In base al provvedimento, in primo luogo, in conformità ai princìpi di necessità e proporzionalità, vanno preferiti, se possibile, dati anonimi e, comunque, raccolte solo immagini pertinenti e non eccedenti rispetto alle finalità perseguite (artt. 3 e 11, comma 1, lett. *d*), del Codice).

Gli interessati devono essere resi edotti dell'esistenza di sistemi di videosorveglianza. Al tal fine, si può utilizzare lo stesso modello semplificato di informativa "minima" messo a disposizione nel *provvedimento* del 2004 (art. 13, comma 3, del Codice). Inoltre, il supporto con l'informativa deve essere chiaramente visibile anche quando il sistema di videosorveglianza sia, eventualmente, attivo in orario notturno. È stato, altresì, predisposto un nuovo modello semplificato di informativa "minima" per i titolari del trattamento che intendono attivare un collegamento diretto con le forze di polizia.

E' tuttavia auspicabile, in particolare, che l'informativa semplificata rinvii ad un testo completo, contenente tutti gli elementi di cui all'art. 13, comma 1, del Codice, disponibile agevolmente e senza oneri per gli interessati.

Inoltre è stato prescritto che l'impiego di sistemi di raccolta delle immagini associate a dati biometrici e dei sistemi *cd. "intelligenti"* - capaci, cioè, di rilevare automaticamente comportamenti o eventi anomali, segnalarli, ed eventualmente registrarli - sia sottoposto alla verifica preliminare, trattandosi di attività di videosorveglianza che comporta rischi specifici per i diritti e le libertà fondamentali.

Per quanto riguarda le misure di sicurezza (artt. 30, 33 *ss.* e Allegato B. al Codice), l'Autorità ha disposto, in particolare, che: agli incaricati e responsabili del trattamento siano conferiti diversi livelli di visibilità e trattamento delle immagini, in relazione alle diverse competenze di ciascuno; siano limitate le ipotesi di visione delle immagini raccolte e registrate; siano predisposte specifiche misure per la cancellazione delle immagini conservate, anche tramite sistemi di sovra-registrazione; sia del tutto eccezionale l'accesso alle immagini nelle ipotesi di manutenzione del sistema; vengano disposti sistemi di protezione da accessi abusivi per gli apparati di ripresa digitali; siano applicate tecniche crittografiche nelle ipotesi di trasmissione di immagini da una rete pubblica o tramite connessioni *wireless*.

Fatte salve speciali esigenze di ulteriore conservazione in relazione alla chiusura di uffici o esercizi, o a specifica richiesta investigativa delle autorità preposte, le immagini devono essere conservate al massimo per ventiquattro ore, dopo la loro rilevazione. La cancellazione può avvenire anche tramite meccanismi automatici di rimozione dei dati obsoleti e gestione automatica delle *policy di retention.* E' ammesso un più ampio tempo di conservazione dei dati, non oltre la settimana, solo in alcuni casi correlati a peculiari esigenze tecniche o alla particolare rischiosità dell'attività svolta dal titolare del trattamento.

Per i comuni e nelle sole ipotesi in cui la videosorveglianza sia finalizzata alla tutela della sicurezza urbana, alla luce delle recenti disposizioni normative, il termine massimo di durata della conservazione dei dati è limitato *"ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione"*, per le quali, ferma restando l'eccezionalità dell'ipotesi, occorre richiedere una verifica preliminare del Garante.

Merita menzione la decisione dell'Autorità di ritenere lecita l'attività di videosorveglianza al fine sia di accertare l'utilizzo abusivo di aree impiegate come discariche di materiali e di sostanze pericolose, sia di monitorare il rispetto delle disposizioni concernenti modalità, tipologia ed orario di deposito dei rifiuti, sempreché tali finalità non possano essere perseguite senza ricorrere al trattamento di dati personali.

La videosorveglianza può essere effettuata da soggetti pubblici, nel rispetto del principio di finalità, per lo svolgimento delle proprie funzioni istituzionali e fornendo previamente idonea informativa agli interessati, anche nei casi in cui i sindaci, quali ufficiali del Governo, ed i comuni utilizzano sistemi di videosorveglianza in luoghi pubblici o aperti al pubblico al fine di tutelare la sicurezza urbana.

La rilevazione di immagini tramite sistemi di videosorveglianza svolta da soggetti privati può avere legittimamente luogo previa acquisizione del consenso degli interessati o in presenza di un requisito equipollente (artt. 23 e 24 del Codice). A tal proposito, il *provvedimento* ha individuato i casi in cui - al fine di perseguire un legittimo interesse del titolare o di un terzo attraverso la raccolta di mezzi di prova o perseguendo fini di tutela di persone e beni rispetto a possibili aggressioni, furti, rapine, danneggiamenti, atti di

vandalismo, o per finalità di prevenzione di incendi o di sicurezza del lavoro - la rilevazione di immagini da parte di soggetti privati può avvenire senza previa acquisizione del consenso degli interessati.

Il Garante ha affrontato anche il tema della videosorveglianza nei condomìni, evidenziando che è stata inoltrata una segnalazione al Governo e al Parlamento volta a sollecitare la disciplina di problemi applicativi emersi negli ultimi anni, concernenti, in particolare, la competenza e le modalità di delibera dell'assemblea condominiale ai fini dell'istallazione degli impianti di videosorveglianza.

Con riferimento ai *cd. "sistemi integrati di videosorveglianza"* tra diversi soggetti, sia pubblici che privati, sono state previste specifiche garanzie relative ai trattamenti di dati effettuati mediante: la gestione coordinata di funzioni e servizi tramite condivisione, integrale o parziale, delle immagini riprese da parte di diversi e autonomi titolari del trattamento, i quali utilizzano le medesime infrastrutture tecnologiche; il collegamento telematico di diversi titolari del trattamento ad un "centro" unico gestito da un soggetto terzo; il collegamento con le forze di polizia, anche nelle predette ipotesi.

Al riguardo, sono state prescritte alcune misure di sicurezza ulteriori concernenti, in particolare: l'adozione di sistemi per la registrazione degli accessi logici effettuati e delle operazioni compiute sulle immagini registrate; la separazione logica delle immagini registrate dai diversi titolari.

Con specifico riferimento ai sistemi di videosorveglianza integrati utilizzati dagli enti territoriali, inoltre, non possono essere tracciati gli spostamenti degli interessati e le immagini gestite da un unico centro devono essere trattate in forma differenziata.

Devono essere sottoposti a verifica preliminare i sistemi integrati di videosorveglianza non rientranti nei modelli sopra descritti e per i quali non sia possibile adottare le misure e gli accorgimenti indicati nel provvedimento.

In considerazione del fatto che anche i dispositivi elettronici per la rilevazione di violazioni al codice della strada comportano un trattamento di dati personali, nel circoscrivere le ipotesi di rilevazione di immagini in caso di infrazione, sono stati disciplinati il regime di accessibilità ed i relativi tempi di conservazione prevedendo, altresì, specifiche

cautele per la riservatezza di eventuali passeggeri presenti a bordo dei veicoli.

In tale ambito è stato precisato che, quando il codice della strada prevede espressamente che si renda nota agli utenti l'installazione degli impianti elettronici di rilevamento automatizzato delle infrazioni o quando il titolare del trattamento utilizza comunque i modelli predisposti in conformità al medesimo codice della strada, è possibile fare a meno di fornire un'ulteriore distinta informativa.

Sono stati infine indicati specifici termini - il cui mancato rispetto può comportare l'applicazione di una sanzione amministrativa - entro i quali i titolari del trattamento di dati personali effettuato tramite sistemi di videosorveglianza sono tenuti ad adeguarsi alle prescrizioni o ad adempiere agli obblighi richiamati nel provvedimento, successivamente pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

15.2. VIDEOSORVEGLIANZA IN AMBITO PRIVATO

Muovendo dalle risultanze di un accertamento ispettivo disposto d'ufficio, l'Autorità ha valutato la liceità del trattamento svolto per il tramite di un impianto di videosorveglianza installato presso un ipermercato (*Provv.* 26 febbraio 2009 [doc. *web* n. 1601522]). Il sistema, alla luce degli elementi acquisiti, è risultato installato anche in aree dell'ipermercato suscettibili di transito da parte dei lavoratori (*box* informazioni; *caveau*; zona di scarico merci), senza che tuttavia fosse stata rispettata la disciplina che regola i controlli a distanza dell'attività dei lavoratori (art. 4, comma 2, della legge 20 maggio 1970, n. 300, *cd.* "statuto dei lavoratori").

Le risultanze documentali hanno altresì evidenziato l'assenza di cartelli recanti l'informativa da rendere agli interessati, nonché la conservazione delle immagini registrate per un arco temporale non giustificato da motivate esigenze organizzative.

Inoltre, i dipendenti che avevano accesso alle immagini, benché ritualmente designati quali incaricati in relazione ad altre tipologie di trattamento, non lo sono risultati relativamente allo specifico trattamento svolto per il tramite del sistema di videosorveglianza installato.

Alla luce di tali considerazioni, l'Autorità ha ritenuto illecito il trattamento perché

in violazione degli artt. 11, comma 1, lett. *a*) ed *e*), e 114, del Codice, disponendone conseguentemente, nelle more dell'eventuale espletamento delle procedure sindacali previste dal richiamato art. 4 dello statuto dei lavoratori, il blocco (limitatamente al trattamento svolto presso le aree suscettibili di transito da parte dei lavoratori), prescrivendo altresì al titolare l'adozione di alcune specifiche misure e accorgimenti a tutela degli interessati (con particolare riferimento all'informativa, ai tempi di conservazione delle immagini e alla specifica designazione dei soggetti incaricati alla loro visione quali incaricati del trattamento).

Sull'installazione di un sistema di videosorveglianza all'interno di un complesso condominiale (*Provv.* 19 febbraio 2009 [doc. *web* n. 1601674]) si è riferito nel *par.* 13.

Di altri casi, nei quali l'utilizzo di sistemi di videosorveglianza si univa al trattamento di dati biometrici, si riferisce di seguito.

15.3. BIOMETRIA

In considerazione della frammentaria regolamentazione della materia è stato attivato un gruppo di lavoro per approfondire diversi profili dell'utilizzo di dati biometrici a fini di sicurezza e per scopi diversi (scopi facilitativi). Il gruppo, composto da professori universitari, rappresentanti del DigitPA (già Cnipa) ed esperti della materia, ha il compito di fornire indicazioni utili al riesame della disciplina in materia, con riferimento all'ambito di applicazione della verifica preliminare e della notificazione del trattamento. A tal fine il gruppo ha preso in considerazione i sistemi e le modalità di trattamento di dati biometrici maggiormente utilizzati, in particolare l'impiego di dati biometrici a fini di verifica/identificazione, per procedere ad una loro classificazione in base al reale grado di rischiosità per i diritti e le libertà degli interessati.

Gli interventi dell'Autorità nel corso dell'anno sono stati diretti, in primo luogo, ad assicurare il rispetto dei princìpi di necessità e proporzionalità nell'utilizzo dei dati biometrici.

Biometria e luoghi di lavoro

Con specifico riferimento al trattamento di dati biometrici sul posto di lavoro, il Garante si è pronunciato sull'impiego di un sistema di rilevazione di impronte digitali

dei dipendenti da parte di una concessionaria di automobili (*Provv.* 15 ottobre 2009 [doc. *web* n. 1664257]), che aveva inizialmente dichiarato di voler utilizzare il sistema per verificare la presenza in servizio. A seguito delle indicazioni fornite dall'Ufficio (che richiamava al rispetto delle *"Linee-guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati"* [doc. *web* n. 1364939]), la concessionaria aveva rappresentato di voler comunque continuare nell'impiego del sistema, sia pure per il perseguimento di finalità diverse da quelle originariamente comunicate. Il rilevatore biometrico sarebbe stato utilizzato per consentire l'accesso all'area "officina" - ritenuta sensibile per la presenza in loco di apparecchiature asseritamente pericolose e di beni di valore (parti di ricambio di autoveicoli) - e solo in via residuale, eventualmente, per verificare l'effettiva presenza dei lavoratori sul luogo di lavoro.

Gli accertamenti ispettivi espletati *in loco* hanno evidenziato l'esistenza di un sistema biometrico idoneo alla rilevazione delle presenze dei lavoratori e alla commisurazione delle ore lavorative dagli stessi prestate. Attraverso un apposito *software* collegato al sistema, infatti, l'ufficio del personale è risultato in grado di formare il *"cartellino mensile delle presenze"* per ciascun dipendente e di visualizzare le relative "timbrature" aggiornate in tempo reale.

L'Autorità, nel confermare l'orientamento già espresso in passato (*Provv.* 21 luglio 2005 [doc. *web* n. 1150679]; *Provv.* 15 giugno 2006 [doc. *web* nn. 1306523, 1306530 e 1306551]; *Provv.* 2 ottobre 2008 [doc. *web* n. 1571502]), ha ritenuto illecito il trattamento, in quanto effettuato dalla concessionaria in assenza di legittimi presupposti (non risultando dalla documentazione specifiche giustificazioni per l'utilizzo di tali peculiari modalità di trattamento) e in violazione dei princìpi di necessità e proporzionalità; ciò a cagione del fatto che il controllo dei lavoratori autorizzati ad entrare nell'area officina avrebbe potuto essere agevolmente effettuato (stante anche l'esiguità del numero dei dipendenti interessati) ricorrendo a modalità alternative (*ad es.*, tramite *badge*); inoltre, la sperimentalità del sistema avrebbe potuto essere ugualmente verificata senza il coinvolgimento dei lavoratori (*ad es.*, tramite gli stessi installatori, ovvero disabilitando

la funzionalità di registrazione delle fasce orarie dei dipendenti). Peraltro, l'illiceità del trattamento svolto è derivata anche dall'inosservanza, da parte della concessionaria, delle garanzie procedurali previste dall'art. 4 della legge 20 maggio 1970, n. 300, così come interpretato dalla recente giurisprudenza proprio in riferimento alle apparecchiature in grado di controllare il rispetto degli orari di entrata e uscita e la presenza sul luogo di lavoro dei dipendenti (Cass. 17 luglio 2007, n. 15892). L'Autorità ha dunque vietato alla concessionaria l'ulteriore trattamento dei dati biometrici dei dipendenti per finalità di rilevazione delle loro presenze e di commisurazione dei relativi tempi di lavoro.

Il Garante è poi intervenuto nei confronti di un importante centro orafo campano adottando, all'esito di una complessa attività istruttoria, un *provvedimento* di divieto e prescrizioni in materia di trattamento di dati personali sia mediante l'impiego di un impianto di videosorveglianza, sia mediante l'installazione di un sistema di rilevazione di dati biometrici.

Il centro, che riunisce quasi quattrocento imprese operanti nel settore dei preziosi, era stato sottoposto a una ispezione per verificare l'uso dei sistemi di videosorveglianza. Gli accertamenti del Garante avevano evidenziato che la società che lo gestisce non aveva predisposto né un'informativa adeguata, né cartelli idonei a segnalare ai lavoratori e ai visitatori la presenza delle circa centoquaranta telecamere installate per monitorare tutta l'area. Era risultata, peraltro, la conservazione delle immagini per un tempo superiore a quello indicato dal Garante con il *provvedimento* generale in materia di videosorveglianza del 29 aprile 2004 [doc. *web* n. 1003482].

Con *provvedimento* del 4 giugno 2009 [doc. *web* n. 1629975], il Garante ha pertanto prescritto alla società di fornire l'informativa agli interessati, nelle forme (semplificate) previste dal modello allegato al *provvedimento* del 2004, con riguardo a tutte le aree interessate dal sistema di videosorveglianza installato a presidio del centro orafo, nonché di integrare tali informazioni, per le aree diverse da quelle esterne, con avvisi circostanziati (riportanti gli elementi di cui all'art. 13 del Codice) collocati presso i varchi d'accesso al centro orafo; ha prescritto altresì di conservare le immagini in relazione alle effettive necessità della raccolta, e comunque, in ragione dell'area geografica ad alto tasso di

criminalità nella quale è stabilito il centro orafo e della natura dei beni ivi commercializzati, per non oltre una settimana.

Con il medesimo provvedimento l'Autorità ha vietato l'uso, in forma centralizzata, dei dati biometrici (*template* tratti dalle impronte digitali) raccolti mediante un sistema di rilevamento utilizzato al fine di agevolare l'accesso al centro orafo di soci ed operatori del settore accreditati. La società, infatti, non aveva addotto ragioni specifiche volte a chiarire la necessità della memorizzazione in un sistema centralizzato dei menzionati *template* e, pertanto, tale misura è stata considerata sproporzionata, ben potendosi adottare - in conformità ai princìpi stabiliti negli artt. 3 e 11, comma 1, lett. *d*), del Codice - misure meno invasive a tutela degli interessati (quali, *ad es.*, sistemi biometrici nei quali il *template* ricavato dalle impronte digitali risiede su una *smart card* posta nell'esclusiva disponibilità del detentore o basati sulla lettura del contorno della mano: in questo senso *v.* l'esito della verifica preliminare condotta su un caso analogo nel *Provv.* 1° febbraio 2007 [doc. *web* n. 1381983]).

Ulteriori contestazioni avevano riguardato la modulistica utilizzata per raccogliere il consenso al trattamento dei dati personali di quanti accedevano all'area. Agli interessati, infatti, veniva sottoposto un unico modulo che autorizzava la società a usare i dati biometrici per l'accesso e i dati personali anagrafici per finalità di *marketing*. Alla società è stato perciò prescritto sia di predisporre nuovi modelli di raccolta del consenso, tali da permettere una libera e autonoma scelta da parte dell'interessato sull'uso dei propri dati, sia di integrare l'informativa fornita nella modulistica con gli elementi mancanti (art. 13 del Codice).

La società ha, successivamente, comunicato di essersi conformata alle prescrizioni del Garante.

Sulle medesime tematiche il Garante è tornato a pronunciarsi nei confronti di un'altra società, che eroga il servizio di trasporto pubblico su gomma nell'ambito di un comune campano e di alcune località limitrofe.

In primo luogo, in relazione al trattamento di dati personali effettuato tramite un sistema di videosorveglianza installato presso un deposito di stazionamento degli autobus,

il periodo di conservazione dei dati registrati era risultato superiore a quanto previsto con il *cit.* provvedimento generale del 2004 e, pertanto, non conforme all'art. 11, comma 1, lett. *e*), del Codice.

Con *provvedimento* del 29 ottobre 2009 [doc. *web* n. 1682066] il Garante ha pertanto prescritto di conservare le immagini in relazione alle effettive necessità della raccolta, nei termini previsti dal menzionato provvedimento generale.

In ordine, poi, ai trattamenti effettuati mediante un sistema di rilevazione di dati biometrici basato sulla elaborazione di *template* tratti dalla lettura delle impronte digitali dei lavoratori operanti alle dipendenze della società, considerato che, in sede ispettiva, non erano risultate comprovate specifiche esigenze idonee a giustificare l'utilizzo di dati biometrici, né per la natura delle attività ivi svolte né, in particolare, per verificare il puntuale adempimento della prestazione lavorativa, il Garante ha disposto nei confronti della società (nelle more della definizione di un procedimento di verifica preliminare medio tempore attivato con apposito interpello), il blocco del trattamento dei dati biometrici dei lavoratori, già trattati illecitamente per accertarne la presenza sul luogo di lavoro, con conseguente possibilità di procedere alla sola conservazione temporanea dei medesimi dati.

La società ha, successivamente, comunicato di essersi conformata alle prescrizioni del Garante.

Relativamente alla sicurezza negli aeroporti il Garante (*Provv.* 17 settembre 2009 [doc. *web* n. 1655708]), in sede di verifica preliminare (art. 17 del Codice), ha autorizzato una società che svolge attività di vigilanza e sicurezza a trattare i dati biometrici dei dipendenti che accedono alle aree riservate ed esposte a rischio sicurezza degli aeroporti di Milano "Linate" e "Malpensa", Roma "Fiumicino", Venezia e Pisa.

Nel progetto sottoposto alla verifica era previsto che i dati biometrici dei dipendenti, costituiti da caratteristiche tratte dall'impronta digitale, fossero memorizzati sotto forma di *template* ed in modalità cifrata, su un supporto (*smart card*) posto nell'esclusiva disponibilità del lavoratore. Il progetto escludeva comunque il controllo sull'orario di lavoro.

L'Autorità ha ritenuto proporzionati la raccolta e l'uso delle impronte digitali dei

dipendenti in relazione agli accessi alle sole *"aree sterili"*. Ha tuttavia prescritto alla società di prevedere modalità alternative di accesso e identificazione e di fornire ai dipendenti un'apposita informativa sulla natura facoltativa del consenso al trattamento dei dati biometrici. La conservazione dei dati relativi agli accessi alle *"aree sterili"* è stata approvata per un tempo massimo di sette giorni.

Analogamente, l'uso di dati personali biometrici per l'accesso ad aree riservate, è stato ammesso dal Garante anche per i locali in cui sono custodite banche di dati personali di particolare rilevanza.

In dettaglio, una società concessionaria dei servizi relativi alle entrate e al recupero dell'evasione fiscale e tributaria per conto del Comune di Roma aveva manifestato al Garante l'esigenza di assicurare la riservatezza di una gran quantità di informazioni, anche di carattere sensibile.

Per evitare accessi indebiti alle aree che ospitano gli archivi informatici, la società aveva, quindi, richiesto la verifica preliminare in merito all'attivazione di un sistema di riconoscimento biometrico basato sull'impronta digitale dei dipendenti, memorizzata - sotto forma di *template* e cifrata - su una *smart card* priva di indicazioni nominative, affidata all'esclusiva disponibilità del lavoratore.

L'Autorità (*Provv.* 8 aprile 2009 [doc. *web* n. 1610018]) ha ritenuto proporzionato, per gli scopi suddetti, l'impiego di dati tratti dalle impronte digitali in ragione delle modalità previste, della delicatezza dei dati custoditi e del numero circoscritto di dipendenti interessati dal sistema di rilevazione.

16. Il registro dei trattamenti

L'art. 154, comma 1, lett. *l*), del Codice impone all'Autorità di tenere il *"registro dei trattamenti"*, formato sulla base delle notificazioni ricevute ai sensi degli artt. 37 e 38. In particolare, l'art. 37, comma 4, stabilisce che il Registro sia accessibile a chiunque e che la sua consultazione gratuita avvenga per via telematica attraverso il sito *web* del'Autorità.

Tali condizioni di accessibilità sono state garantite fin dal 2004, con la realizzazione di una procedura di notificazione telematica ed un'apposita sezione del sito internet dell'Autorità, dedicata alla consultazione *online* del Registro.

Per quanto concerne più specificamente il contenuto della notificazione, occorre ricordare che sin dal 2004 l'Autorità aveva posto in essere profondi cambiamenti in relazione alla relativa procedura, e che ulteriori snellimenti delle modalità di compilazione del modello informatico e dei suoi contenuti sono stati disposti con la modifica dell'art. 38, nel quadro delle finalità di semplificazione e accelerazione delle procedure amministrative previste dall'art. 29 del d.l. n. 112/2008, come modificato dalla legge di conversione n. 133/2008.

Il nuovo modello di notificazione, introdotto con *provvedimento* del Garante del 22 ottobre 2008, oltre ad una generale riorganizzazione del modello stesso, ha tra l'altro limitato i casi in cui si deve indicare il luogo principale di custodia dei dati ed ha sottratto al pagamento dei diritti di segreteria la modifica di elementi quali il numero telefonico, di fax e l'indirizzo di posta elettronica.

E' rimasto inalterato l'ormai tradizionale servizio di assistenza *online*, realizzato con messaggi di posta elettronica (tanto originati in automatico dalla procedura quanto predisposti in modo specifico dal personale addetto), sempre affiancato dal supporto telefonico. Anche nel 2009 questi servizi hanno registrato un positivo *trend* di crescita, quantitativa e qualitativa. I meccanismi di controllo in tempo reale della procedura sono stati ulteriormente affinati, garantendo una ancor più rapida ed efficiente risposta ai problemi dell'utenza. Le difficoltà riscontrate sono peraltro ridotte in maniera sensibile, tanto per i miglioramenti intervenuti nella procedura che per la maggiore confidenza

del pubblico con gli strumenti utilizzati (pagamenti *online*, firma digitale, consultazione telematica).

E' aumentato il numero dei cittadini interessati al contenuto del Registro che si sono avvalsi del servizio di ausilio offerto dal Dipartimento. Sono altresì numerosi gli accessi diretti al Registro da parte degli utenti, con una media giornaliera che ha superato i novanta accessi, e punte superiori ai trecento. Tale modalità di fruizione delle notificazioni è segno della effettiva realizzazione del dettato dell'art. 37, comma 4, del Codice, sulla consultazione telematica gratuita del Registro. In tal senso, si sono rivelate decisive le funzioni di stampa integrale delle notificazioni (un tempo da richiedere al Dipartimento), la possibilità di seguire l'*iter* delle diverse modifiche e cessazione successive alla prima notificazione anche in caso di modifica totale della denominazione del titolare, le modalità di ricerca, semplice ma realmente efficace.

Sono ovviamente proseguite le attività di controllo delle notificazioni effettuate e di accertamento delle violazioni dell'obbligo di notificazione, in vista delle attività ispettive del Garante.

Il 2009 ha fatto registrare una inversione di tendenza rispetto al numero delle notificazioni presentate, con una contrazione di circa il 15% rispetto all'anno precedente.

Risultano stabili, dopo la forte contrazione dell'anno scorso, le notificazioni di trattamenti relativi a dati idonei a rivelare lo stato di salute e la vita sessuale, mentre si consolida il numero dei trattamenti di dati effettuati con strumenti elettronici e volti a definire il profilo o la personalità dell'interessato, o ad analizzarne abitudini o scelte di consumo.

Per quanto concerne la distribuzione geografica dei titolari, si conferma il distacco del nord del Paese (nord est e nord ovest rappresentano ormai il 56% dei titolari presenti) rispetto al resto del territorio; ciò oltre che a diversità economiche di natura strutturale, potrebbe esser da collegare anche ad elementi legati alla fase più acuta della crisi economica, che ha maggiormente inciso sulla tipologia di titolari presenti nel sud (ditte individuali, artigiani, società a responsabilità limitata di piccole o piccolissime dimensioni).

17. LA TRATTAZIONE DEI RICORSI

17.1. CONSIDERAZIONI GENERALI

La prima osservazione sull'attività istruttoria e decisoria svolta nell'anno 2009 in relazione ai ricorsi proposti ai sensi degli artt. 145 *ss.* del Codice - che per la trasversalità e l'eterogeneità dei temi affrontati, si presta maggiormente a riflessioni di carattere generale - è la constatazione di un rinnovato, significativo aumento delle trattazioni.

Dopo diversi anni (dal 2005 in avanti) che avevano visto un progressivo calo nel numero di decisioni assunte, l'anno appena trascorso segna (dopo l'assestamento già registratosi nel 2008) un aumento apprezzabile delle decisioni adottate (il totale dell'anno ammonta a trecentosessanta).

Lo strumento del ricorso appare, quindi, sempre vitale. Per un verso si consolida come strumento ordinario e consueto per consentire il "dominio" dell'interessato sui dati personali che lo riguardano (attraverso l'esercizio del diritto di accesso) o per ripristinare il controllo sulle informazioni illegittimamente trattate (a mezzo delle richieste di blocco, cancellazione od opposizione al trattamento). Per altro verso è uno strumento duttile che si adatta efficacemente agli ambiti e alle situazioni più diverse e consente agli interessati (spesso impegnati o protesi verso contenziosi di più ampia portata) di disporre di potenzialità nuove per sostenere le proprie ragioni e interloquire efficacemente nella dialettica processuale. Ne sono prova i tanti procedimenti che dimostrano come i diritti tutelati dall'art. 7 del Codice hanno una imprevedibile e amplissima possibilità di adattarsi ai contesti più diversi, spesso aprendo scenari nuovi e "costringendo" l'Autorità a confrontarsi continuamente e innovativamente con le categorie generali disciplinate dalla legge e dalla direttiva comunitaria.

E' in realtà il concetto base di "dato personale" che ha una oggettiva, ampia possibilità di espansione e soprattutto di adattamento ai nuovi contesti tecnologici con i quali quotidianamente l'Autorità si deve confrontare. In effetti, un esame più approfondito dei tanti casi affrontati mette in luce come la presenza e le potenzialità della rete internet sia sempre più lo sfondo delle decisioni sui ricorsi.

Vengono in considerazione non solamente il fenomeno dello *spamming* a fini genericamente promozionali e pubblicitari, ma soprattutto le conseguenze dell'utilizzo della rete - specie quelle di lungo periodo indotte dalla persistenza sulla rete stessa dei dati - che sono emerse negli ultimi mesi. La diffusione, senza limiti di durata, delle informazioni e la loro facile reperibilità su internet grazie all'ausilio dei *cd.* "motori di ricerca", se da un lato espande e facilita le possibilità conoscitive, dall'altro (specie in caso di informazioni inesatte, incomplete o addirittura lesive della dignità della persona) aumenta i rischi di danno legati appunto ad una loro persistenza indefinita, capace di porre nel nulla le aspettative connesse al *cd.* "diritto all'oblìo".

Questi temi, già difficili da affrontare in relazione al comune funzionamento della rete, diventano di ancora più complessa soluzione, utilizzando gli ordinari strumenti giuridici, con riferimento al fenomeno in prepotente e velocissima espansione dei *cd. "social network"*. In tale ambito, determinare le fattispecie eventualmente sottoponibili al campo di applicazione della legge è operazione assai complessa.

Se le sfide delle nuove tecnologie si sono affacciate anche nella trattazione di diversi ricorsi, bisogna comunque osservare che, anche nel 2009, lo "zoccolo duro" degli ambiti trattati si conferma ancora quello più "tradizionale" emerso negli ultimi anni.

Ancora una volta è l'insieme dei trattamenti di dati ruotanti attorno alla realtà bancaria e finanziaria ad assorbire il maggior numero di trattazioni, includendo in questo totale i numerosi casi di esame della disciplina concernente la Centrale rischi della Banca d'Italia, l'archivio della *cd.* "centrale d'allarme interbancaria", i trattamenti concernenti i sistemi di informazioni creditizie.

Merita poi di essere evidenziato il significativo aumento delle trattazioni concernenti il trattamento dei dati dei dipendenti (sia da parte di datori di lavoro pubblici che privati) nonché quelle riferite ai trattamenti svolti in ambito giornalistico (nell'ampia accezione in cui il termine è considerato dal Codice).

Infine, un'ultima notazione sul tipo di decisioni adottate riguarda l'elevatissimo numero di declaratorie di "non luogo a provvedere".

Ciò conferma che, spesso, dopo l'iniziale silenzio serbato dai titolari del trattamento

a fronte degli interpelli proposti dagli interessati, la presentazione formale del ricorso al Garante apre la strada ad una rapida definizione della vicenda, superando ostacoli e ritardi spesso determinati da incompleta o inesatta conoscenza delle disposizioni del Codice.

17.2. PROFILI PROCEDURALI

La vasta casistica affrontata nel corso dell'anno consente di estrarre diverse decisioni che consentono di far emergere aspetti significativi connessi alla procedura dei ricorsi. Ciò, mettendo in luce sia aspetti ormai consolidati nella "giurisprudenza" del Garante, sia problematiche nuove oggetto di primo esame da parte dell'Autorità.

Si propongono di seguito alcuni casi di particolare interesse.

17.2.1. Proponibilità del ricorso nei confronti di particolari soggetti

Il ricorso, come detto, è strumento di amplissimo utilizzo. Pur tuttavia, esistono ambiti particolari nei quali, per espressa disposizione del Codice, tale strumento di tutela non trova applicazione o situazioni nelle quali emerge l'errata individuazione di un soggetto quale (supposto) titolare di un determinato trattamento.

A tal proposito, si può citare la *decisione* del 3 novembre 2009 [doc. *web* n. 1687662] con la quale è stato rilevato il difetto di legittimazione passiva di *Google Italy S.r.l.* in ordine al rinvenimento, per il tramite del noto motore di ricerca *"Google"*, di una pagina *web* contenente informazioni ritenute inesatte dalla ricorrente. L'istruttoria svolta ha messo in luce l'estraneità della società evocata nel procedimento (*Google Italy S.r.l.*) rispetto al trattamento di dati in questione, limitandosi la predetta società ad una *"mera attività di* marketing, *ricerca clienti e raccolta della pubblicità"*.

Particolarmente interessante è anche la vicenda culminata nella *decisione* del 16 luglio 2009 [doc. *web* n. 1638472] con la quale è stato dichiarato inammissibile un ricorso proposto nei confronti dell'amministrazione del Senato della Repubblica in relazione ai dati personali di una persona citata nel testo di un'interrogazione parlamentare risalente nel tempo e tuttora disponibile sul sito internet del Senato.

Nel caso di specie il Garante ha anzitutto rilevato le esigenze di tutela e i problemi connessi alla prolungata reperibilità sulla rete di informazioni suscettibili di riverberarsi in negativo sulla figura e l'identità dell'interessato. Ma l'Autorità ha altresì riscontrato che lo specifico trattamento in questione viene effettuato nell'esercizio di funzioni e prerogative parlamentari e in ossequio al principio relativo alla pubblicità degli atti parlamentari. Tale trattamento, svolto appunto da un organo costituzionale, è disciplinato dallo stesso in conformità al rispettivo ordinamento nell'ambito della sfera di autonomia riservata alle Camere dalla Costituzione (art. 64 Cost.). Ciò induce a ritenere che la legge sulla protezione dei dati non possa regolare tale ambito riservato di spettanza parlamentare, in ragione della *"indipendenza guarentigiata"* delle Camere nei confronti di ogni altro potere, riconosciuta anche dalla Corte costituzionale (sentenza n. 154 del 1985).

Va poi ricordata l'ulteriore *decisione* 4 febbraio 2010 [doc. *web* n. 1703923] che ha sancito l'inammissibilità di un ricorso proposto nei confronti dell'Agenzia informazioni e sicurezza esterna (Aise), trattandosi di soggetto - al pari di tutti gli altri organismi di informazione e sicurezza - nei cui confronti non può essere attivata la procedura dei ricorsi (ai sensi dell'art. 58 del Codice).

17.2.2. Tempistica e formalità per la proposizione dei ricorsi

Il procedimento dei ricorsi, anche in ragione dei previsti termini assai brevi, è caratterizzato da requisiti formali minimi e da una notevole agilità procedurale. Tuttavia alcuni punti fermi sono stati più volte ribaditi dall'Autorità al fine di evitare che la doverosa attenzione al dato sostanziale non determini incertezza e indeterminazione nelle modalità di esercizio dei diritti. Va in questa direzione il *provvedimento* 22 dicembre 2009 [doc. *web* n. 1695163] che - nel ricordare che in termini generali il ricorso può essere proposto solo dopo che siano trascorsi quindici giorni dall'avvenuta ricezione, da parte del titolare del trattamento, dell'interpello preventivo - ha rammentato l'esigenza di una prova della sussistenza del presupposto (ovvero un *"pregiudizio imminente e irreparabile"*) che solo può giustificare la presentazione immediata del ricorso, senza seguire appunto il procedimento ordinario che richiede la previa proposizione di un'istanza ai sensi dell'art. 7 del Codice.