I diversi accorgimenti prescritti dal Garante ai fornitori (ai quali è stato assegnato un termine di centottanta giorni per l'adeguamento) riguardano in particolare: l'individuazione più selettiva del ristretto numero di incaricati designati a trattare i dati; la separazione tra i dati di carattere contabile e i dati documentali prodotti nel corso delle attività svolte su richiesta dell'autorità giudiziaria; l'adozione di procedure di autenticazione robuste per l'accesso informatico da parte del personale incaricato ai dati trattati, con il ricorso anche a caratteristiche biometriche; l'adozione di sistemi di comunicazione con l'autorità giudiziaria basati su aggiornati strumenti telematici e tecniche di firma digitale, evitando l'uso di sistemi meno sicuri (*ad es.*, il fax); la protezione dei dati, per il periodo di presenza nelle banche dati dei gestori, con strumenti avanzati di cifratura; la cancellazione immediata dei dati dopo la loro comunicazione all'autorità giudiziaria.

15.8. *Servizi telefonici non richiesti*

Anche nell'anno di riferimento sono pervenuti al Garante numerosi reclami, segnalazioni e quesiti con i quali sono state lamentate ripetute violazioni del diritto al corretto e lecito utilizzo dei dati personali nella prestazione di alcuni servizi di comunicazione elettronica da parte, oltre che dei fornitori di servizi, anche dei rivenditori dislocati sul territorio. In particolare sono state evidenziate violazioni connesse all'indebita attivazione di contratti, schede o servizi telefonici non richiesti dagli interessati; in alcuni casi, soggetti cui erano state intestate falsamente schede di telefonia mobile senza consenso si sono trovati addirittura coinvolti in indagini penali.

Le segnalazioni pervenute hanno riguardato anche ulteriori problematiche legate alla selezione automatica dell'operatore e all'attivazione di servizi non richiesti, tra i quali segreterie telefoniche e collegamenti Internet a banda larga.

L'ampia portata del fenomeno risulta, peraltro, anche dalla trattazione di diversi ricorsi presentati all'Autorità, la quale da tempo si occupa della tematica, avendo svolto negli anni passati (*v. Relazione* 2003, pp. 87 e 140), anche impegnativi accertamenti di carattere ispettivo.

Sulla base delle informazioni acquisite, anche in occasione di nuovi accertamenti ispettivi effettuati presso alcuni tra i maggiori operatori telefonici, il Garante ha effettuato un'apposita istruttoria al fine di intervenire sul fenomeno con un provvedimento di carattere generale volto ad individuare un quadro di garanzie che assicuri il rispetto dei diritti e delle libertà fondamentali dei cittadini.

Nel *provvedimento* adottato il 16 febbraio 2006 ([doc. *web* n. 1242592], in *G.U.* 6 marzo 2006, n. 54), il Garante ha quindi imposto agli operatori telefonici la predisposizione di procedure che consentano di rilevare tempestivamente le intestazioni multiple di schede telefoniche prepagate ad una medesima persona. In particolare, quando le intestazioni siano superiori a 4 (per le persone fisiche) e a 7 utenze (per le società) l'operatore dovrà chiederne espressa conferma all'intestatario. Resta vietato attivare servizi senza aver acquisito l'espresso consenso preventivo degli interessati; inoltre, le persone vanno contattate per finalità pubblicitarie o promozionali solo se hanno manifestato uno specifico e preventivo consenso a ricevere a tal fine chiamate e comunicazioni. Gli addetti ai *call center* devono, al momento del contatto, spiegare agli interessati da dove siano stati estratti i dati che li riguardano. Deve essere, inoltre, registrata immediatamente e rispettata la volontà di non ricevere il servizio, nonché l'eventuale contrarietà espressa in relazione all'uso dei dati.

Il Garante ha inoltre imposto ad operatori telefonici, di comunicazione elettronica e *call center* di verificare attentamente, anche attraverso controlli a campione,

l'attività di rivenditori e incaricati, allo scopo di rintracciare immediatamente chi materialmente abbia effettuato eventuali attivazioni indebite.

15.9. *Informativa con modalità diverse da quelle ordinarie*

Nel mese di dicembre dell'anno di riferimento l'Autorità ha ricevuto la richiesta di un operatore telefonico volta a consentire di informare gli interessati in modo diverso da quello ordinario ai sensi dell'art. 13 del Codice.

La richiesta riguardava un progetto di fusione per incorporazione (avvenuta poi nei primi mesi del 2006) tra la società istante ed un altro operatore, del quale la prima ha acquisito il complesso aziendale con tutti i rapporti giuridici attivi e passivi in atto, assumendo di conseguenza la qualità di titolare del trattamento dei dati personali dei relativi interessati. All'esito dell'istruttoria sono state individuate modalità di informazione sostitutive di quelle rivolte, caso per caso, a ciascun interessato, con particolare riguardo alle caratteristiche, anche comunicative, del contenuto dell'avviso da pubblicare sugli organi di stampa.

15.10. *Il codice deontologico*

La prossima definizione del codice deontologico per gli operatori Internet consentirà di introdurre, in un settore in continua evoluzione, specifiche garanzie al cui rispetto sarà subordinata la liceità e la correttezza dei diversi trattamenti di dati personali (art. 12, comma 3, del Codice). L'obiettivo principale è indicare soluzioni effettive, adeguate e dinamiche ad alcune questioni relative al trattamento dei dati personali *on-line* che possano, da un lato, sensibilizzare maggiormente gli utenti in rete sui rischi in materia correlati all'uso di Internet, offrendo loro ulteriori opportunità di tutela e, dall'altro, indicare ai diversi operatori interessati concreti strumenti per adempiere agli obblighi di legge (anche per quanto riguarda i principi di cui all'art. 11 del Codice) assicurando un più elevato livello di rispetto della normativa sulla protezione dei dati personali.

In questa prospettiva sono proseguiti nel 2005 gli incontri nel tavolo di lavoro composto dagli operatori del settore –rappresentati dalle relative organizzazioni di categoria– e dalle associazioni dei consumatori che hanno entrambi aderito all'invito a parteciparvi rivolto dall'Autorità.

In tale ambito sono state affrontate diverse esigenze fra le quali quelle relative: all'obbligo di informare adeguatamente gli utenti circa i possibili trattamenti, impliciti o espliciti, che possono riguardarli; al consenso da manifestare espressamente e liberamente; ai presupposti e ai limiti entro i quali è legittimo l'uso di marcatori o dispositivi analoghi *on-line*; alle modalità semplificate per esercitare i diritti di cui all'art. 7 del Codice; ai trattamenti che possono presentare rischi specifici per la sicurezza degli utenti in rete, come nel caso del *phishing*; allo *spamming*, con particolare riferimento alla possibilità di individuare misure di filtraggio a tutela degli interessati. Il gruppo di lavoro ha poi riscontrato l'opportunità di affrontare altri temi impegnativi quali quello del trattamento dati rispetto ai nomi a dominio, al diritto all'oblìo in rete e, quindi, alle garanzie rispetto ai motori di ricerca.

Alla luce dei vari contributi e delle riflessioni svolte, il tavolo redigerà una prima bozza di codice deontologico che sarà pubblicata sul sito Internet dell'Autorità per una consultazione pubblica. Sulla base delle osservazioni e proposte che perverranno, il tavolo apporterà le eventuali modifiche al testo che, sottoposto all'esame

dell'Autorità e da questa "certificato" in conformità alle procedure in tema di codici deontologici in fase di generale formalizzazione, verrà trasmesso al Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* e la sua allegazione al Codice sulla protezione dei dati personali.

15.11. *Motori di ricerca e diritto all'oblìo*

La problematica relativa al *cd.* "diritto all'oblìo", ossia il diritto ad "essere dimenticato" nella dimensione pubblica o, comunque, non più privata, precedentemente acquisita, presenta profili di particolare complessità laddove le informazioni personali che si intendano cancellare siano state diffuse in Internet. Inserendo nei motori di ricerca più comuni alcune parole chiave è infatti particolarmente agevole risalire in tempo reale ad un numero considerevole di informazioni di carattere personale riguardanti una stessa persona e riferite ad epoche assai diverse.

Questa efficiente profilazione generalizzata può porsi in conflitto con il diritto di un soggetto interessato a veder delimitata nel tempo la diffusione indifferenziata di molte informazioni che lo riguardano, che può non essere più giustificata alla luce delle finalità e delle circostanze originarie; ciò, senza considerare i casi nei quali le informazioni pubblicate risultino sin dall'inizio non corrette o, comunque, incomplete o non aggiornate.

In questo quadro diversi interessati contestano spesso la circostanza che le copie *cache* (e le relative sintesi) –attraverso le quali i motori di ricerca mettono a disposizione degli utenti le pagine *web* indicizzate contenenti le parole chiave utilizzate nelle ricerche– non riportano automaticamente le modifiche già intervenute nelle pagine *web* dei "siti sorgente", anche quando queste ultime siano state modificate o cancellate da diverso tempo. I motori di ricerca non procedono infatti ad una revisione automatica ed immediata dei propri indici a fronte della modifica dei siti richiamati, bensì effettuano aggiornamenti periodici degli stessi attraverso l'utilizzo di un *software* (*cd. crawler*).

Sul ruolo dei motori di ricerca, è stata pertanto avviata una specifica riflessione da parte dell'Autorità, anche alla luce dei numerosi ricorsi e segnalazioni pervenuti.

Fra questi ultimi merita menzione almeno un ricorso proposto nei confronti di Google Italy S.r.l.. In tale occasione, il Garante, con una decisione intervenuta poi di recente, ha infine riconosciuto in capo al motore di ricerca un'autonoma titolarità del trattamento, consistente nella creazione e nella conservazione di cosiddette copie *cache* di pagine *web* pubblicate sul sito sorgente. Tuttavia, non risultando provato che il trattamento contestato fosse effettuato da un soggetto stabilito sul territorio dello Stato, l'Autorità si è riservata di esaminare, nell'ambito di una distinta attività, le questioni relative alla tutelabilità dei diritti dell'interessata in rapporto a titolari situati all'estero (nella specie, Google Inc. avente sede negli Stati Uniti). A tal fine, è stata sollecitata una fattiva collaborazione con tale società, per individuare nel breve periodo soluzioni concrete che permettano di garantire pienamente sul territorio italiano i diritti e le libertà fondamentali degli interessati, anche quando gli strumenti utilizzati per il trattamento siano situati in Paesi non appartenenti all'Unione europea (*cfr. Comunicato stampa* 13 aprile 2006; sulla tematica, *v.* anche quanto riportato al par. 18.3).

15.12. *Televisione digitale: i servizi interattivi*

Nel 2005 l'Autorità ha adottato un provvedimento generale (*Provv.* 3 febbraio 2005 [doc. *web* n. 1109503]) con il quale ha prescritto ai fornitori dei servizi televisivi interattivi di adottare misure necessarie per conformare i loro trattamenti alle disposizioni in materia di protezione dei dati personali. Il provvedimento si è reso necessario per evitare eventuali forme invasive di controllo sulle abitudini delle persone ed operazioni illecite di profilazione, oltre che per garantire ad utenti ed abbonati una piena consapevolezza sui trattamenti di dati personali che li riguardano, anche al fine di esercitare liberamente le loro scelte ed i loro diritti, senza essere pregiudicati nella fruizione di servizi e di opportunità.

La circostanza che la televisione digitale interattiva trovi usuale utilizzo in un ambito segnatamente "privato", quale quello familiare, richiedeva particolare attenzione da parte del Garante. In tali contesti, l'utente nutre la ragionevole aspettativa di essere al riparo da forme di controllo; spesso, poi, ad uno stesso apparecchio televisivo possono corrispondere più fruitori differenziati (appartenenti o estranei al nucleo familiare dell'abbonato), i quali debbono essere messi tutti in grado di compiere liberamente le loro scelte, senza che ciò comporti schedature o profilazioni.

Nello scorso anno si è registrato un aumento sensibile del numero degli utenti e degli operatori del settore (a prescindere dalla tecnica di trasmissione impiegata, che può implicare l'utilizzo del satellite, del cavo o del digitale terrestre), unitamente a novità tecnologiche che possono presentare nuovi rischi o, comunque, profili di interesse per la sfera privata degli interessati.

Nel richiamato provvedimento l'Autorità ha pertanto prescritto agli operatori del settore le misure di carattere generale volte a garantire il rispetto dei principi di necessità, liceità, correttezza e proporzionalità. In primo luogo, occorre ridurre al minimo l'utilizzo delle informazioni relative ad abbonati e utenti identificabili, privilegiando l'uso di dati anonimi (come schede prepagate). In questo caso, anche l'acquirente del *decoder* digitale terrestre deve essere anonimo, ferma restando la necessità di prender nota del nome al solo fine di evitare un'attribuzione multipla del relativo contributo statale. Si prefigura diversamente, invece, il caso del rapporto contrattuale che debba intercorrere necessariamente con un abbonato identificato. Resta poi ferma l'illiceità di eventuali banche dati di titolari di antenne televisive o satellitari (il cosiddetto "catasto delle antenne").

Profilazione

Quanto, poi, alla profilazione attraverso la tv interattiva, il Garante ha stabilito che non è lecito trattare dati personali quali quelli relativi a tempi di connessione, visioni di programmi ed eventi, nonché ad analisi del comportamento in presenza di spazi pubblicitari, a meno che l'interessato, debitamente informato, non abbia prestato il proprio consenso libero e specifico. In tal caso, i dati di dettaglio su acquisti e servizi possono essere tuttavia conservati per un periodo comunque non superiore a dodici mesi dalla loro registrazione, salva la loro trasformazione in forma anonima. Le eventuali intenzioni di trattare i dati oltre tali termini possono essere attuate solo previa valutazione preliminare dell'Autorità ai sensi dell'art. 17 del Codice.

Sondaggi e ricerche di mercato

Con riguardo ai sondaggi, alle ricerche di mercato e alle altre ricerche campionarie, il fornitore deve adottare una tecnica che separi il voto espresso dal nominativo di chi ha partecipato al sondaggio; laddove la commistione risulti tecnicamente inevitabile, deve rendere le risposte realmente anonime subito dopo la loro raccolta, escludendo a maggior ragione ogni eventuale comunicazione a terzi o diffusione dei dati personali.

Non è di regola ammesso il trattamento di dati sensibili, né per l'ordinaria pre-

stazione di servizi televisivi, né per eventuali finalità di profilazione o fidelizzazione della clientela, a meno che tale trattamento sia realmente indispensabile in rapporto ad uno specifico bene o servizio richiesto e sia altresì autorizzato dal Garante, oltre che consentito dall'interessato in forma scritta o telematica equiparabile allo scritto.

Informativa

L'Autorità ha, poi, prescritto ai gestori di servizi televisivi l'obbligo di fornire informative più chiare e complete, prevedendo anche l'inserimento, prima di ogni acquisto o altro tipo di rapporto interattivo, di un'apposita schermata-video. Il consenso può essere manifestato anche elettronicamente attraverso il telecomando e deve essere libero da qualsiasi condizionamento. In caso di fatturazione degli acquisti (*ad es.* di partite o film), l'abbonato deve avere la possibilità di non ricevere una fatturazione dettagliata. Gli acquisti devono essere indicati per importo totale, data e costo, mentre vanno forniti i "titoli" specifici solo su richiesta.

L'Autorità ha poi imposto agli operatori di indicare nell'informativa il termine di conservazione dei dati dopo la cessazione del rapporto (termine che non può essere comunque superiore ad un trimestre, salvi eventuali obblighi di legge specifici sulla conservazione di documentazione contabile), nonché di predisporre idonei meccanismi di cancellazione automatica dei dati anche da parte di terzi ai quali gli stessi siano stati eventualmente comunicati.

Verifica preliminare

Il Garante ha inoltre previsto in capo ai fornitori dei servizi televisivi interattivi l'obbligo di richiedere la verifica preliminare ai sensi dell'art. 17 del Codice laddove il trattamento di dati consista nella "*richiesta –rivolta dal fornitore ai singoli utenti– di identificarsi nominativamente al momento in cui essi inviano informazioni attraverso il canale di ritorno*". Ciò, al fine di poter prescrivere specifici accorgimenti e misure a garanzia degli interessati, nei casi in cui all'utente (persona fisica eventualmente diversa dall'abbonato) sia richiesto di essere individuato specificamente nel momento in cui compia un'operazione diversa da quelle effettuabili "ordinariamente" nel quadro del comune svolgimento di un rapporto. A tale riguardo sono già pervenute all'Autorità alcune richieste di valutazione preliminari sulle quali il Garante è in procinto di pronunciarsi caso per caso.

È stata infine avviata una complessa attività ispettiva volta a verificare il corretto e completo adeguamento degli operatori alle prescrizioni impartite dall'Autorità in materia.

15.13. Pornosquatting

Sono pervenute a questa Autorità diverse segnalazioni con le quali è stata lamentata la violazione del diritto all'immagine, al nome ed alla professionalità, commessa presso alcuni siti Internet a contenuto pornografico. I segnalanti lamentano in particolare che, digitando il loro nome su un qualsiasi motore di ricerca, compaiono, fra i risultati, anche alcuni indirizzi di siti pornografici che associano al loro nome contenuti osceni e denigratori della reputazione.

Da alcune ricerche preliminari curate da questa Autorità, si è potuto verificare che i casi di specie rientrano nel fenomeno, diffuso in Internet, meglio noto come "*pornosquatting*" che consiste nell'inserire nomi di personaggi famosi, o di noti marchi, tra le parole chiave riscontrabili nei *cd.* "*meta-tag*" (stringhe ipertestuali) della pagina *web*, che dovrebbero descrivere essenzialmente il contenuto del sito.

Tale pratica risulta piuttosto lesiva degli interessati in quanto la tecnologia dei motori di ricerca imposta le ricerche proprio in base alle parole contenute in tali stringhe ipertestuali. Di conseguenza, se si cercano in rete notizie relative ad un

determinato soggetto e il suo nome è contenuto nei "*meta-tag*" di un sito *web*, l'indirizzo di quest'ultimo verrà sicuramente presentato tra i risultati dal motore di ricerca interrogato.

La circostanza che i titolari dei siti pornografici utilizzino nomi di personaggi noti per rendere maggiormente "reperibili" gli indirizzi dei siti stessi può peraltro essere considerata alla stregua di uno sfruttamento illegittimo della notorietà delle persone coinvolte, oltre che un'induzione in errore degli utenti.

L'Autorità sta ultimando, anche avvalendosi della collaborazione della Guardia di finanza, i necessari accertamenti preliminari.

15.14. Rfid

In un *provvedimento* del 9 marzo 2005 [doc. *web* n. 1109493] il Garante ha impartito prescrizioni specifiche per chi intenda produrre ed utilizzare le cosiddette "etichette intelligenti", minuscoli *chip* a radiofrequenza (*Radio Frequency Identification-Rfid*) attivati da lettori ottici, che hanno iniziato a trovare applicazione anzitutto nell'ambito di aziende, esercizi commerciali e della grande distribuzione per ottenere alcuni vantaggi, a volte anche per il consumatore (migliore gestione di prodotti aziendali, maggiore rapidità di operazioni commerciali, agevole rintracciabilità dell'origine di particolari prodotti e controllo degli accessi a luoghi riservati).

Alcuni utilizzi di questa tecnologia –che non si limitino a tracciare un prodotto per garantire l'efficienza del processo di produzione industriale– possono comportare anche una violazione del diritto alla protezione dei dati personali e determinare forme di controllo sulle persone. Con l'uso di *Rfid* si potrebbero, infatti, raccogliere innumerevoli dati sulle abitudini dei consumatori a fini di profilazione ed essere in grado di tracciare i percorsi effettuati dagli stessi, controllarne la posizione geografica o verificare quali prodotti usano, indossano o trasportano.

I sistemi *Rfid* possono essere impiegati da soggetti pubblici o privati anche ad altri scopi quali l'identificazione personale o la tutela della salute. Alcuni particolari usi come l'impianto di *microchip* sottopelle hanno già sollevato problematiche di grande delicatezza. Ulteriori pericoli possono derivare dall'adozione di *standard* comuni in materia, tali da favorire la possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (*ad es.*, mediante la loro riscrittura). I rischi possono accrescersi nel caso in cui si integrino le tecniche *Rfid* con infrastrutture di rete avvalendosi della telefonia e di Internet, e sulla base dello stesso sviluppo tecnologico che, potenziando i sistemi, potrebbe consentire una "lettura" delle etichette a distanze sempre maggiori.

Il provvedimento generale si collega a quello varato nello stesso periodo dal Gruppo art. 29, allo scopo di stabilire alcune misure per rendere conformi l'impiego dei sistemi *Rfid* alle norme sulla *privacy* nei casi in cui si trattino dati personali relativi a persone identificate o identificabili, e tutelare la loro dignità e la libertà.

Informativa

In particolare, l'Autorità ha prescritto che gli interessati siano adeguatamente informati dell'utilizzo di sistemi *Rfid,* così come dell'esistenza dei lettori ottici che attivino l'etichetta. La presenza di avvisi nei luoghi nei quali le tecniche *Rfid* sono utilizzate non esime, peraltro, dall'apporre un'informativa più specifica in relazione agli stessi oggetti e prodotti che recano le etichette intelligenti.

L'uso di etichette intelligenti deve risultare proporzionato agli scopi che si intendono perseguire. I dati possono essere utilizzati solo per le finalità per le quali sono stati raccolti e devono essere conservati per il tempo strettamente necessario.

L'utilizzo delle *Rfid* che comporta un trattamento di dati personali può avvenire

solo con il consenso espresso e specifico degli interessati, a meno che ricorra uno degli altri presupposti di legge; il consenso non è valido se ottenuto con pressioni o condizionamenti sull'interessato.

Rfid e profilazione

Se le etichette intelligenti sono associate all'utilizzo di carte di fedeltà, e si trattano dati a fini di profilazione dei consumatori, occorre informare ed acquisire il consenso degli interessati; il consenso non è invece necessario quando le etichette intelligenti sono adoperate solo per modalità di pagamento e tale impiego non comporti alcuna riconducibilità dei prodotti ad acquirenti identificati o identificabili.

Deve comunque essere garantito comunque il diritto di asportare, disattivare o interrompere gratuitamente ed in maniera agevole il funzionamento delle *Rfid* al momento dell'acquisto del prodotto sui cui è apposta l'etichetta. Le etichette devono essere posizionate in modo tale da risultare facilmente asportabili senza danneggiare o limitare la funzionalità del prodotto (*ad es.*, collocate solo sulla confezione); non è, di regola, lecita l'installazione di *Rfid* destinate a rimanere attive oltre la barriera-cassa dell'esercizio commerciale.

Nei casi di impiego delle *Rfid* per la verifica di accessi a determinati luoghi riservati devono essere predisposte idonee cautele per i diritti e le libertà delle persone; in particolare, per i luoghi di lavoro, va rispettato quanto previsto dallo Statuto dei lavoratori relativamente al divieto di utilizzo di impianti per controlli a distanza di dipendenti. Per l'accesso occasionale di terzi a determinati luoghi occorre predisporre un meccanismo che, nel caso di indisponibilità ad usare *Rfid* da parte dell'interessato, permetta comunque l'ingresso.

L'avvio di trattamenti di dati che indichino la posizione geografica di persone o oggetti mediante reti di comunicazione elettronica o che siano effettuati allo scopo di costruire profili o personalità di un individuo deve essere, inoltre, comunicato preventivamente al Garante.

Impianto di *microchip* sottopelle

Il Garante ha inoltre ritenuto che l'impianto di *microchip* sottopelle debba essere in via di principio escluso in quanto contrastante con i diritti, le libertà fondamentali e la dignità della persona. Tali impianti sono limitatamente ammissibili, in casi eccezionali, per comprovate e giustificate esigenze di tutela della salute delle persone. L'interessato, comunque, deve poter ottenere la rimozione del *microchip* e l'interruzione del relativo trattamento dei dati che lo riguardano; si devono inoltre prevedere modalità di impianto che garantiscano la riservatezza circa la presenza delle etichette nel corpo dell'interessato. Il Garante ha stabilito infine che i soggetti che intendono utilizzare tali *microchip* devono sottoporre i relativi sistemi alla verifica preliminare dell'Autorità.

16 La sicurezza dei dati e dei sistemi

Anche nel corso del 2005 sono pervenute numerose richieste di chiarimenti circa la disciplina in materia di "misure minime" di sicurezza introdotta dal Codice.

Documento programmatico sulla sicurezza

Il Garante ha in numerose occasioni confermato le indicazioni già fornite agli operatori con una *nota* di carattere generale del 22 marzo 2004 [doc. *web* n. 771307] con riguardo alla natura del documento programmatico sulla sicurezza (d.p.s.). In particolare, si è precisato che: la redazione e/o l'aggiornamento del d.p.s. rientra tra le misure minime di sicurezza; di esso deve dotarsi qualsiasi titolare che effettui un trattamento di dati sensibili e/o giudiziari con strumenti elettronici; è sostenibile affermare che il d.p.s. sia una "nuova" misura minima, con la conseguenza che anche a questo adempimento è applicabile la disciplina transitoria (art. 180, comma 1, del Codice); deve essere conservato dal titolare presso la propria struttura, essendone doverosa l'esibizione o l'invio al Garante in caso di accertamenti ispettivi o su richiesta dell'Autorità (art. 34, comma 1, lett. *g)*, del Codice e regola 19 dell'Allegato B) al Codice).

I principi già affermati dall'Autorità con la citata *nota* del 22 marzo 2004 sono stati, da ultimo, ribaditi nella risposta ad un quesito della Confederazione nazionale dell'artigianato e delle piccole e medie imprese (Cna). Richiamandosi ai contributi già resi dall'Autorità in materia, con specifico riguardo alla redazione di una guida operativa disponibile sul sito del Garante [doc. *web* n. 1007740], volta ad agevolare la stesura e l'aggiornamento di un d.p.s. ancor più semplificato e impostato per le esigenze peculiari delle piccole e medie imprese, l'Ufficio del Garante si è reso disponibile a fornire ulteriori contributi alla categoria, precisando che eventuali provvedimenti di esonero o di deroga non rientrano tra i poteri attribuiti al Garante dal Codice (*Nota* 1 marzo 2005). Si è pertanto sviluppata una proficua collaborazione con la Confederazione che ha portato allo studio e alla definizione di modalità operative semplificate di stesura del d.p.s. reputate dal Cna maggiormente idonee a rappresentare le istanze e le caratteristiche dei piccoli e medi operatori del mercato.

Utilizzo di credenziali biometriche

Un ultimo caso interessante, a riprova del crescente interesse all'impiego di tecniche di autenticazione biometrica, ha riguardato il quesito di una multinazionale operante nel settore della promozione e vendita di prodotti farmaceutici, riguardo al progetto di attivazione di un sistema di credenziali di autenticazione dei propri agenti ed informatori scientifici basato sull'impiego delle loro impronte digitali.

In base alla dettagliata descrizione fornita dalla società è risultato che gli agenti (tutti incaricati del trattamento dei dati del proprio pacchetto clienti) ricevono in dotazione dalla società un *computer* portatile che contiene, come dotazione *standard*, un dispositivo per la rilevazione delle impronte digitali gestito da un *software* installato sul *computer*. Il dispositivo di riconoscimento e il relativo *software*, presenti su ciascun *computer*, sono attivabili solo dall'agente che voglia avvalersene. L'immagine dell'impronta viene registrata esclusivamente su un'area protetta del disco fisso del *computer* stesso ed associata ad una *password* scelta dall'utente e solo dallo stesso modificabile successivamente, senza alcuna centralizzazione in archivi aziendali o possibilità di accesso da parte della società al dato biometrico (anche in caso di malfunzionamento, il *computer* viene reso alla direzione informatica della

società che formatta il disco cancellando l'impronta registrata), il quale resta nell'esclusivo controllo dell'utente-incaricato che può cancellarlo in qualsiasi momento.

Nel caso di specie non è apparsa necessaria la valutazione preventiva del Garante tenuto conto delle caratteristiche del tutto peculiari del progetto e, soprattutto, della finalità di autenticazione informatica perseguita. L'adozione di un sistema di autenticazione informatica (mediante il quale gli incaricati dotati di apposite credenziali possono effettuare specifici trattamenti di dati personali), conforme ai requisiti tecnici indicati dalle regole 1.11. dell'Allegato B) al Codice, costituisce infatti una misura minima di sicurezza che il titolare, il responsabile (ove designato) e l'incaricato sono tenuti ad utilizzare (art. 34, comma 1, lett. *a)*, del Codice). Tali credenziali di autenticazione, come nel caso di specie, possono consistere anche in una caratteristica biometrica dell'incaricato, eventualmente associata ad un codice identificativo o a una parola chiave.

17 Registro dei trattamenti

Il registro dei trattamenti previsto dall'art. 37 del Codice ha consolidato la propria veste nel corso del 2005, nella nuova connotazione informatica che ha fornito esiti ancora più positivi in termini di efficienza, efficacia, economicità e rapidità nel monitoraggio.

Nel registro confluiscono come è noto le notificazioni del trattamento di dati personali, le quali pervengono al Garante secondo le procedure previste dall'art. 38. L'intera notificazione (compresa la firma) avviene telematicamente. Il registro è pubblico e chiunque può consultarlo, tramite il sito dell'Autorità, mediante un apposito motore di ricerca.

I contenuti della notificazione sono limitati alle informazioni essenziali sui trattamenti effettuati; rendono però possibile effettuare ampi controlli, estrazioni di dati ed elaborazioni statistiche. Il registro viene pertanto utilizzato dall'Autorità a fini di monitoraggio, controllo e orientamento delle attività ispettive in determinati settori.

Gli obiettivi posti con il nuovo sistema di notificazione (flessibilità del sistema; contenimento delle notizie da richiedere e ai titolari; semplificazione della procedura; pubblicità completa del registro dei trattamenti), la filosofia e il modello posti alla base della procedura, sono stati in seguito tenuti presenti per altre attività legate ai trattamenti che presentano rischi specifici *ex* art. 17 del Codice (verifica preliminare del Garante).

Preme evidenziare, rispetto all'esperienza di applicazione relativa all'anno precedente, il fattivo ausilio offerto all'utenza che ha avuto occasione di sollecitare ed ottenere chiarimenti dal dipartimento dell'Ufficio che vi è preposto.

Tra i momenti istituzionali di contatto con l'utenza si segnala la possibilità, offerta al notificante, di sospendere la notificazione in qualsiasi momento e di continuarla successivamente, utilizzando un codice numerico che viene spedito automaticamente dall'Ufficio, con due vantaggi immediati:

- l'utente può indicare il motivo della sospensione; il dipartimento è messo in grado di intervenire tempestivamente nel caso in cui l'utente stia effettuando una notificazione non dovuta, sia in difficoltà o non abbia compreso alcuni elementi, ovvero semplicemente intenda essere "guidato" o agevolato nella compilazione;
- viene così reso noto all'utente l'indirizzo *e-mail* dell'Ufficio, in seguito utilizzato frequentemente per altre richieste e segnalazioni.

Le difficoltà incontrate dagli utenti nella compilazione della notificazione (trattasi di un fenomeno comunque assai marginale) attengono –salvo quanto si dirà di seguito– quasi esclusivamente all'apposizione della firma digitale (possesso di un certificato scaduto, mancata lettura delle istruzioni, ecc.).

A questi elementi, deve aggiungersi l'esperienza che il dipartimento può continuare ad offrire rispetto ad alcuni dubbi interpretativi emersi nell'individuazione dei soggetti obbligati alla notificazione, anche dopo il provvedimento di esonero del Garante del 2004 e le connesse delucidazioni fornite con una risposta di ordine generale a quesiti (*Provv.* n. 1 del 31 marzo 2004 [doc. *web* n. 852561]; *Nota* 23 aprile 2004 [doc. *web* n. 993385]; *v.* anche *Nota* 26 aprile 2004 [doc. *web* n. 996680], visto che l'art. 37 del Codice descrive il suo ambito di applicazione con una disciplina

generale senza entrare in innumerevoli dettagli legati alle migliaia di diversi titolari del trattamento e di banche dati.

Nel 2005, a parte i picchi registratisi in occasione della scadenza di taluni termini per l'adempimento ad obblighi previsti dal Codice (a volte erroneamente associati all'obbligo di notificazione, come è avvenuto per la redazione del documento programmatico sulla sicurezza), il numero di notificazioni giornaliere ha oscillato tra le sei e le sette.

Le tabelle statistiche riportate in altra parte della presente relazione forniscono altri elementi utili per valutare come il registro si evolve. Ad esempio, dalle tabelle relative alle singole tipologie di trattamenti notificati, si riscontra una netta prevalenza di quelli riferiti alla salute, alla profilazione e alla solvibilità economica rispetto ad altri trattamenti.

Il versamento dei diritti di segreteria (euro 150,00 per ciascuna notificazione) resta possibile utilizzando *on-line* una carta di credito (circa il 22% dei casi) o con altri sistemi quali il bonifico bancario (30 %) o il conto corrente postale (48 %).

Sono stati poi previsti particolari accorgimenti sul piano della sicurezza: un messaggio di avvenuta ricezione della notificazione viene spedito dal dipartimento al notificante, unitamente ad un codice segreto (codice univoco del notificante, Cun) che permette l'eventuale modifica della precedente notificazione o la sua cessazione. Tale aspetto è monitorato costantemente ed eventuali anomalie sono segnalate ad altri dipartimenti dell'Ufficio.

Per agevolare il compito di apposizione della firma digitale, l'Autorità continua inoltre a dare applicazioni ad alcune convenzioni con Poste italiane S.p.A., Unappa (Unione nazionale professionisti pratiche amministrative), Alar (Associazione lavoratori autonomi riuniti) e Comune di Livorno, per permettere la notificazione, tramite l'ausilio di intermediari qualificati, anche a chi non voglia o non possa dotarsi del *kit* di firma digitale. Altri tentativi intrapresi dall'Autorità per estendere le convenzioni ad altri soggetti (banche, comuni, camere di commercio) non hanno per ora riscontrato l'interesse degli interlocutori.

Il notificante può inoltre rivolgersi a soggetti di fiducia (commercialisti, avvocati, notai, conoscenti, purché in possesso di chiave per la firma digitale), senza limitazioni. Il costo del servizio reso dall'intermediario convenzionato, consistente nella stampa della notificazione, nell'apposizione della firma digitale, nell'inserimento di eventuali riferimenti ai diritti di segreteria e nell'invio del *file* è pari ad un massimo di euro 25,00 che l'utente paga direttamente all'intermediario.

Alla data del 31 dicembre 2005, risultavano inoltrate 6.439 notificazioni tramite gli intermediari convenzionati, con prevalenza dell'utilizzo di Poste italiane S.p.A.

Va operato un cenno alla possibilità, consentita dal sistema in uso, di monitorare il flusso dei dati in arrivo e di compiere ricerche ed elaborazioni di statistiche, anche al fine di riscontrare richieste dei dipartimenti dell'Ufficio operanti nel settore giuridico, in particolare allo scopo di coadiuvare l'attività ispettiva. Risultano in particolare interessanti le interrogazioni volte ad estrarre, all'interno delle tabelle descrittive dei trattamenti, le categorie di dati, di interessati, le finalità e le modalità del trattamento, l'eventuale comunicazione dei dati e l'utilizzazione, per il trattamento dei dati, di un sito *web*.

A titolo sperimentale, il dipartimento ha assunto infine l'iniziativa di inviare automaticamente un messaggio di posta elettronica ad alcuni dipartimenti interni (compreso quello ispettivo), segnalando volta per volta l'avvenuta notificazione di trattamenti più significativi (*ad es.*, il trattamento di dati genetici trasferiti all'estero).

18 La trattazione dei ricorsi

18.1. *Considerazioni generali*

Uno strumento di tutela agile e "multiuso": questa definizione, nella sua sinteticità, sembra fotografare efficacemente il ruolo e la funzione che il ricorso, ai sensi degli artt. 145 e ss. del Codice, è venuto ad assumere nel quadro più generale della tutela dei dati personali. L'analisi del numero e della tipologia dei ricorsi proposti nel 2005 attesta la veridicità della definizione a conferma di un *trend* chiaramente emerso già negli ultimi anni. L'esame dell'ampia casistica affrontata in questi mesi dal Garante sottolinea, poi, l'utile funzione di "antenna" di questo strumento di tutela che segnala tempestivamente nuove frontiere della protezione dei dati e, al tempo stesso, evidenzia settori di maggiore "utilizzo" delle opportunità di tutela che il Codice offre.

In questo senso, lo sguardo agli ultimi due anni mette in luce un'autentica "esplosione" dei ricorsi relativi al trattamento di dati effettuato da banche e società finanziarie, con particolare riferimento alla comunicazione e conservazione delle informazioni negli archivi dei Sic (sistemi di informazioni creditizie), già comunemente noti come "centrali rischi private". La vicenda è significativa e rappresenta un interessante esempio di intreccio fra la dinamica sociale ed economica (la crescita esponenziale del credito al consumo in connessione con una fase di limitata disponibilità reddituale delle famiglie) e lo sforzo di disciplina di un settore che era privo di una normativa organica di riferimento.

In questo quadro sono emerse con forza le esigenze di tutela dei dati personali dei consumatori (esattezza dei dati, tempestività degli aggiornamenti, chiarezza informativa dei meccanismi di segnalazione nei citati Sic, definizione dei tempi di conservazione delle posizioni, ecc.) che, in equilibrato contemperamento con le esigenze di garanzia e stabilità degli operatori finanziari, hanno ispirato la disciplina ora affidata, essenzialmente, all'apposito codice di deontologia e di buona condotta di settore (*Provv.* n. 8 del 16 novembre 2004 [doc. *web* n. 1070713] e connesso provvedimento sul bilanciamento di interessi, *Provv.* n. 9 del 16 novembre 2004 [doc. *web* n. 1070779]).

Anche ricorsi presentati in altri campi hanno, parimenti, permesso di far emergere aspetti nuovi. Ne sono testimonianza diverse decisioni che hanno avuto a tema i trattamenti in Internet, così come l'utilizzo dei dati personali da parte degli operatori telefonici o le nuove forme che può assumere, nel quadro tecnologico attuale, il controllo sui lavoratori (*v.* par. 18.3).

18.2. *Profili procedurali*

Venendo in primo luogo a profili più strettamente procedurali, è possibile rilevare alcune linee di tendenza ormai consolidate.

Il ricorso, specie se proposto con l'assistenza di un legale, appare sempre più spesso utilizzato come "tassello" di una più ampia strategia difensiva: diventa, cioè, il veicolo privilegiato per acquisire le informazioni indispensabili alla tutela della posizione di un soggetto o per contestare, sotto lo specifico profilo della protezione

dei dati, operazioni poste in essere, ad esempio, nell'ambito di un rapporto contrattuale. In questo quadro, acquisisce rilievo l'intero "catalogo" dei diritti previsti dall'art. 7 del Codice per la cui tutela il ricorso viene proposto. Lo stesso, quindi, non è più funzionale solamente alla tutela del diritto di accesso ai dati, ma viene frequentemente e consapevolmente utilizzato per accertare l'origine dei dati personali, le finalità o le modalità di uno specifico trattamento o per sollecitare, in caso di violazione di legge, la cancellazione dei dati stessi.

La più ampia conoscenza dei diritti di cui all'art. 7 del Codice e della loro tutelabilità con lo strumento del ricorso ha fatto poi sviluppare, negli ultimi mesi, l'attività di terzi (talvolta associazioni di consumatori, in altri casi soggetti operanti in veste professionale di delegato) che hanno promosso numerose richieste volte ad accedere ai dati e ad ottenere successivamente la loro cancellazione, con particolare riferimento alle informazioni conservate negli archivi dei già citati Sic.

In alcuni casi, peraltro, la procedura del ricorso è dovuta passare attraverso una necessaria fase di regolarizzazione, secondo il disposto dell'art. 148, comma 2, del Codice, in quanto –ad esempio– le procure rilasciate ai soggetti incaricati di presentare ricorso in nome dell'interessato non erano accompagnate dalla necessaria firma autenticata dello stesso. In altri casi, la presentazione del ricorso è avvenuta senza essere stata preceduta dalla doverosa presentazione di un'istanza formulata ai sensi del citato art. 7 del Codice, allegando solamente l'esistenza di generici motivi di urgenza.

Al riguardo, il Garante è pervenuto a declaratorie di inammissibilità (*ad es.*, *Provv.* 14 luglio 2005 [doc. *web* n. 1157708]), ricordando che la presentazione in via di urgenza del ricorso è possibile, ai sensi dell'art. 146, comma 1, del Codice, solo fornendo prova del pregiudizio imminente e irreparabile che avrebbe impedito di procedere all'invio dell'interpello preventivo e di attendere il decorso dei quindici giorni previsti dalle citate disposizioni del Codice.

È stata altresì richiamata più volte l'attenzione degli interessati sul disposto dell'art. 5, comma 3, del Codice secondo il quale "il trattamento dei dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del (...) Codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione". Ciò ha reso inammissibile la presentazione di ricorsi incentrati su ipotesi di trattamento di dati relativi, ad esempio, a controversie fra vicini per installare impianti di sorveglianza (*Provv.* 19 ottobre 2005 [doc. *web* n. 1191132]), ferma restando l'applicazione del Codice quando il trattamento è risultato effettuato nell'ambito di un'attività professionale ed economica (*Provv.* 27 ottobre 2005 [doc. *web* n. 1195275]).

Infine, qualche breve annotazione statistica: nel corso dell'anno solare 2005, come evidenziato anche nelle tabelle riportate in altra parte della presente *Relazione*, il Garante ha definito la trattazione di 634 ricorsi.

18.3. *Brevi cenni sulla casistica*

Come in passato, si offre in questo paragrafo una succinta sintesi sui principali temi affrontati con le decisioni in materia di ricorsi, rimandando alle altre parti della relazione per l'ulteriore esame di alcune problematiche sottese alle decisioni stesse.

Diffusione di dati personali tramite siti Internet istituzionali

Meritano anzitutto di essere ricordate due vicende che hanno riguardato la diffusione di dati personali tramite i siti Internet di due autorità amministrative indipendenti.

Nel primo caso (*Provv.* 10 novembre 2004 [doc. *web* n. 1116068]; *cfr.* anche *Newsletter* 21-27 marzo 2005), il ricorso concerneva l'opposizione per motivi legittimi

al trattamento di dati personali contenuti in alcune decisioni (una delle quali risalente nel tempo) adottate dall'Autorità garante della concorrenza e del mercato pubblicate, tra l'altro, sul sito Internet della medesima autorità. Tali decisioni erano state correttamente pubblicate, in adempimento di specifici obblighi normativi, in relazione all'attività di un operatore economico sanzionato per pubblicità ingannevole.

Il provvedimento del Garante ha esaminato le implicazioni della conoscibilità via Internet di tali provvedimenti (specie in relazione alla possibilità di rinvenire agevolmente tali informazioni tramite l'utilizzo di motori di ricerca). Tale forma di diffusione dei dati può comportare infatti un sacrificio sproporzionato dei diritti dell'interessato, specie quando si tratta di provvedimenti risalenti nel tempo e che hanno raggiunto le finalità perseguite.

La questione affrontata nel caso di specie è risultata particolarmente delicata, richiedendo il contemperamento fra il dovere di informazione da parte di organi pubblici sulla propria attività, il diritto degli utenti e dei consumatori di conoscere l'esito di determinati provvedimenti sanzionatori e le non convergenti aspettative dei soggetti cui si riferiscono i dati "sanzionatori" diffusi. Con la decisione adottata, il Garante ha tra l'altro riconosciuto il pieno diritto-dovere dell'Antitrust di continuare a pubblicare i propri provvedimenti sul relativo sito *web*, modulando però nel tempo il periodo entro il quale le decisioni del tipo di quella in questione potranno essere direttamente individuabili nel sito Internet dell'Autorità tramite motori di ricerca esterni al sito stesso (non è stato posto in discussione un sistema di ricerca rapida delle decisioni all'interno del medesimo sito).

In un diverso caso, esaminato con decisione del 19 maggio 2005 [doc. *web* n. 1151205], l'Autorità ha invece constatato come non fosse giustificata da un idoneo presupposto normativo la diffusione indifferenziata, tramite il sito Internet dell'Autorità per la vigilanza sui lavori pubblici, di alcune specifiche informazioni contenute nel "Casellario informatico delle imprese qualificate". Per espressa limitazione derivante dalla specifica disciplina applicabile al caso di specie, tali dati devono essere resi agevolmente disponibili, ma solo alle stazioni appaltanti, e non possono essere invece oggetto di una diffusione indifferenziata in rete (*v. amplius* par. 2.5).

Le citate fattispecie, venute ad evidenza in conseguenza delle straordinarie potenzialità diffusive della rete Internet e dei meccanismi di "navigazione" nella stessa, hanno così fatto emergere prepotentemente e il tema del "diritto all'oblìo" e della sua declinazione nel presente quadro tecnologico.

Altri trattamenti svolti da soggetti pubblici

Vari, e molto differenziati tra loro, sono risultati i ricorsi che hanno riguardato trattamenti effettuati da pubbliche amministrazioni. Fra le principali problematiche emerse si può ricordare la decisione del 3 novembre 2005 [doc. *web* n. 1198422] con la quale il Garante ha riconosciuto come lecite e conformi alle disposizioni del Codice le modalità di acquisizione (tramite le liste elettorali) e di successivo utilizzo dei dati personali impiegati per inviare una pubblicazione istituzionale curata dal Ministero della salute.

Con altre decisioni (in particolare, quelle del 16 giugno 2005 [doc. *web* n. 1149999] e del 21 dicembre 2005 [doc. *web* n. 1217532]), sono stati esaminati nuovamente i profili concernenti l'accesso ai dati personali di dipendenti di pubbliche amministrazioni; ciò, richiamando le corrette modalità di riscontro a tali istanze delineate dall'art. 10 del Codice e le linee differenziali rispetto al diritto di accesso ad atti e documenti amministrativi disciplinato dalla l. n. 241/1990.

Sempre con riferimento a problematiche concernenti impiegati pubblici va ricordato il *provvedimento* del 30 novembre 2005 [doc. *web* n. 1215256] con cui è stata esaminata una vicenda relativa alla lamentata diffusione di dati personali sensibili a seguito dell'affissione di una determinazione dirigenziale all'albo pretorio di un

Comune. Con *provvedimento* del 21 dicembre 2005 [doc. *web* n. 1219054] l'attenzione è stata invece rivolta allo svolgimento di un procedimento disciplinare, sempre nell'ambito di un'amministrazione comunale.

I casi in cui i dati personali degli interessati sono stati oggetto di comunicazione ad altri soggetti pubblici o a privati, nonché le ipotesi di diffusione dei medesimi dati (a mezzo affissione all'albo pretorio, pubblicazione a stampa, divulgazione tramite la rete Internet, ecc.), sono stati, quindi, le principali ipotesi che hanno formato oggetto del contenzioso dinanzi all'Autorità in relazione all'attività degli enti pubblici. Ciò, a conferma della particolare sensibilità degli interessati per quelle operazioni di trattamento (comunicazione e diffusione appunto) che moltiplicano le potenzialità lesive di un eventuale uso illecito dei dati.

Trattamenti svolti presso sistemi di informazioni creditizie

Come già ricordato, il settore rispetto al quale si è registrato il maggior numero di ricorsi è stato quello dei Sic. Il 2005 ha rappresentato il primo anno di applicazione delle nuove disposizioni introdotte con il codice deontologico di settore e le decisioni adottate in proposito sono state l'occasione per una verifica del livello di conoscenza e di applicazione delle stesse. Forse in ragione di una non perfetta conoscenza del predetto codice deontologico e del connesso provvedimento di bilanciamento degli interessi, sono pervenuti molti ricorsi incentrati su richieste di "cancellazione totale" delle posizioni riferite ad un interessato, senza che sussistessero, però, i presupposti per un loro accoglimento: ciò, pur in presenza di ritardi o di altre patologie nei rimborsi dei finanziamenti o in ragione di regolarizzazioni molto recenti e destinate quindi a rimanere annotate negli archivi in questione per il lasso temporale previsto dal predetto codice deontologico.

I ricorsi proposti nei confronti dei gestori dei Sic hanno dato luogo spesso a decisioni molto articolate, soprattutto in presenza di numerose posizioni segnalate nelle relative banche dati dei Sic, riferite a prestiti, mutui, carte di credito a saldo o rateali, ecc.

Occorre infatti discernere fra posizioni "positive" (relative a finanziamenti regolari di cui è possibile chiedere la cancellazione previa revoca del consenso al trattamento dei relativi dati) e "negative" (per le quali opera il già richiamato provvedimento sul bilanciamento degli interessi e che possono essere conservate negli archivi dei Sic nel rispetto dell'articolata tempistica che il codice deontologico ha delineato).

Altri archivi contenenti dati relativi ad attività economiche e finanziarie

Numerosi ricorsi sono stati rivolti nei confronti di altri archivi di dati e relativi ad attività economiche.

L'esigenza di assicurare un ordinato svolgimento dei rapporti economici, di permettere una rilevazione puntuale dei rischi creditizi, di garantire la stabilità del sistema finanziario e di prevenire fenomeni di sovraindebitamento ha portato negli ultimi anni sia ad un'estensione del tipo di operazioni e/o di "patologie" finanziarie oggetto di monitoraggio, sia ad un rapido adeguamento alle procedure informatiche dei sistemi di rilevazione, al fine di garantire un maggior livello di affidabilità e trasparenza di questi ultimi.

Il soggetto più antico operante nel settore è, come noto, la "centrale rischi" gestita dalla Banca d'Italia, istituita già nel 1964 per raccogliere le segnalazioni relative ai finanziamenti di importo pari o superiore attualmente a euro 75.000 e ai crediti in "sofferenza". Nei confronti di tale soggetto (art. 8, comma 2, lett. *d)*, del Codice), non è però esperibile il ricorso *ex* art. 145 del Codice, pur rimanendo la possibilità di proporre una segnalazione all'Autorità. Ciò spiega perché alcuni ricorsi pervenuti in ordine a tali trattamenti siano stati dichiarati inammissibili.

Le istanze rivolte *ex* art. 7, e gli eventuali, successivi ricorsi, possono essere invece proposti nei confronti dei trattamenti effettuati presso "la centrale rischi di

importo contenuto" gestita, in conformità alle istruzioni della Banca d'Italia, da S.i.a. S.p.A. cui possono essere rivolte le istanze citate.

Con riferimento ai finanziamenti di più limitato importo ricadenti prevalentemente nel novero del credito al consumo operano, infine, le già indicate disposizioni sui Sic, soggetti rispetto ai quali, come detto, si è concentrato in maggior misura il contenzioso su ricorso del 2005.

Tipologicamente diverso è invece il fenomeno (oggetto di attenzione in numerosi ricorsi) della conservazione in appositi archivi distinti da quelli relativi ai Sic, di altri tipi di informazioni quali dati personali tratti dai registri immobiliari e dagli archivi delle ex-conservatorie, ai quali si applica quindi il disposto dell'art. 24, comma 1, lett. *c)*, del Codice.

A tale riguardo (nei numerosi casi che hanno riguardato richieste di cancellazione rivolte a Crif S.p.A.) l'Autorità ha preso atto della già avvenuta sospensione della loro visualizzazione nella banca dati, anche in relazione alle intervenute modifiche legislative concernenti i nuovi presupposti (oggetto peraltro di ampio contenzioso giudiziario) per la riutilizzazione commerciale di tali dati di cui all'art. 1, commi 368/371, l. n. 311/2004, nonché all'art. 1, comma 5, d.l. 10 gennaio 2006, n. 2, convertito con l. 11 marzo 2006, n. 81.