Codice sono rimaste in gran parte inattuate (*v. Relazione* 2007, *p.* 127).

L'attuazione di tali prescrizioni dipende, in misura preponderante, da misure strutturali – oltre che dalla disponibilità delle indispensabili risorse finanziarie – di competenza del Ministero della giustizia, in relazione alle sue attribuzioni in tema di organizzazione e funzionamento dei servizi relativi alla giustizia.

Con *provvedimento* del 13 ottobre 2008 è stata rappresentata, pertanto, al Ministero della giustizia la necessità di fornire al Tribunale ordinario di Roma le risorse necessarie ad attuare le prescrizioni impartite con il citato *provvedimento* del 2007, che sono state confermate, invitando altresì il Ministero ad un tempestivo riscontro circa le determinazioni da adottare.

Di rilievo anche il *provvedimento* del 29 maggio 2008 [doc. *web* n. 1537606], relativo al trattamento dei dati nel sistema Eurodac per l'esame delle domande di asilo presentate ad uno Stato membro e in applicazione della Convenzione di Dublino (regolamento Ce n. 2725/2000). In particolare, il citato *provvedimento* ha ad oggetto il confronto delle impronte digitali dei richiedenti l'asilo registrate già presso l'unità centrale al fine di concorrere alla determinazione dello Stato membro competente.

Le prescrizioni impartite sono relative, tra l'altro, all'individuazione del titolare e degli eventuali responsabili del trattamento, all'informativa da fornire agli interessati, anche per

consentire loro l'esercizio del diritto di accesso e degli altri diritti collegati, alle misure per garantire la sicurezza del trattamento nelle diverse operazioni compiute.

1.1.2. Trattamento dei dati di traffico telefonico e telematico

Con *provvedimento* del 24 luglio 2008 (*G.U.* 13 agosto 2008, n. 189 [doc. *web* n. 1538224]) è stato individuato il termine del 30 aprile 2009 entro il quale i gestori telefonici devono mettersi in regola con le prescrizioni che l'Autorità aveva già individuato nel *provvedimento* 17 gennaio 2008 (*G.U.* 5 febbraio 2008, n. 30 [doc. *web* n. 1482111]) per garantire elevati *standard* tecnologici ed organizzativi a protezione dei dati di milioni di utenti. Il *provvedimento* del 24 luglio reca in allegato il testo aggiornato del *provvedimento* del 17 gennaio 2008 (*v. Relazione* 2007, *p.* 122 ss.).

Il nuovo *provvedimento* si è reso necessario anche per le novità introdotte dalla Convenzione del Consiglio d'Europa sul *cybercrime* (ratificata dall'Italia con la l. n. 48/2008) e, soprattutto, dalla direttiva 2006/24/Ce, *cd. "direttiva Frattini"* (recepita con il d.lg. n. 109/2008), che ha ridotto i tempi di conservazione dei dati di traffico telefonico: due anni per il traffico telefonico e un anno per quello telematico. Nel gennaio 2008, all'epoca del primo *provvedimento* del Garante, i dati di traffico telefonico potevano invece essere conservati, per essere utilizzati solo in caso di indagini penali, fino ad otto anni, mentre quelli di traffico telematico fino a circa quattro anni.

Con il *provvedimento* del 29 aprile 2009 (in corso di pubblicazione nella *Gazzetta Ufficiale* [doc. *web* n. 1612508]), l'Autorità ha fissato al 15 dicembre 2009, limitatamente alle misure specificamente indicate, il nuovo termine per adempiere, prevedendo altresì che, entro la medesima data, tutti i titolari del trattamento interessati debbano dare conferma al Garante delle misure e degli accorgimenti adottati, attestandone l'integrale adempimento.

Il termine tiene conto anche delle istanze pervenute da Asstel e da Assoprovider, associazioni che rappresentano le società che forniscono servizi di telecomunicazioni, che hanno chiesto ampi margini di tempo per completare l'adozione delle complesse misure di sicurezza indicate nel *provvedimento* del luglio 2008.

1.1.3. Sicurezza e trasparenza dei dati relativi all'attività tributaria

Anagrafe tributaria: sicurezza e accessi

L'attività tributaria presenta, da un lato, esigenze di trasparenza da ricollegare all'obbligo sancito dalla Costituzione di contribuire alle spese pubbliche in ragione della capacità contributiva, dall'altro, esigenze di sicurezza per la delicatezza e la rilevanza dei dati trattati, e in primo luogo per prevenire accessi impropri ai dati medesimi.

Nel 2008 entrambi i profili sono stati oggetto di provvedimenti del Garante.

Più in particolare, al termine della prima fase dell'attività ispettiva del Garante sull'Anagrafe tributaria (*v. Relazione* 2007, *p.* 49) sono stati riscontrati molti punti di criticità: mancata conoscenza del numero complessivo degli utenti che accedono al sistema informativo e della loro effettiva identità; scarsa capacità di monitoraggio su eventuali accessi anomali o utilizzi impropri di *password* e credenziali; inadeguate misure tecnologiche a protezione dei dati contenuti nel *database*.

Per porre rimedio alle carenze riscontrate e rendere il trattamento dei dati conforme alle norme sulla protezione dei dati l'Autorità ha imposto all'Agenzia delle entrate, con *provvedimento* del 18 settembre 2008 [doc. *web* n. 1549548] un'articolata serie di misure, tecnologiche ed organizzative, in particolare per innalzare i livelli di sicurezza degli accessi all'Anagrafe tributaria da parte degli enti esterni. Le misure dovranno essere adottate dall'Agenzia delle entrate entro un periodo che va da tre mesi ad un anno, a seconda della complessità degli adempimenti.

L'iniziativa va inquadrata in un più ampio programma di controllo sul sistema informativo della fiscalità, volto anche ad anticipare l'enorme lavoro di messa in sicurezza della gestione delle banche dati, tributarie e fiscali, che la realizzazione del federalismo fiscale renderà sempre più complessa e strategica.

Pubblicazione *on-line* dei dati dei contribuenti da parte dell'Agenzia delle entrate

L'Autorità era in precedenza intervenuta in via d'urgenza (*Provv.* 30 aprile 2008 [doc. *web* n. 1510761]) sulla pubblicazione, nel sito Internet dell'Agenzia delle entrate, dei dati relativi ai contribuenti per l'anno d'imposta 2005, decisa, senza acquisire il parere del Garante, dal Direttore dell'Agenzia delle entrate.

La forma di diffusione adottata poneva, infatti, evidenti problemi di conformità con il quadro normativo in materia. L'Autorità, il 30 aprile, ha chiesto ulteriori delucidazioni

all'Agenzia, invitandola a sospendere la diffusione dei dati su Internet.

Con *provvedimento* del 6 maggio 2008 [doc. *web* n. 1512255] poi, a conclusione dell'istruttoria, ha stabilito che la modalità utilizzata dall'Agenzia è stata illegittima, poiché contrastava con la disposizione secondo cui all'Agenzia spetta solo il compito di fissare annualmente le modalità di formazione degli elenchi delle dichiarazioni dei redditi, non le modalità della loro pubblicazione, che rimangono prerogativa del legislatore.

In seguito, la modifica dell'art. 69 del d.P.R. 29 settembre 1973, n. 600 (*cfr.* art. 42, d.l. 25 giugno 2008, n. 112, convertito, con modificazioni, in l. 6 agosto 2008, n. 133), ha ammesso la visione e l'estrazione di copia degli elenchi nei modi e con i limiti stabiliti dalla disciplina in materia di accesso ai documenti amministrativi, nonché da specifiche disposizioni di legge, durante l'anno di deposito degli elenchi presso i comuni e gli uffici dell'Agenzia.

1.1.4. Giornalismo - Dati di vittime di abusi. Accessibilità on-line *di archivi storici dei quotidiani*

Il delicato bilanciamento tra libertà d'informazione e diritto alla riservatezza ha impegnato il Garante nel 2008 in relazione a diversi aspetti dell'attività giornalistica.

In particolare con riferimento a tre episodi di violenza sessuale, l'Autorità è intervenuta (*Provv.* 10 luglio 2008 [doc. *web* n. 1536583], 2 ottobre 2008 [doc. *web* n. 1557470], 16 febbraio 2009 [doc. *web* n. 1590076]), come in precedenti occasioni (*v. Relazione* 2007, *p.* 73-74), nei confronti di testate giornalistiche che hanno violato le specifiche garanzie poste a tutela delle vittime. In particolare, oggetto dei citati interventi è stata la pubblicazione di numerosi dettagli (tra i quali iniziali di nome e cognome delle vittime, quartiere di residenza, professione dei genitori e di parenti, luoghi di villeggiatura frequentati, *ecc.*) la cui compresenza nel servizio giornalistico (diversamente articolata nei tre casi esaminati) era idonea a rendere identificabili le vittime stesse. Nei riguardi delle testate è stato disposto un divieto del trattamento per la violazione del principio di *"essenzialità dell'informazione"* (art. 137, comma 3, del Codice) e delle specifiche disposizioni a tutela dei minori (*v.* in particolare, art. 114, comma 6, c.p.p.; art. 7 del codice di deon-

tologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica; Carta di Treviso).

Presentano, invece, caratteri di novità le questioni connesse alla libera disponibilità degli archivi storici *on-line* dei principali quotidiani.

Tale disponibilità ha comportato che, anche attraverso i motori di ricerca, notizie risalenti nel tempo (spesso legate alla cronaca giudiziaria) divengano facilmente rintracciabili, proiettando un'immagine negativa dei protagonisti, anche quando il tempo trascorso ha invece portato ad un loro naturale oblio.

Del contrasto fra le esigenze conoscitive e quelle, contrapposte, di tutela della riservatezza è significativo esempio la decisione adottata su ricorso l'11 dicembre 2008 [doc. *web* n. 1583162].

Accogliendo, seppur in parte, la domanda dell'interessato, a suo tempo coinvolto in un'inchiesta penale, l'Autorità ha voluto evitare gli effetti pregiudizievoli derivanti dalla rappresentazione istantanea e cumulativa, ottenuta con l'utilizzo di motori di ricerca, di fatti ormai risalenti. A tal fine si è ordinato all'editore di adottare ogni misura tecnicamente idonea ad evitare che le generalità del ricorrente contenute nell'articolo di un quotidiano continuino ad essere rinvenibili direttamente attraverso l'utilizzo dei motori di ricerca generalisti, ferma rimanendo la possibilità di consultare la versione integrale dell'articolo medesimo accedendo direttamente al sito *web* dell'editore.

La soluzione mira al contemperamento fra due interessi confliggenti e la sua tenuta potrà essere verificata in progresso di tempo in relazione alla molteplicità delle fattispecie concrete (in materia *v.* anche le decisioni adottate l'11 dicembre 2008 [doc. *web* n. 1582866] ed il 19 dicembre 2008 [doc. *web* n. 1583152]).

1.1.5. Iniziativa economica: profilazioni personalizzate e marketing *telefonico*

L'utilizzo a fini commerciali di dati personali può risultare in contrasto con la normativa in materia, sia per ragioni inerenti alla qualità dei dati trattati, sia per quanto riguarda i presupposti stessi del trattamento e, in particolare, il consenso dell'interessato. Di entrambi i profili, talora connessi, si è occupato il Garante nel 2008.

Informazioni commerciali

L'improprio trattamento dei dati relativi ad informazioni commerciali è stato oggetto di diversi provvedimenti del Garante, tra i quali uno – relativo al maggiore operatore del settore (*Provv.* 30 ottobre 2008 [doc. *web* n. 1570327]) ed adottato in esito ad un'approfondita istruttoria in relazione a numerosi reclami e segnalazioni degli interessati – utile a fornire indicazioni di carattere generale sull'applicazione, anche in tale materia, del principio di pertinenza dei dati (art. 11 del Codice).

Le informazioni commerciali esprimono, seppure in forma sintetica, apprezzamenti sull'affidabilità degli operatori economici e, se non pienamente soddisfacenti, sostanziano in modo particolarmente rilevante il pregiudizio per gli interessati.

In sintesi, dall'attività svolta è risultato che in diversi casi il *"dossier persona"* relativo ad un individuo, conteneva informazioni riferibili a terzi (*v.* anche, *infra par.* 17.2.4, decisione su ricorso del 12 giugno 2008 [doc *web* n. 1537684] sull'arbitrario accostamento fra l'interessato ed il fallimento di una società di cui lo stesso era stato socio accomandante).

Anche gli elementi utilizzati per le valutazioni sintetiche sull'affidabilità commerciale degli interessati sono risultati talora riconducibili a soggetti diversi dall'interessato (*ad es.*, riferiti anche a eventi – talora negativi – riconducibili a *"imprese connesse"*) e perciò in contrasto con i princìpi di correttezza, pertinenza e non eccedenza, oltre che in violazione del diritto all'identità personale (artt. 2 e 11 del Codice).

Inoltre, è emerso che la società ha utilizzato congiuntamente (e indifferentemente), per classificare l'affidabilità degli operatori, un indice costituito da due aggettivi – nullo/basso – e che la modalità di utilizzo di tali aggettivi, che non sono sinonimi, non forniva un quadro chiaro dell'affidabilità commerciale del soggetto censito.

L'associazione impropria degli elementi è stata ritenuta non pertinente, anche per la possibile alterazione della proiezione sociale e professionale che può derivarne al soggetto censito e la lesione del diritto all'identità personale (art. 2 del Codice).

I *dossier* contenenti indici sull'affidabilità commerciale dei soggetti censiti sono risultati essere non – come prospettato dalla società – mere sintesi di informazioni tratte da pubblici registri, bensì autonome valutazioni, sulla base di un peso ponderato attribuito alle diverse informazioni e, come tali, dati personali autonomi, distinti dalle informazioni

originarie ricavate dalle fonti pubbliche, il cui trattamento – a differenza di quello relativo a dati pubblicamente disponibili – necessita del consenso degli interessati (art. 23 del Codice) o di altro presupposto equipollente previsto dall'art. 24 del Codice.

Nel corso degli accertamenti è emerso, inoltre, che la società non solo trattava informazioni eccessive e non pertinenti, ma raccoglieva anche dati personali da fonti dalle quali non poteva attingere, come le liste elettorali, o addirittura le dichiarazioni dei redditi del 2005, acquisite in occasione della loro messa *on-line* da parte dell'Agenzia delle entrate (diffusione dichiarata dall'Autorità illegittima *v. supra* n. 1.1.3).

È stata perciò prescritta alla società l'adozione di ogni misura necessaria e idonea ad evitare l'associazione a un soggetto di informazioni al medesimo non direttamente riconducibili.

Il Garante ha altresì prescritto alla società di tenere distinti i casi in cui l'indice sia *"basso"* da quelli in cui sia *"nullo"* e ha inoltre vietato alla medesima, in particolare: l'utilizzo di informazioni non pertinenti agli interessati per l'elaborazione degli indici sintetici; il trattamento per le finalità dichiarate dalla società dei dati provenienti dalle liste elettorali; il trattamento dei dati relativi alle dichiarazioni dei redditi pubblicati dall'Agenzia delle entrate, con prescrizione di cancellarli.

Divieto di utilizzo di banche dati a fini di *marketing* telefonico

L'altro profilo, riguardante il consenso degli interessati, è emerso con particolare rilievo nei provvedimenti relativi all'utilizzo di banche dati a fini di *marketing* telefonico, dapprima vietato dal Garante per l'assenza di consenso dell'interessato, poi consentito sino al 31 dicembre 2009 da una modifica normativa e, di conseguenza, oggetto di nuovo *provvedimento* dell'Autorità.

I provvedimenti inibitori del 26 giugno 2008 [doc. *web* nn. 1544315, 1544326, 1544338] sono stati emanati dopo verifiche svolte, su segnalazioni di numerosi abbonati, presso le società che hanno fornito i *database*. Dagli accertamenti è emerso che i dati degli utenti erano stati raccolti e ceduti a terzi senza informare gli interessati, o informandoli in maniera inadeguata, e senza un loro preventivo specifico consenso. Una delle società offriva sul proprio sito i dati di oltre quindici milioni di famiglie italiane suddivise per redditi e stili di vita, senza che gli interessati fossero stati informati o avessero dato il loro assenso alla comunicazione dei dati a terzi.

Da parte loro le aziende e le compagnie telefoniche che hanno acquistato i dati, utilizzandoli a fini di *marketing* telefonico, non si erano preoccupate di accertare, come prevede invece la disciplina sulla protezione dei dati, che gli abbonati avessero acconsentito alla comunicazione dei propri dati e al loro uso a fini commerciali.

Successivamente, l'art. 44, comma 1-*bis* del d.l. 30 dicembre 2008, n. 207, convertito, con modificazioni, in l. 27 febbraio 2009, n. 14 (*G.U.* 28 febbraio 2009, n. 28), ha stabilito che i dati personali presenti nelle banche dati costituite sulla base dei vecchi elenchi telefonici sono utilizzabili per fini promozionali fino al 31 dicembre 2009 da coloro che hanno creato tali banche dati precedentemente al 1° agosto 2005. Il *provvedimento* del 12 marzo 2009 (*G.U.* 20 marzo 2009, n. 66 [doc. *web* n. 1598808]) precisa i limiti entro i quali le società che effettuano attività promozionale, anche tramite *call center*, possono avvalersi della deroga.

Il mancato rispetto delle prescrizioni del *provvedimento* comporta una sanzione amministrativa che va da trentamila a centottantamila euro e che, nei casi più gravi, può raggiungere anche i trecentomila euro. In sintesi, le società devono documentare in modo adeguato che la banca dati, costituita con i numeri telefonici e gli indirizzi degli abbonati, sia stata effettivamente creata prima del 1° agosto 2005. Esse devono usare questi dati direttamente e non possono cederli a nessun titolo ad altre aziende.

L'eventuale contrarietà dell'abbonato ad essere nuovamente contattato deve essere registrata immediatamente dall'operatore, tenuto, se richiesto, a comunicare all'abbonato stesso il suo identificativo. I dati non possono in alcun modo essere usati per acquisire nuove informazioni o il consenso degli abbonati ad effettuare chiamate dopo la data del 31 dicembre 2009, poiché in tal modo gli effetti della temporanea deroga verrebbero a protrarsi oltre il termine previsto dal legislatore.

Le società che svolgono attività di *marketing* devono comunicare al Garante, entro quindici giorni dalla pubblicazione in *Gazzetta Ufficiale* del *provvedimento*, di essere in possesso di banche dati costituite anteriormente al 1° agosto 2005 e di volerle utilizzare per attività promozionali, chiarendo se il trattamento di dati venga effettuato anche per conto terzi.

1.1.6. Protezione dei dati dei lavoratori dipendenti e dei collaboratori

In questo settore gli interventi del Garante sono stati relativi principalmente alla trasparenza del trattamento, per evitare utilizzi dei dati non oggetto di informativa agli interessati, al rispetto delle forme di legge per il controllo a distanza dei lavoratori (art. 4 della l. n. 300/1970), alla qualità dei dati, perlopiù per evitare il trattamento di dati non pertinenti.

In termini generali, esprimendo il parere previsto dall'art. 154 del Codice (*Provv.* 31 marzo 2008 [doc. *web* n. 1504941]) sullo schema di decreto legislativo volto a dare attuazione alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza nei luoghi di lavoro, è stata evidenziata l'esigenza di verificare l'indispensabilità e la necessità dei dati da trattare, di adottare le misure di sicurezza necessarie e di salvaguardare il segreto professionale.

Accogliendo il reclamo di un'organizzazione sindacale (*Provv.* 2 aprile 2008 [doc. *web.* n. 1519695]) è stato bloccato – nelle more dell'espletamento delle procedure di legge – l'ulteriore trattamento dei dati dei dipendenti di una compagnia aerea, limitatamente alle informazioni connesse all'utilizzo per finalità formative di *computer* portatili. È, infatti, emerso che le funzioni di tracciamento e registrazione degli accessi al corso di formazione, utili al monitoraggio dell'andamento del processo formativo, erano idonee al controllo a distanza dell'attività lavorativa dei dipendenti, ciò senza l'osservanza delle procedure a tal fine richieste dall'art. 4 della l. n. 300/1970, oltre che in assenza dell'informativa agli interessati e del loro consenso.

Sistemi di localizzazione, *event data recorder* e servizi di trasporto pubblico

Per garantire la sicurezza dei passeggeri e l'efficienza del servizio è stato consentito ad una società di trasporto pubblico, in sede di verifica preliminare (*Provv.* 5 giugno 2008 [doc. *web* n. 1531604]), l'utilizzo di sistemi di localizzazione e di registrazione di *"eventi di guida"*, previo rispetto delle procedure previste dallo Statuto dei lavoratori.

Il sistema prevede il riconoscimento attraverso un codice identificativo cifrato del conducente del veicolo, al quale – direttamente o anche in un secondo tempo – possono essere associati tutti i dati ricavati dal sistema. Le garanzie procedurali previste dall'art. 4 della l. n. 300/1970 (accordo sindacale o autorizzazione della Direzione provinciale del

lavoro) dovranno essere rispettate poiché il sistema può determinare un controllo a distanza dei lavoratori, ancorché giustificato da esigenze organizzative e produttive della società.

I dati raccolti dovrebbero confluire in un *database* gestito dal fornitore del servizio e fruibile dall'azienda grazie ad un portale (compreso anch'esso nel progetto) al quale si accederà solamente attraverso l'utilizzo di un sistema identificativo comprensivo di *userId* e *password*.

Il Garante ha stabilito, inoltre, che siano fornite agli interessati informazioni dettagliate sulla natura dei dati trattati e sulle caratteristiche del sistema e che l'accesso ai dati dovrà essere consentito ai soli incaricati della società. L'Autorità ha sottolineato, infine, che le informazioni ricavate da tale sistema di localizzazione potranno essere utilizzate a fini di sicurezza e miglioramento del servizio e conservate per il tempo necessario a perseguire le finalità indicate nel provvedimento.

Comunicazione a terzi di dati relativi a procedimenti penali pendenti

Decidendo su un reclamo, l'Autorità ha vietato a due società l'ulteriore comunicazione a terzi di dati personali relativi, tra l'altro, ad un procedimento penale a carico di una ex collaboratrice (*Provv.* 2 aprile 2008 [doc. *web* n. 1519711]), essendo stata la comunicazione effettuata in violazione dei princìpi di necessità e finalità (artt. 3 e 11, comma 1, lett. *b*), del Codice), oltre che in assenza della prescritta informativa. Il Garante ha rilevato che non era necessario dare notizia ai terzi del procedimento penale, essendo sufficiente comunicare l'interruzione del rapporto di collaborazione.

Trattamento di dati personali raccolti in occasione di programmi di fidelizzazione e loro utilizzo per fini disciplinari nell'ambito del rapporto di lavoro

Due divieti (*Provv.* 2 aprile 2008 [doc. *web* n. 1519679] e 6 novembre 2008 [doc. *web* n. 1573780]) sono stati emessi su istanze degli interessati, in relazione all'utilizzo per procedimenti disciplinari, sfociati in licenziamenti, di dati dei dipendenti raccolti per finalità di *marketing* e fidelizzazione (gli interessati, dipendenti di esercizi commerciali, "caricavano" sulla propria carta di fidelizzazione gli acquisti effettuati dalla clientela).

I dati acquisiti sono stati utilizzati anche per controllare l'esecuzione della prestazione lavorativa e l'osservanza dell'obbligo di fedeltà dei dipendenti anziché essere trattati, come sarebbe dovuto accadere in base all'informativa fornita agli interessati, nel solo ambito del programma di fidelizzazione.

Il Garante ha vietato pertanto alle due società di effettuare, nel contesto del rapporto di lavoro, ulteriori trattamenti dei dati connessi all'utilizzo della carta di fidelizzazione in violazione dei princìpi di liceità e finalità (artt. 11, comma 1, lett. *a*) e *b*), del Codice).

1.1.7. Adempimenti semplificati per finalità amministrative e in materia di sicurezza dei dati

L'esigenza di snellire gli adempimenti formali previsti dalla normativa, per dare maggior rilievo agli aspetti sostanziali che incidono sull'effettiva protezione dei dati degli interessati, ha portato all'adozione nel 2008 di importanti misure di semplificazione.

Semplificazione di taluni adempimenti rispetto a trattamenti per finalità amministrative e contabili

Con *provvedimento* del 19 giugno 2008 [doc. *web* n. 1526724] sono state individuate soluzioni per agevolare il trattamento dei dati nell'ordinaria attività di gestione amministrativa e contabile – in particolare nei casi in cui non sono trattati dati di carattere sensibile o giudiziario – enunciando nuove linee-guida interpretative della normativa ed individuando alcune modalità innovative per semplificare taluni adempimenti, in modo particolare per l'informativa agli interessati e il consenso.

In sostanza, l'Autorità ha fornito indicazioni per la redazione di un'informativa unica per il complesso dei trattamenti di dati personali a fini esclusivamente amministrativi e contabili; gli operatori potranno redigere una prima informativa breve che può rinviare a un testo più articolato, disponibile su siti Internet, reti Intranet, in bacheca o presso gli sportelli. Le associazioni di categoria sono state invitate a predisporre informative-tipo per determinati settori o categorie di trattamenti.

Per quanto riguarda il consenso sono stati indicati i casi in cui esso non è richiesto, ad esempio quando i trattamenti sono svolti per adempiere ad obblighi contrattuali o normativi o quando i dati provengono da registri o elenchi pubblici, o sono relativi allo svolgimento di attività economiche.

Semplificazione delle misure di sicurezza

Con *provvedimento* del 27 novembre 2008 (*G.U.* 9 dicembre 2008, n. 287 [doc. *web* n. 1571218]) sono state dettate modalità più snelle per l'applicazione delle misure di sicurezza alle attività di corrente gestione amministrativa e contabile, svolte specie presso piccole e medie imprese, liberi professionisti e artigiani, senza ridurre le garanzie per i cittadini.

In particolare, il *provvedimento* riguarda sia amministrazioni pubbliche e società private che utilizzano dati personali non sensibili o che trattano come unici dati sensibili dei dipendenti quelli relativi allo stato di salute o all'adesione a organizzazioni sindacali, sia piccole e medie imprese, liberi professionisti o artigiani che trattano dati solo per fini amministrativi e contabili.

In base al citato *provvedimento*, il Garante ha stabilito, tra l'altro, che le istruzioni in materia di misure minime possono essere impartite agli incaricati anche oralmente; per l'accesso ai sistemi informatici è possibile utilizzare qualsiasi sistema di autenticazione basato su un *username* e una *password*; l'*username* deve essere disattivato quando vengono meno le condizioni per il legittimo accesso ai dati. Con riguardo alle misure di sicurezza, i programmi volti a prevenire la vulnerabilità di strumenti elettronici (*ad es.*, gli antivirus) devono essere aggiornati almeno annualmente e i dati possono essere salvaguardati anche attraverso il loro salvataggio almeno mensile. Sono state anche fornite alcune indicazioni per la redazione del documento programmatico per la sicurezza semplificato ed indicate procedure più snelle per chi tratta dati senza l'impiego di sistemi informatici.

Semplificazione delle notificazioni

Il 22 ottobre 2008 il Garante ha adottato un *provvedimento* (*G.U.* 9 dicembre 2008, n. 287 [doc. *web* n. 1571196]) che semplifica il modello utilizzato per effettuare le notificazioni (*cfr.* art. 38 del Codice, come modificato dalla l. 6 agosto 2008, di conversione, con modificazioni, del d.l. 25 giugno 2008, n. 112), ossia le dichiarazioni da fare all'Autorità quando si intende avviare un trattamento di particolari tipi di dati (genetici, biometrici, procreazione assistita, *ecc.*). Il *provvedimento* sulla notificazione non comporta l'obbligo di notificare di nuovo o modificare le notificazioni a carico di chi lo abbia già fatto.

1.1.8. Prescrizioni in materia di gestione di sistemi complessi e di rottamazione di apparecchiature elettroniche

Amministratori di sistema

Con *provvedimento* del 27 novembre 2008 (*G.U.* 24 dicembre 2008, n. 300 [doc. *web* n. 1577499]) il Garante, in considerazione della particolare delicatezza delle funzioni di amministratore di sistema in una banca dati, ha fissato le regole per l'adozione, da parte

di enti, amministrazioni pubbliche e società private, delle misure tecniche e organizzative che riguardano tali peculiari figure, chiamate a svolgere delicate funzioni di gestione e manutenzione di un impianto di elaborazione, che comportano spesso la concreta possibilità di accedere a tutti i dati trattati informaticamente nelle banche dati.

Tali misure sono dirette a migliorare i criteri di individuazione degli amministratori di sistema, e ad agevolare la verifica sull'attività degli amministratori da parte di chi ha la titolarità delle banche dati e dei sistemi informatici, e non riguardano i trattamenti di dati effettuati a fini amministrativo-contabili, che pongono solitamente minori rischi per gli interessati.

In particolare, è prevista la registrazione degli accessi logici degli amministratori ai sistemi di elaborazione e agli archivi elettronici, da conservare per un periodo non inferiore a sei mesi. L'operato degli amministratori di sistema deve essere verificato almeno annualmente da parte dei titolari del trattamento, analogamente a quanto richiesto dal Codice relativamente ai responsabili. Gli estremi identificativi degli amministratori di sistema e l'elenco delle funzioni loro attribuite devono essere indicati in un documento disponibile in caso di accertamenti da parte del Garante.

L'Autorità, in ragione della complessità degli interventi necessari per l'adeguamento dei sistemi, su richiesta dalle associazioni degli operatori interessati ha prorogato i termini per gli adempimenti.

In particolare, dopo l'unificazione dei vari termini e il differimento al termine unico del 30 giugno 2009 (*Provv.* 12 febbraio 2009, in *G.U.* 24 febbraio 2009, n. 45 [doc. *web* n. 1591970]), ha avviato, con *provvedimento* del 21 aprile 2009 (in corso di pubblicazione in *Gazzetta Ufficiale* [doc. *web* n. 1611986]), una consultazione pubblica per *"acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del dispositivo del provvedimento del 27 novembre 2008"*.

Sicurezza dei dati personali nella rottamazione di apparecchiature elettroniche

Con *provvedimento* del 13 ottobre 2008 [doc. *web* n. 1571514] sono state indicate le misure organizzative e tecniche da adottare per garantire l'effettiva cancellazione (o la trasformazione in forma non intelligibile) dei dati personali contenuti in apparati elettrici ed