installare lettori di impronte digitali in ristoranti e pizzerie convenzionati al fine di controllare che l'accesso al servizio di ristorazione avvenisse esclusivamente da parte degli aventi diritto, l'Autorità aveva già avuto modo di chiarire nei primi mesi del 2004 che tale sistema era sproporzionato rispetto alle finalità di controllo della spesa perseguite (*Newsletter* 12-18 gennaio 2004).

In seguito, il Garante ha accertato che tale ente regionale per il diritto allo studio ha nuovamente manifestato la concreta volontà di installare tali sistemi di rilevazione delle impronte digitali per l'accesso ai servizi di ristorazione convenzionati, avendo riscontrato un aumento degli ingressi a tali esercizi di ristorazione da parte di soggetti non autorizzati. L'Autorità ha quindi disposto il blocco del trattamento di dati personali degli studenti effettuato tramite tale sistema di rilevazione delle impronte digitali, riaffermando il principio secondo cui la raccolta generalizzata di dati biometrici di un gruppo selezionato di individui (tutti gli studenti universitari iscritti ad un ateneo) risulta sproporzionata rispetto ad un generico bisogno di "regolare l'utilizzo del servizio ristorazione" in assenza di reali esigenze di sicurezza determinate da concrete e gravi situazioni di rischio (*Provv.* 16 dicembre 2004).

In tale occasione, è stato anche ribadito che i sistemi di rilevazione di impronte digitali rappresentano una *extrema ratio,* potendo essere attivati solo quando, dopo matura riflessione, altre misure (nel caso esaminato, la vigilanza all'ingresso delle mense, ovvero l'esibizione del tesserino di riconoscimento da parte degli studenti) siano valutate del tutto insufficienti o inattuabili, e non quando tale scelta risulti semplicemente meno costosa o di più rapida attuazione ovvero risponda a mere esigenze di apparenza o di "prestigio".

Sono in corso, inoltre, vari approfondimenti in merito a diversi progetti attivati da enti pubblici diretti a sostituire il normale controllo degli accessi al luogo di lavoro (foglio firme, *badge* magnetico) con sistemi di rilevazione delle impronte digitali o di altri dati biometrici come la geometria della mano.

15 Reti di comunicazione elettronica

15.1. *Notazioni introduttive*

Il rapido sviluppo tecnologico degli ultimi anni ha reso sempre più urgente l'individuazione a favore degli utenti dei servizi di comunicazione elettronica di un elevato livello di protezione dei diritti della personalità, con particolare riguardo alla protezione dei dati e del segreto nelle comunicazioni.

Anche in considerazione della crescente convergenza fra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione, l'Autorità è intervenuta, cooperando talora con altri soggetti istituzionali (come riferito nel par. 21.4) e con i diversi operatori del settore, svolgendo un'ampia serie di attività: adozione di provvedimenti, attività istruttorie ed ispettive (in taluni casi a seguito di ricorsi decisi dall'Autorità); intense, inoltre, le attività di studio e monitoraggio che in alcuni casi, come si vedrà più avanti, sono giunte ad uno stadio avanzato, con l'apertura di procedure di consultazione pubblica.

15.2. *Dati di traffico*

Si è già dato conto (v. *Relazione 2003*) delle modifiche apportate all'art. 132 del Codice, in materia di conservazione di dati di traffico per finalità di accertamento e repressione di reati (*ex* art. 3, decreto-legge 24 dicembre 2003 n. 354, convertito, con modificazioni, dalla legge 26 febbraio 2004, n. 45). Si può qui brevemente ricordare che, nella sua formulazione originaria, l'art. 132 prevedeva che, per le predette finalità, i fornitori di servizi di comunicazione elettronica dovessero conservare i dati relativi al traffico telefonico per trenta mesi; il citato decreto legge, approvato a ridosso dell'entrata in vigore del Codice, aveva prolungato il periodo di conservazione ad un periodo massimo di cinque anni, estendendolo anche al traffico su Internet.

Tale soluzione suscitò forti preoccupazioni anche al di fuori del circuito istituzionale; il Garante manifestò forti riserve, soprattutto alla luce della prevista estensione delle nuove regole al traffico su Internet, che avrebbe determinato una forte compressione delle garanzie della persona, anche in relazione ai principi costituzionali in materia di libertà delle comunicazioni e segretezza della corrispondenza.

La soluzione adottata in sede di conversione del decreto-legge ha portato a sopprimere ogni riferimento ai dati di traffico diversi da quello telefonico (in particolare Internet), determinando in complessivi quattro anni i tempi di conservazione dei soli dati di traffico telefonico.

Analoghe preoccupazioni, con espresso riferimento all'ipotesi di conservazione dei dati di traffico telematico, sono state ribadite dall'Autorità –nell'audizione in Commissione giustizia della Camera dei Deputati il 24 novembre 2004– in sede di esame del disegno di legge del Governo recante disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet (del quale si è riferito nel par. 1.2).

In questa occasione sono stati richiamati, oltre al quadro normativo europeo e nazionale e alla giurisprudenza costituzionale in materia di segretezza delle comuni-

cazioni, anche le conclusioni cui è pervenuto lo stesso Parlamento, in particolare nel corso della discussione del decreto-legge n. 354/2003 (cfr. par. 1.2). Nell'ambito dei dati di traffico telematico è stata altresì sottolineata la difficoltà di distinguere, anche sul piano tecnico, i dati "esteriori" (tutelati anch'essi dalla garanzia costituzionale, ma acquisibili sulla base di un ordine di esibizione da parte dell'autorità giudiziaria, senza le garanzie previste dal codice di procedura penale in materia di intercettazioni) da quelli di "contenuto". Infatti, vi sono diversi casi in cui dati apparentemente "esteriori" sono idonei a rivelare il contenuto della comunicazione (ad esempio, i messaggi allegati alle *e-mail*, i contenuti di *chat* e *newsgroup*), le scelte della persona e, in alcuni casi, anche dati sensibili (è il caso di dati di accesso ai siti *web*).

Fermo restando il potere-dovere dell'autorità giudiziaria e di polizia di accedere a fonti di prova eventualmente disponibili in base alla legge (ad es. i dati di traffico telefonico), è stato evidenziato il rischio che un eventuale obbligo di (indiscriminata) conservazione di tutti i dati di traffico telematico configuri già, esso stesso, una sostanziale limitazione della libertà e segretezza della corrispondenza e di ogni altra forma di comunicazione.

Con riferimento alla conservazione dei dati di traffico telefonico, il Garante, conformemente alla previsione dell'art. 132, comma 5, del Codice, ha avviato i lavori necessari a individuare le misure e gli accorgimenti al cui rispetto è subordinato il trattamento per le finalità di accertamento e repressione dei reati. A tale scopo sono stati acquisiti elementi utili nel corso di incontri con diversi operatori telefonici, al fine della verifica preliminare dei sistemi attualmente utilizzati, in conformità con quanto stabilito dall'art. 17, comma 2, del Codice, cui l'art. 132, comma 5, fa espresso richiamo.

Accesso ai dati di traffico

Per quanto concerne l'accesso ai dati personali relativi alle comunicazioni telefoniche "in entrata", l'Autorità ha più volte sottolineato (v., da ultimo, *Provv.* 18 febbraio 2004) come il Codice realizzi al riguardo un primo bilanciamento tra il diritto dell'interessato di conoscere i dati che lo riguardano e il diritto alla riservatezza di terzi (utenti chiamanti e soggetti chiamati diversi dall'abbonato), circoscrivendo il diritto del chiamato di accedere ai dati identificativi di telefonate in entrata alle sole informazioni la cui mancata conoscenza possa comportare "*un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397*" (art. 8, comma 2, lett. *f*), del Codice).

L'Autorità ha ricordato che l'interessato può presentare la propria richiesta di accesso anche prima che sia instaurato un procedimento penale: l'attività investigativa può essere svolta, ai sensi dell'art. 391-*nonies* c.p.p., anche dal difensore che ha ricevuto apposito mandato dalla persona offesa dal reato, per l'eventualità che si instauri un procedimento penale (*Provv.* 15 aprile 2004). Il Garante, pertanto, ha accolto una richiesta di accesso a dati personali relativi al traffico telefonico "in entrata", avendo ritenuto che sussistesse un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive che poteva derivare al ricorrente dalla mancata identificazione del numero telefonico chiamante.

Come evidenziato già nella *Relazione* 2003, il diritto d'accesso ai dati relativi al traffico telefonico può essere esercitato dall'interessato soltanto nei confronti dei dati che lo riguardano, risultando inammissibile la richiesta volta a identificare utenze diverse da quella dell'interessato medesimo.

In relazione a ciò, e in particolare all'accesso ai dati relativi alle chiamate nella telefonia mobile, l'Autorità ha valutato con esito positivo la risposta fornita da un operatore ad una richiesta formulata ai sensi dell'art. 157 del Codice. Il Garante, in particolare, aveva chiesto di conoscere la procedura predisposta dalla società e le

misure di sicurezza adottate al fine di identificare i soggetti che richiedono l'accesso stesso utilizzando il telefono mobile o i servizi *on-line*.

15.3. *I nuovi elenchi telefonici*

La disciplina degli elenchi è stata oggetto di significative modifiche. Scopo peculiare degli elenchi è di consentire la ricerca degli abbonati per le comunicazioni interpersonali; ciò è ora previsto espressamente dall'art. 129, comma 2, del Codice che sancisce, in relazione a tale finalità, il principio della massima semplificazione per l'inserimento degli abbonati negli elenchi e, per le finalità ulteriori, la necessità del preventivo consenso specifico ed espresso degli interessati.

In applicazione di tale principio, e in esito ad un'intensa attività svolta anche in collaborazione con l'Autorità per le garanzie nelle comunicazioni, il Garante ha individuato le modalità da osservare per il corretto inserimento e successivo utilizzo dei dati personali degli abbonati nei nuovi elenchi telefonici (*Provv.* 15 luglio 2004).

Nei nuovi elenchi telefonici possono essere pubblicati anche i dati relativi alle utenze mobili, nonché informazioni ulteriori quali l'indirizzo di posta elettronica, la professione e il titolo di studio. Nel caso in cui l'interessato abbia manifestato il proprio consenso a ricevere informazioni commerciali o promozionali, l'indirizzo o il numero telefonico saranno contrassegnati da uno speciale simbolo: in tal modo l'abbonato potrà ricevere pubblicità telefonica tramite operatore o materiale pubblicitario a domicilio. Diversamente, nel caso di iniziative pubblicitarie realizzate mediante sistemi automatizzati (fax, chiamate senza operatore, messaggi *sms* o di posta elettronica), è comunque necessario raccogliere a parte il consenso specifico dell'interessato. Le scelte espresse dagli interessati possono essere modificate in ogni momento e senza alcun onere.

Il Garante ha altresì predisposto, con la cooperazione dell'Autorità per le garanzie nelle comunicazioni e la collaborazione delle associazioni dei consumatori, un modulo di informativa e richiesta di consenso che gli operatori telefonici devono inviare ai propri clienti entro il 31 gennaio 2005.

Successivamente all'adozione del provvedimento, si sono svolti presso l'Autorità ulteriori incontri con rappresentanti degli operatori telefonici e delle associazioni di consumatori. Nel corso di tali incontri, e principalmente dall'esame dei primi moduli predisposti dalle diverse compagnie, sono emersi alcuni elementi che hanno reso necessario un nuovo intervento del Garante, volto a fornire agli operatori stessi prescrizioni integrative di quelle già impartite, nonché a dare l'avvio alla campagna informativa prevista nel provvedimento stesso.

L'Autorità ha curato una prima campagna di informazione attraverso un apposito *depliant*, che, su sua autorizzazione, verrà inviato dai gestori al domicilio degli abbonati. Un'apposita conferenza stampa si è tenuta il 26 gennaio 2005.

15.4. Spam

È costantemente all'attenzione dell'Autorità il fenomeno dell'invio ad indirizzi di posta elettronica di comunicazioni non sollecitate, non solo di contenuto commerciale, ma anche riconducibili all'ambito del cd. *marketing* politico (cfr. *Provv.* 12 febbraio 2004, oltre al più recente provvedimento del 12 ottobre 2004, presi in considerazione nel par. 8.2).

Gli utenti della Rete hanno manifestato un'accresciuta sensibilità in relazione al

fenomeno *spam*, desumibile dall'intenso contenzioso che ha investito l'Autorità anche nel 2004 (come ricordato nel par. 18.3), oltre che dalle azioni proposte dinanzi all'autorità giudiziaria ordinaria.

Sono proseguite le attività di controllo e verifica effettuate presso i fornitori di servizi di comunicazione elettronica (individuati grazie alle segnalazioni pervenute) al fine di accertare eventuali violazioni dell'art. 130 del Codice e delle prescrizioni contenute nel provvedimento di carattere generale emanato dal Garante il 29 maggio 2003.

Per arginare il fenomeno, il Garante ha partecipato ad alcuni incontri tenuti presso il Ministero delle comunicazioni, cui sono intervenuti operatori di telefonia fissa e mobile, e associazioni di fornitori dei servizi Internet e dei consumatori.

In tali incontri si è lavorato alla possibile stesura di un codice di autoregolamentazione in relazione al quale è stata chiesta la collaborazione di questa Autorità, che fornirà il proprio contributo tenendo però presente il valore cogente delle norme che saranno contenute nel codice di deontologia e di buona condotta per Internet (v. par. 15.8).

Proprio in questo settore, grande rilievo sugli organi di informazione ha avuto la vicenda relativa all'indagine giudiziaria curata dalla Guardia di finanza nei confronti di una società quotata in borsa in relazione all'utilizzo di migliaia di indirizzi *e-mail* per finalità di *marketing*, in assenza del consenso informato degli interessati.

Sulla vicenda, per la quale sono indagati due responsabili della società per reati che vanno dall'illecito trattamento dei dati personali alla frode informatica ed all'accesso abusivo a sistemi informatici, il Garante ha ricevuto di recente copia di alcuni atti e valuterà a breve l'eventuale adozione dei provvedimenti di competenza.

15.5. Sms *istituzionali*

In occasione delle elezioni del 12 e 13 giugno 2004, gli utenti di telefonia mobile hanno ricevuto *Sms* "firmati" dalla Presidenza del Consiglio dei ministri con i quali si comunicavano orari e modalità di voto delle imminenti consultazioni elettorali.

A seguito di più di 4500 reclami e segnalazioni il Garante, al fine di acquisire ogni elemento idoneo a valutare la questione, ha richiesto informazioni al Ministero dell'interno (che aveva disposto l'invio degli *Sms* con proprio d.m. del 9 marzo 2004) ed agli operatori di telefonia mobile.

Pur prendendo atto dell'esistenza nel caso specifico di un formale provvedimento del Ministro che ravvisava ragioni contingibili e urgenti, l'Autorità ha sottolineato in termini generali il rischio che impropri riferimenti all'eccezionalità, all'emergenza e alle calamità possano condurre ad una "banalizzazione" dell'invio di messaggi *Sms* da parte di diversi soggetti istituzionali, anche a livello locale (*Provv.* 7 luglio 2004).

Il Garante aveva peraltro già individuato nella eccezionalità e straordinarietà delle circostanze le condizioni per l'invio di comunicazioni via *Sms*, anche in mancanza di previo consenso dell'interessato (*Provv.* 12 marzo 2003).

In relazione alla decisione del Ministero dell'interno di indicare la Presidenza del Consiglio dei ministri come firmataria del messaggio, l'Autorità ha rilevato come nel caso di specie non operasse una disposizione della legge n. 150/2000 sulla comunicazione istituzionale, che riguarda l'invio di messaggi da parte della concessionaria del servizio pubblico radiotelevisivo (art. 3). Con riferimento all'invio di *Sms* in caso di disastri o calamità naturali o per ragioni di tutela dell'ordine pubblico, il soggetto istituzionale "mittente" delle comunicazioni deve poi essere sempre identificabile.

Nel medesimo provvedimento è stata altresì evidenziata la necessità per gli operatori telefonici di integrare l'informativa fornita ai cittadini inserendo la previsione dell'eventualità che, tra i vari trattamenti di dati legati alle utenze, vi sia quello dell'invio di *Sms* istituzionali per effetto di provvedimenti d'urgenza. Tutte le compagnie telefoniche interessate hanno integrato il modello di informativa come richiesto dal Garante.

È stata da ultimo richiesta la cooperazione del Garante da parte della Presidenza del Consiglio dei ministri e del Ministero degli affari esteri ai fini dell'acquisizione dalle compagnie di telefonia di alcuni dati relativi all'utenza mobile di cittadini italiani che si trovavano nelle zone colpite dal maremoto in Asia del 26 dicembre 2004; ciò, in particolare, al fine di consentire al Ministero di inviare un *Sms* agli interessati, invitandoli a dare notizie di sé (cfr. anche par. 1.3 e 15.10).

15.6. *Videochiamate*

Ha formato oggetto di esame da parte dell'Autorità il fenomeno delle cd. videochiamate, ossia le chiamate –realizzate attualmente tramite la rete *Umts*– nel corso delle quali vengono trasmesse, oltre ai suoni, anche immagini dei soggetti coinvolti nella conversazione. La caratteristica peculiare dei trattamenti realizzati in occasione delle videochiamate consiste nel fatto che, a differenza di quanto accade con l'invio degli *Mms* (in relazione al quale si veda il *Provv.* 12 marzo 2003), le immagini vengono trasmesse contestualmente all'effettuazione della chiamata e coinvolgono il chiamante, il chiamato ed eventuali persone situate nelle loro vicinanze.

Ferma restando la generale liceità dell'utilizzo di tali nuove applicazioni tecnologiche, sono di tutta evidenza anche i potenziali pericoli insiti nelle stesse: le videocamere, infatti, oltre ad essere normalmente di dimensioni assai ridotte, il più delle volte non sono dotate di dispositivi acustici o visivi atti a rivelarne il funzionamento all'esterno.

Al fine di acquisire ulteriori elementi di valutazione, il Garante ha attivato una consultazione pubblica preordinata ad un provvedimento che fornirà indicazioni di carattere generale sul corretto utilizzo dei nuovi telefoni mobili c.d. di terza generazione.

15.7. *Servizi di comunicazione elettronica offerti a titolo gratuito*

Non di rado viene rappresentata da parte di utenti dei servizi gratuiti di accesso ad Internet ed alla posta elettronica l'impossibilità di esprimere un consenso specifico e differenziato con riferimento alle diverse finalità del trattamento operato dai fornitori dei medesimi servizi. In particolare, viene talvolta negata la stessa opportunità di usufruire dei predetti servizi nel caso in cui l'utente non presti il consenso al trattamento dei dati per finalità pubblicitarie e commerciali.

In occasione della trattazione di uno specifico ricorso (*Provv.* 12 ottobre 2004) il Garante ha chiarito che è improprio richiedere un ampio e generalizzato consenso –peraltro anche quando lo stesso Codice permette di prescindere da esso, come, ad esempio, per l'eventuale comunicazione dei dati all'autorità giudiziaria (cfr. art. 24, comma 1, lett. *a*), del Codice)– associandovi finalità pubblicitarie e di profilazione per le quali non è lasciata all'utente alcuna libertà nella manifestazione di volontà. La mancata richiesta di consensi differenziati (e limitatamente ai casi in cui sono necessari) determina un quadro confuso che non permette all'utente di esprimere scelte libere, consapevoli e non contraddittorie fra loro.

In questa prospettiva, l'Autorità ha riaffermato la necessità che il consenso sia realmente espresso senza condizionamenti che ne influenzino sotto vari profili la libera manifestazione (art. 23, comma 3, del Codice).

Quanto all'eventuale trattamento dei dati dell'interessato per finalità di profilazione, è stato precisato che tale trattamento potrebbe risultare lecito in determinate circostanze qualora, per i rapporti contrattuali, la società preveda l'assegnazione di un accesso gratuito ad Internet dietro "corrispettivo" di una profilazione lecita, corretta e proporzionata dell'interessato medesimo.

15.8. *Il codice deontologico*

Nell'ambito delle iniziative promosse in vista della predisposizione del codice deontologico e di buona condotta sui trattamenti dei dati personali effettuati dai fornitori dei servizi di comunicazione ed informazione offerti per via telematica (art. 133 del Codice), è stata avviata la consultazione delle organizzazioni rappresentative degli operatori del settore e dei consumatori che hanno aderito all'invito a partecipare formulato in precedenza dall'Autorità. Ciò è stato ritenuto opportuno al fine di identificare, congiuntamente ai soggetti a vario titolo interessati, gli aspetti che presentano particolari criticità sotto il profilo della protezione dei dati.

Alla luce dei primi contributi pervenuti, nonché degli studi da tempo avviati dalla stessa Autorità, sono state individuate alcune specifiche questioni che potranno essere oggetto di disciplina nell'adottando codice. Tra queste si ricordano, ad esempio, le modalità ed i contenuti dell'informativa; i profili relativi all'acquisizione del consenso ed ai diritti degli interessati; l'adozione di particolari misure di sicurezza; gli strumenti tecnici e giuridici di contrasto del fenomeno dello *spamming*, ivi compresa l'adozione di procedure di filtraggio o altre misure praticabili; l'individuazione di bollini di qualità per il trattamento dei dati posti in essere dagli operatori del settore; i problemi relativi alla registrazione dei nomi a dominio.

La definizione del codice in questione potrà fornire, sia agli operatori, sia agli utenti delle reti di comunicazione elettronica, riferimenti più precisi per assicurare il rispetto della normativa sulla protezione dei dati personali e, in particolare, dei principi generali di cui all'art. 11 del Codice.

15.9. *La televisione digitale: i servizi interattivi*

L'Autorità ha ultimato uno specifico studio sulle caratteristiche della televisione satellitare e interattiva individuando alcuni primi aspetti di rilevanza per la normativa sulla protezione dei dati personali.

Grazie allo sfruttamento delle potenzialità offerte dalla tecnologia digitale, è possibile offrire attraverso la televisione anche servizi caratterizzati dall'interattività: attraverso il collegamento di un apposito apparecchio (*decoder*) alla linea telefonica, l'utente può, ad esempio, partecipare a sondaggi, giochi, test o usufruire di particolari servizi di pubblica utilità erogati dalle amministrazioni pubbliche (cd. *T-government*), o ancora, usufruire di servizi cd. transattivi, previa identificazione ed autorizzazione, grazie all'inserimento nel *decoder* medesimo di particolari "carte identificative" (*smart card*).

Agli indubbi vantaggi derivanti da questa tecnologia, si affiancano, tuttavia, alcune criticità con riguardo alla tutela della sfera privata degli utenti: l'uso dei servizi e programmi interattivi può determinare un'esposizione, anche inconsapevole,

dei gusti, delle abitudini ed in generale della personalità dell'utente. Questi dati, opportunamente raccolti e trattati, potrebbero dare luogo al monitoraggio delle preferenze e dell'attività dell'utente medesimo. La circostanza che la raccolta dei dati avvenga in un ambito tipicamente "privato" (come quello familiare, nel quale l'individuo nutre la ragionevole aspettativa di essere al riparo da forme di controllo esterne) suscita ulteriori preoccupazioni. Inoltre, ad uno stesso apparecchio televisivo corrispondono di regola più fruitori (appartenenti o estranei al nucleo familiare dell'abbonato), i quali debbono essere messi in grado di compiere liberamente le proprie scelte in merito al trattamento dei dati personali che li riguardano.

Proprio al fine di approntare idonee cautele onde evitare che siano svolte illecite operazioni di profilazione ed invasive forme di controllo sulle abitudini delle persone, l'Autorità ha avviato una consultazione pubblica in vista della predisposizione di un provvedimento a carattere generale.

15.10. *Dati relativi all'ubicazione*

Negli ultimi anni si è assistito ad una rapida diffusione dei servizi basati sull'ubicazione. Tali servizi, pur presentando aspetti di indubbia utilità, possono comportare seri rischi per le libertà civili dell'interessato, potendo determinare un'esposizione, anche inconsapevole, dello stesso ad un controllo sistematico dei suoi spostamenti ovvero dei gusti e delle abitudini manifestati in occasione di specifiche richieste.

In questa prospettiva assume una particolare importanza il fatto che l'interessato sia pienamente a conoscenza delle caratteristiche del trattamento di dati che lo riguarda, nonché dei soggetti che svolgono il trattamento medesimo; ciò, anche al fine di prestare un consenso libero, specifico ed informato.

Proprio in ragione della particolare delicatezza di tali trattamenti, l'Autorità intende offrire indicazioni e chiarimenti ai soggetti che vogliano fornire tali tipologie di servizi. Al riguardo si segnala che il Garante sta ultimando la predisposizione di un provvedimento di carattere generale a completamento di quanto già disposto in materia dall'art. 126 del Codice.

Uno sviluppo di queste problematiche si è avuto con la menzionata richiesta della Presidenza del Consiglio dei ministri di acquisire dai vari gestori di telefonia mobile i dati di cittadini italiani che, in relazione alle informazioni sull'ubicazione dell'apparecchio disponibili presso i gestori stessi, risultavano trovarsi negli stati colpiti dal maremoto in Asia (v. par. 1.3 e 15.5).

Ferma restando la necessità di bilanciare la tutela della riservatezza con esigenze di salvaguardia della vita e dell'incolumità delle persone, questa vicenda pone (su un piano più generale) l'interrogativo se i dati relativi all'ubicazione degli apparecchi di telefonia mobile (e quindi, indirettamente, delle persone che li detengono), allorché siano diversi dai dati relativi al traffico telefonico –assistiti, questi ultimi, dalle garanzie costituzionali di libertà e segretezza della corrispondenza– godano comunque di una tutela costituzionale, e quale, anche alla luce del principio della libertà di circolazione (art. 16 Cost.).

15.11. Radio Frequency Identification

Il Garante ha seguito con grande attenzione lo sviluppo delle tecniche di identificazione via radiofrequenze (*Radio Frequency Identification-Rfid*).

Tali tecnologie si fondano sull'utilizzo di micro-processori che, collegati ad

un'antenna ed impiegati come etichette di riconoscimento (*cd. etichette intelligenti*), sono in grado di trasmettere –attraverso onde radio– segnali leggibili da appositi lettori dotati di un'antenna di attivazione/ricezione.

La *Rfid* rappresenta uno strumento utile in numerosi settori e per diverse finalità: essa può essere impiegata, ad esempio, per il "tracciamento" di singole unità di prodotto nella catena di distribuzione dell'industria; per la prevenzione di furti e di contraffazioni dei prodotti; per garantire una maggiore rapidità nelle operazioni commerciali; per il controllo degli accessi ad aree riservate. L'utilizzo di questa tecnologia può, in alcuni casi, comportare un trattamento di dati personali rendendo necessaria l'applicazione della relativa normativa. Attraverso le cd. "etichette intelligenti" si possono trattare, anche senza che l'interessato ne sia a conoscenza, innumerevoli dati personali che lo riguardano, compresi quelli di natura sensibile; raccogliere dati sulle abitudini del medesimo ai fini di profilazione attraverso l'aggregazione con altre informazioni di carattere personale; verificare prodotti (vestiti, accessori, medicine, ecc.) indossati o trasportati; tracciare i percorsi effettuati.

Il Garante ha svolto una prima attività di approfondimento della materia in questione, rivolgendo l'attenzione al possibile impatto che le tecniche di identificazione via radio possono già avere sulle condizioni di esercizio delle libertà delle persone e alle problematiche che la loro introduzione è destinata a sollevare relativamente all'applicazione della normativa sulla tutela dei dati personali.

Tutto questo anche in vista del fatto che, se attualmente il terreno di elezione della *Rfid* appare ancora il settore industriale (soprattutto all'interno della catena di distribuzione, dove però la sua applicazione non comporta, il più delle volte, un trattamento di dati personali), tale tecnologia presenta enormi potenzialità: in prospettiva, anche in vista dell'ulteriore sviluppo tecnologico, dell'abbattimento dei costi di produzione, della possibilità di integrazione con altre infrastrutture di rete (telefonia, Internet, ecc.), le tecniche di identificazione via radio-frequenza potranno avere un impiego sempre maggiore e nei più diversi settori.

Occorre tenere altresì presente che più gravi pericoli per gli interessati possono derivare dal prevedibile incremento della potenza dei sistemi di *Rfid* (i quali potrebbero rendere fattibile una "lettura" delle etichette a maggiori distanze) nonché –specie in ragione dell'adozione di *standard* tecnici comuni– dalla possibilità che terzi non autorizzati "leggano" i contenuti delle etichette o intervengano sugli stessi (mediante, ad esempio, "riscrittura").

L'attività istruttoria compiuta dall'Autorità in merito al trattamento dei dati nell'ambito della *Rfid* si è svolta anche attraverso contatti in Italia e all'estero con alcuni operatori del settore, che hanno portato ad un proficuo scambio di informazioni.

Consultazione pubblica

Al medesimo scopo è stata indetta una specifica consultazione pubblica cui è stata data ampia visibilità anche attraverso il sito *web www.garanteprivacy.it*. A completamento delle informazioni già acquisite, l'Autorità si è così potuta avvalere degli ulteriori elementi di valutazione provenienti da osservazioni e commenti inviati dalle associazioni di utenti, consumatori, operatori dei settori interessati e singoli cittadini.

Impianto sottocutaneo di etichette *Rfid*

Uno dei più recenti ambiti di utilizzo di questa tecnologia riguarda l'impianto sottocutaneo di dispositivi *Rfid* anche su persone. Si ha già notizia dell'avvio, anche in Italia, di tecniche di inserimento di *microchip* nel corpo umano per diverse finalità: ad esempio, allo scopo, di conservare e rendere all'occorrenza disponibili informazioni sullo stato di salute del paziente; al fine di verificare l'accesso a determinati luoghi riservati; ancora, per garantire pagamenti rapidi in transazioni commerciali di vario tipo.

La delicatezza di tali interventi è di tutta evidenza, sì da sollevare interrogativi circa le ripercussioni che i relativi trattamenti possono avere sulla dignità della persona (art. 2, comma 1, del Codice).

16 Sicurezza dei dati e dei sistemi

16.1. *Le misure minime di sicurezza*

L'Autorità –a seguito di numerose richieste di proroga e di chiarimenti pervenute circa il nuovo quadro normativo in materia di misure minime di sicurezza introdotto dal Codice– ha precisato che l'applicazione delle misure minime (artt. 33-35 del Codice e allegato B), la cui omessa adozione costituisce reato (art. 169 del Codice), va graduata a seconda che i trattamenti di dati personali, sensibili e giudiziari, siano effettuati con o senza l'ausilio di strumenti elettronici. Queste misure rappresentano, però, solo i requisiti minimi ai quali tutti i titolari del trattamento (anche a mezzo del responsabile, ove designato) devono attenersi nella protezione dei dati. Vi è, infatti, il dovere più generale di adottare misure preventive idonee (art. 31 del Codice), la cui mancata predisposizione può esporre il titolare a responsabilità civile per eventuali danni cagionati a terzi (*Nota* 22 marzo 2004).

Nella stessa sede il Garante ha ricordato anche che la redazione del Documento programmatico sulla sicurezza (Dps) rientra tra le misure minime di sicurezza e che qualsiasi titolare pubblico o privato deve redigerlo se effettua un trattamento di dati sensibili e/o giudiziari con strumenti elettronici.

Inoltre, le misure minime già previste dal d.P.R. n. 318/1999 e riprodotte nell'allegato B) restano obbligatorie senza differimenti. Il termine transitorio, di recente nuovamente prorogato al 30 giugno 2005 (decreto-legge 9 novembre 2004, n. 266, convertito, con modificazioni, con legge 27 dicembre 2004, n. 306; salva l'ulteriore proroga al 30 settembre 2005, da riferire al solo caso in cui obiettive ragioni tecniche non consentano di adottare subito alcune misure) riguarda, infatti, solo le "*nuove*" misure minime che non erano già previste dal citato d.P.R. n. 318/1999 (art. 180, comma 1 e 3, del Codice).

L'Autorità ha inoltre precisato che è sostenibile ipotizzare che la redazione del Dps sia una "nuova" misura minima, con la conseguenza che, anche per questo adempimento, vale il termine del 30 giugno 2005. Il Garante ha poi messo a disposizione degli operatori, sul proprio sito *web*, una guida utilizzabile per agevolarne la redazione soprattutto presso le realtà medio-piccole.

Gli stessi principi sono stati tra l'altro confermati dall'Autorità nel già richiamato parere reso al Consiglio nazionale forense (*Nota* 3 giugno 2004) sui principali adempimenti in materia di protezione di dati personali nello svolgimento dell'attività forense, con il quale si è anche precisato che, per quanto riguarda l'organizzazione del lavoro quotidiano di studio, non occorre affatto depennare il nome delle parti dalla copertina dei fascicoli cartacei ed utilizzare solo numeri identificativi. Resta invece necessario seguire opportune modalità per rendere i fascicoli e la relativa documentazione accessibili agli incaricati del trattamento nei casi e per le finalità previsti.

L'orientamento del Garante è stato inoltre ribadito con un recente parere, anch'esso già menzionato (*Nota* 3 dicembre 2004), in materia di trattamento dei dati personali da parte dei notai rilasciato al Consiglio nazionale del notariato (v. pure par. 10.2).

Profili applicativi

Su richiesta di un dipendente di un ufficio legale comunale, l'Autorità ha rilevato i limiti entro i quali un dirigente può utilizzare la *password* del dipendente per accedere ai dati contenuti nel suo *computer* in caso di assenza di quest'ultimo.

L'adozione di un sistema di "autenticazione informatica" per gli incaricati del trattamento effettuato con strumenti elettronici rientra tra le misure "minime" di sicurezza aggiornate dal Codice. Secondo le modalità tecniche specificate nell'allegato B) del Codice, tale sistema deve basarsi sull'attribuzione all'incaricato di credenziali di autenticazione che possono consistere anche in un codice per l'identificazione associato ad una parola chiave riservata conosciuta solamente a quest'ultimo (regole nn. 1 e 2).

In particolare, quando i dati sono accessibili soltanto attraverso l'uso di parole chiave è possibile rendere disponibili le medesime informazioni solo in caso di prolungata assenza o impedimento dell'incaricato, sempre che l'intervento si rilevi indispensabile e indifferibile e sia altresì esclusivamente motivato da esigenze di operatività o di sicurezza del sistema. Proprio in vista di tali evenienze, è necessario individuare con chiarezza le modalità attraverso le quali il titolare può assicurare la disponibilità dei dati mediante idonee e preventive indicazioni fornite per iscritto. In tal caso, l'incaricato deve essere tempestivamente informato dell'intervento effettuato (regola n. 10 dell'allegato B).

Tali accorgimenti, oltre a consentire di proteggere i dati personali contenuti nella memoria dell'elaboratore dalla possibile intrusione di soggetti non autorizzati –specie se si tratta di dati giudiziari, come del caso sottoposto all'esame dell'Autorità–, permettono contestualmente di renderli disponibili in particolari casi di necessità e urgenza per trattamenti consentiti ed effettuati secondo modalità predeterminate chiaramente per iscritto dal titolare (*Nota* 16 luglio 2004).

A conclusione degli accertamenti svolti in seguito ad alcune segnalazioni relative alla raccolta e al trattamento di dati personali di clienti effettuato da una società nell'ambito di un servizio sperimentale di gestione *on-line* di polizze assicurative, l'Autorità ha ritenuto soddisfacente il riscontro fornito circa le misure tecniche ed organizzative adottate a protezione delle transazioni effettuate sul proprio *server web*. Gli accessi alle banche di dati personali relativi alle polizze assicurative, consentiti solo ad utenti registrati in apposite aree riservate del sito *web* della società, sono risultati protetti tramite specifiche misure di sicurezza (cd. protocollo *https*).

Si è comunque ricordato alla società che, per il trattamento di dati personali sensibili e/o giudiziari effettuato con strumenti elettronici, devono essere comunque adottate preventivamente idonee misure di sicurezza (art. 31 del Codice), oltre a quelle minime prescritte dal Codice (*Nota* 22 ottobre 2004).

L'Autorità sta concludendo accertamenti a seguito di un reclamo con il quale si è segnalata la diffusione di dati personali causata dall'asserito abbandono di documenti, da parte di una filiale della banca, in occasione del rilascio dei locali ove si svolgeva la sua attività (*Nota* 29 luglio 2004).

Il Garante si è inoltre pronunciato sul reclamo di un lavoratore che contestava le modalità di consegna di una lettera di sanzione disciplinare da parte del datore di lavoro (*Nota* 23 novembre 2004). Il dipendente aveva ricevuto una comunicazione di sanzione disciplinare contenuta in un foglio non spillato, né racchiuso in busta sigillata, consegnatogli a mano e recante la chiara indicazione dell'oggetto della lettera e della sanzione comminata. Dando attuazione ai principi di proporzionalità, pertinenza e non eccedenza dei dati, è stato chiesto alla società di prevedere che la comunicazione della sanzione all'interessato venga in ogni caso inserita in busta chiusa e sigillata; è stato inoltre prescritto di impartire precise istruzioni a tutti gli uffici e dipendenti formalmente incaricati di tali trattamenti di dati, volte all'ado-

zione di modalità e misure idonee a garantire la sicurezza e la riservatezza di comunicazioni contenenti dati relativi ai lavoratori interessati e ad evitare un accesso, anche casuale, da parte di terzi non autorizzati ai dati riportati al loro interno.

Ricevuta la segnalazione di un dipendente di una società che, alla ripresa del servizio dopo un prolungato periodo di assenza dal lavoro, non aveva trovato alcuni documenti personali lasciati in un armadio aziendale, l'Autorità dovrà valutare se sussistono o meno profili di violazione della normativa di protezione dei dati, anche in relazione alla circostanza che i documenti in questione siano relativi a trattamenti effettuati per ragioni di servizio.

17 Registro dei trattamenti

17.1. *La notificazione*

Linee normative

La nuova modalità di notificazione del trattamento dei dati personali al Garante (disciplinata dagli artt. 37, 38, 181, comma 1, lett. *c*), del Codice) presenta profondi cambiamenti sia nei contenuti, sia nelle modalità di compilazione, rispetto alla precedente normativa (artt. 7, 16 e 28, l. n. 675/1996): basti qui ricordare che, mentre quest'ultima prescriveva un obbligo di carattere generale di notificazione per un numero consistente di trattamenti –salve, comunque, le varie eccezioni previste dalla legge–, il Codice reca ora un più ristretto "elenco positivo" di trattamenti soggetti ad obbligo di notificazione, che il Garante può peraltro sviluppare attraverso un proprio provvedimento, il che attesta la conformità della soluzione innovativa ora prescelta dal legislatore italiano alla direttiva europea.

Il provvedimento di esonero

Il Garante si è già avvalso del potere di esonerare dal predetto obbligo alcuni trattamenti rientranti nelle generali previsioni di cui all'art. 37, ma in concreto ritenuti non suscettibili di recare specifico pregiudizio ai diritti e alle libertà dell'interessato (art. 37, comma 2). In base a tale disposizione con il provvedimento n. 1 del 31 marzo 2004 (v. *Documentazione* par. 39), l'Autorità ha individuato diverse ipotesi di trattamento sottratte all'obbligo di notificazione: è stato previsto, ad esempio, un esonero per il trattamento di dati genetici e biometrici trattati in maniera non sistematica da esercenti la professione sanitaria, purché non organizzati in banche dati accessibili da terzi; o, ancora, per il trattamento dei medesimi dati da parte degli avvocati, purché necessario a condurre investigazioni difensive o a far valere o difendere un diritto anche da parte di terzi in sede giudiziaria. È altresì possibile che, all'esito di questa prima fase di applicazione del Codice, si possano individuare, anche in collaborazione con le categorie interessate, ulteriori esoneri dall'obbligo di notificazione.

Il Garante ha poi ritenuto, allo stato, di non individuare ulteriori trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in aggiunta alla lista figurante nell'art. 37, comma 1, e pertanto da sottoporre all'obbligo di notificazione.

Ulteriori chiarimenti del Garante

Dopo il provvedimento che ha espressamente escluso la notificazione per alcuni trattamenti di dati personali, l'Autorità ha fornito numerosi chiarimenti per il settore privato (imprese, banche, assicurazioni, professionisti, enti *no-profit*) su alcuni trattamenti che devono ritenersi comunque sottratti all'obbligo di notificazione in base ad una corretta interpretazione delle disposizioni del Codice (*Nota* 23 aprile 2004; v. anche *Newsletter* n. 209 del 5-25 aprile 2004); ulteriori chiarimenti sono stati forniti in risposta a quesiti presentati dalla FnomCeo, dalla Fimmg e dall'Anisap, circa l'esatta individuazione dei trattamenti da notificare al Garante in ambito sanitario (*Nota* 26 aprile 2004; v. anche *Newsletter* n. 210 del 26 aprile-2 maggio 2004, consultabili sul sito *web* dell'Autorità).

La nuova notificazione

Accanto alla forte riduzione del numero dei trattamenti, è stata operata contemporaneamente, alla luce dell'esperienza, una drastica semplificazione dei contenuti e delle

modalità di compilazione del modello informatico. La nuova notificazione può avvenire anzitutto solo in via telematica e accompagnata dalla firma digitale; gli elementi richiesti sono pochi, ma significativi, di immediata comprensione e di facile redazione.

Il nuovo sistema ha così prodotto solo un numero limitato di notificazioni (circa 10.000 rispetto alle oltre 330.000 pervenute precedentemente ai sensi della legge n. 675/1996), circoscrivendo l'istituto alle sole ipotesi di trattamento "rischioso" per gli interessati, come prescritto dalla normativa comunitaria, e azzerando i casi di notificazione irregolare che avevano comportato in passato un onere assai rilevante per l'Ufficio del Garante.

Risoluzione di inconvenienti tecnici

Alcune temporanee e iniziali difficoltà tecniche dovute all'enorme traffico telematico registrato a ridosso della scadenza del termine per adempiere all'obbligo di notificazione fissato per il 30 aprile 2004 hanno indotto il Garante, avvalendosi delle facoltà previste dall'art. 38 del Codice, a riconoscere ulteriori quindici giorni a coloro che avevano tempestivamente intrapreso le operazioni di notificazione e che, per impossibilità tecniche a loro non imputabili, non erano riusciti a concludere la procedura. Alcuni interventi sulla stampa di dirigenti dell'Ufficio hanno ricostruito i punti estremamente interessanti di questo primo riuscito esperimento generalizzato nella p.a. di utilizzo della firma digitale per la produzione di un atto a rilevanza giuridica anche penale.

Il consistente potenziamento della banda trasmissiva utilizzata anche da molti visitatori interessati ad analizzare la procedura pur non dovendo notificare in concreto, e il breve differimento al 15 maggio 2004 del termine per concludere la notificazione hanno offerto agli utenti idonee opportunità di completare le operazioni di notificazione senza ulteriori problemi.

I vantaggi della procedura telematica

La procedura per la notificazione in via telematica ha dato ottima prova anche sotto l'aspetto della facilità d'uso. Il fatto che la medesima possa essere avviata e portata a termine nella sua interezza da una qualsiasi postazione, in qualunque momento e con l'assistenza *on-line* da parte del personale dell'Autorità durante l'orario d'ufficio, costituisce un indubbio vantaggio per l'utente.

Le procedure telematiche di notificazione si sono rivelate di qualità elevata per celerità nell'effettuare adempimenti e ricerche, affidabilità del programma di gestione, correttezza dei dati inseriti e puntualità nei riscontri.

Ulteriori prospettive

Permane tra gli obiettivi del Garante quello di mantenere alta la qualità del sistema di notificazione arricchendolo nel tempo di ulteriori elementi e procedure anche al fine di tenerlo al passo con lo sviluppo tecnologico e le prospettive di miglioramento complessivo delle attività dell'Autorità.

Accanto al perfezionamento dell'attuale versione, non va esclusa nel medio periodo la possibilità che, in conformità a quanto verrà deciso a livello europeo sulla standardizzazione della notificazione nei vari paesi, siano apportate modifiche al registro dei trattamenti e ai contenuti della notificazione. Una delle modifiche potrebbe, ad esempio, riguardare la redazione del modello anche in lingua inglese.

Nel corso dell'anno 2005 il Dipartimento registro dei trattamenti sarà comunque impegnato già nella predisposizione e messa a disposizione del modello di notificazione in lingua tedesca (come già avvenuto per la provincia di Bolzano con il vecchio modello di notificazione su carta).

Doppia notificazione

Nonostante il sistema di notificazione risulti agevole anche a fronte delle istruzioni esaustive e replicate in diversi passaggi della procedura, si sono riscontrati

pochi casi (limitati a qualche decina) di doppia notificazione da parte dello stesso titolare o di richiesta di annullamento di quella già inviata in quanto non dovuta.

L'orientamento dell'Ufficio è stato quello di restituire l'importo dei diritti di segreteria a coloro che, pur avendo iniziato la notificazione, non avevano ancora proceduto all'invio della medesima al Garante. Nei casi di doppia notificazione, invece, su dichiarazione del titolare, l'Ufficio ha provveduto ad "oscurare" una delle due, restituendo i diritti di segreteria pagati in eccesso.

Annullamento di notificazione inviata

Non sono state accolte, invece, le richieste di semplice "annullamento" della notificazione da parte di coloro che l'avevano validamente inviata, nonostante fosse a posteriori ritenuta non dovuta secondo il giudizio sopravvenuto del (solo) titolare del trattamento. Questo diverso orientamento si giustifica con il fatto che in tali casi la notificazione è regolarmente inserita nel registro (pubblico) dei trattamenti e ha dispiegato i suoi effetti (tenuto conto, tra l'altro, che l'inserimento nel registro non produce conseguenze negative sul titolare).

Assistenza agli utenti

Come già detto, il Garante ha fornito –e continua a fornire– ai soggetti tenuti alla notificazione un'attività di assistenza che si sostanzia in diverse forme: risposta ai numerosi quesiti e dubbi sulla notificazione, comunque formulati; controlli costanti dei messaggi inoltrati via *web* dagli utenti in caso di sospensione della notificazione e immediato riscontro via posta elettronica; effettuazione di controlli richiesti dai vari dipartimenti del Garante in occasione di istruttorie, attività ispettive e ricorsi.

17.2. *Il registro dei trattamenti e futuri sviluppi*

Le notificazioni regolarmente presentate sono confluite nel registro dei trattamenti.

Tale registro si è rivelato di maggiore utilità ed efficacia rispetto al precedente, non solo al fine di predisporre interventi ispettivi nei confronti di soggetti tenuti alla notificazione. Ulteriori benefici provenienti dal *database* riguardano, infatti, la possibilità di elaborare più efficacemente varie statistiche: esse costituiscono un importante strumento di comprensione dei fenomeni che ruotano intorno a trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà degli interessati; forniscono, inoltre, al Garante un significativo quadro di insieme in merito ai trattamenti effettuati; danno impulso, infine, alle attività di controllo assistite dal nucleo della Guardia di finanza.

In tale prospettiva, il Garante intende procedere all'affinamento di specifiche statistiche e alla creazione di sistemi che prevedano l'invio di una segnalazione automatica nel caso in cui la notificazione contenga elementi che si ritiene debbano essere sottoposti ad approfondimento.

Particolare cura verrà posta nel riscontro automatico dei pagamenti dei diritti di segreteria effettuati mediante banca e uffici postali, con la collaborazione della banca tesoriera e di Poste S.p.A.

Controlli a campione e audizioni in caso di contestazioni amministrative

Esaurita la fase di immissione della maggior parte delle notificazioni alla scadenza del 30 aprile 2004, sono stati effettuati diversi controlli a campione sulla congruenza dei dati dichiarati, sul ritardo o l'omissione della notificazione. A richiesta, il notificante viene ammesso ad un'audizione nella quale un funzionario del dipartimento stila una relazione sullo stato della notificazione.