La sicurezza pubblica e privata

36 Il trasferimento dei dati *Pnr (Passenger name record)* dei passeggeri

Anche nel corso del 2003 il trasferimento dei dati personali dei passeggeri alle autorità doganali di Paesi non appartenenti all'Ue ha rappresentato uno dei punti chiave dell'attività del Gruppo costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE. Tali tematiche, già affrontate nel 2002 in relazione agli Stati Uniti (Parere 6/2002 WP 66 del 24 ottobre 2002), hanno assunto speciale rilevanza nell'ultimo anno anche per le istanze presentate in proposito da Canada ed Australia, alimentando il dibattito europeo ed internazionale sul giusto equilibrio fra misure di controllo delle frontiere e di lotta al terrorismo e tutela del diritto fondamentale alla protezione dei dati personali.

Il trasferimento dei dati *Pnr* da e verso gli Stati Uniti

Il confronto con gli Stati Uniti si è aperto quando, in seguito agli eventi dell'11 settembre 2001, sono stati adottati leggi e regolamenti che impongono alle compagnie aeree di trasferire alle autorità doganali degli Usa i dati personali dei passeggeri e dell'equipaggio in volo da o verso il territorio statunitense. In particolare, le autorità americane hanno chiesto l'accesso elettronico ai dati contenuti nei sistemi di prenotazione e distribuzione delle compagnie aeree (cd. dati *Pnr-Passenger name record*), prevedendo in caso contrario controlli minuziosi e lunghi dei passeggeri e dei membri dell'equipaggio all'arrivo, nonché pesanti sanzioni pecuniarie, e disponendo persino la perdita dei diritti di atterraggio. Secondo il sistema proposto, un numero ingente di dati riguardante la totalità dei passeggeri dei voli transatlantici dovrebbe essere raccolto elettronicamente nei *database* delle compagnie aeree e dei sistemi di prenotazione, e poi analizzato e conservato per lunghi periodi dalle autorità statunitensi. Le autorità doganali potrebbero poi comunicarli ad altre autorità degli Usa o di altri Paesi al fine di valutare la pericolosità dei passeggeri, negando eventualmente l'imbarco ai soggetti ritenuti pericolosi (cd. sistema *"Capps II"*). Tutto ciò avverrebbe, però, in assenza di un quadro normativo negli Stati Uniti che garantisca ai passeggeri europei una tutela dei dati personali equivalente a quella assicurata dalla direttiva n. 95/46/CE.

La posizione del Gruppo dei garanti europei

Il Gruppo si è pronunciato nuovamente sul tema sia nel giugno 2003 (Parere 4/2003 WP 78 del 13 giugno 2003), sia nel gennaio 2004 (Parere 2/2004 WP 87 del 29 gennaio 2004), seguendo con attenzione gli sviluppi dei negoziati fra la Commissione europea e le autorità statunitensi e cercando di fornire elementi utili alla configurazione di meccanismi di trasferimento compatibili con il diritto alla protezione dei dati personali. Le carenze di tutela, evidenziate già nel parere del giugno 2003, e le conseguenti perplessità sulla possibilità di considerare adeguata la protezione prevista per i dati personali dei passeggeri europei, sono state confermate nel parere del gennaio 2004, adottato al termine dei negoziati fra Commissione e Stati Uniti.

In tale occasione il Gruppo ha tenuto conto sia dell'ultima versione degli impegni statunitensi ("Dichiarazione d'intenti dell'Ufficio doganale e di protezione dei confini *(Cbp)* del Dipartimento per la sicurezza interna" del 12 gennaio 2004), sia della comunicazione della Commissione europea ("Trasferimento dei dati contenuti nel *Passenger name record*: un approccio globale dell'Ue" COM(2003) 826 *final* del 16 dicembre 2003). In quest'ultimo documento, la Commissione manifesta l'intenzione di associare alla decisione sull'adeguatezza un accordo internazionale bilaterale che autorizzerebbe le compagnie aeree a considerare la richiesta degli Stati Uniti un obbligo di legge, imponendo nel contempo agli Usa di garantire ai cittadini europei l'esercizio dei propri diritti.

Nel sottolineare come anche nella lotta contro il terrorismo occorra tutelare le libertà individuali e i diritti fondamentali, compresi il rispetto della vita privata e la protezione dei dati, il Gruppo ha ribadito che il sistema deve rispettare almeno i principi fondamentali stabiliti dalla direttiva europea, ossia:

- principio di finalità. I dati del *Pnr* devono essere utilizzati soltanto per contrastare il terrorismo ed altri specifici reati connessi al terrorismo; inoltre, devono essere specificati chiaramente i soggetti ai quali i dati possono essere comunicati e non deve essere ammessa l'utilizzazione dei dati in rapporto ad altri sistemi, come ad esempio il *Capps II*;

- principio di proporzionalità. Devono essere trasferiti solo i dati necessari per le finalità indicate, evitando la raccolta di informazioni eccessive o non pertinenti;

- conservazione per un periodo di tempo limitato;

- divieto di trattare dati sensibili;

- esercizio dei diritti degli interessati. I passeggeri devono ricevere informazioni chiare e accurate su chi tratterà i loro dati e sugli scopi del trattamento, nonché sulle modalità per l'esercizio dei diritti riconosciuti dalla direttiva n. 95/46/CE e dalle leggi nazionali (accesso, rettifica, ecc.). Restano perplessità sui poteri del *Chief Privacy Officer* creato presso il *Department of Homeland Security*, anche alla luce dei problemi sul grado di vincolatività giuridica degli "impegni" assunti dall'Amministrazione degli Stati Uniti.

La posizione del Parlamento europeo

L'inadeguatezza dell'attuale configurazione del sistema di trasferimento dei cd. dati *Pnr* verso gli Usa è stata sostenuta dal Parlamento europeo che ha approvato una serie di risoluzioni in cui, nell'invitare la Commissione europea a definire un quadro giuridico chiaro per il trasferimento dei dati dei passeggeri verso gli Stati Uniti, ha rilevato varie lacune nelle garanzie offerte dal sistema statunitense e nella soluzione proposta dalla Commissione. Il Parlamento europeo ritiene pertanto che, per tutelare il diritto alla protezione dei dati personali sancito dall'art. 8 della Carta dei diritti fondamentali dell'Ue, sia necessario un accordo internazionale, possibilmente a carattere multilaterale, in cui chiarire il ruolo svolto dalle compagnie aeree e le garanzie offerte ai passeggeri.

Da ultimo il Parlamento europeo, con un'apposita risoluzione, ha censurato la

soluzione proposta della Commissione europea, invitando quest'ultima a ritirare il progetto di decisione sul trasferimento dei dati personali dei passeggeri aerei negli Stati Uniti e riservandosi il diritto di adire la Corte di giustizia per verificare la legalità dell'accordo raggiunto. Ciò in quanto gli impegni (cd. *undertakings*) assunti dall'Amministrazione statunitense sono stati giudicati una base giuridica inadeguata per la decisione della Commissione europea (*Comunicato stampa* 31 marzo 2004).

L'opportunità di un negoziato multilaterale, già evidenziata dal Gruppo nei propri pareri, si desume anche dalle richieste di trasferimento dei dati dei passeggeri recentemente formulate dalle autorità doganali canadesi ed australiane, oltre che da quanto sta emergendo in relazione a Paesi quali il Sudafrica e la Corea del Sud. Il Gruppo, in proposito, ha constatato che l'obiettivo di prevenire il terrorismo può essere efficacemente perseguito anche attraverso sistemi più rispettosi del diritto alla protezione dei dati personali dei passeggeri.

Così, un approccio certamente più equilibrato caratterizza il sistema australiano, rispetto al quale il Gruppo ha espresso un parere sostanzialmente favorevole, pur se condizionato ad alcune modifiche e miglioramenti (Parere 1/2004 WP 85 del 16 gennaio 2004). Tale sistema prevede, infatti, la trasmissione di un numero più limitato di dati personali. Inoltre, le finalità della raccolta sono circoscritte alla prevenzione del terrorismo e dei reati connessi, non è prevista la conservazione sistematica dei dati raccolti ed i diritti dei passeggeri sono garantiti da un quadro normativo ed istituzionale più conforme alle esigenze di tutela della vita privata.

Per quanto riguarda il Canada, il Gruppo ha adottato un ulteriore parere (Parere 3/2004 WP 88 del 11 febbraio 2004) in cui si evidenziano le questioni da risolvere e le modifiche da apportare al sistema canadese prima che possa essere approvata una pronuncia di adeguatezza da parte della Commissione europea.

La questione dell'utilizzazione dei dati dei passeggeri ad opera delle autorità di frontiera continua ad occupare un ruolo di primo piano non solo nell'agenda del Gruppo e delle istituzioni comunitarie, ma anche di altri organismi internazionali, quali l'Ocse e l'Icao, che più di recente hanno inteso contribuire allo sviluppo di un approccio globale a tale tematica (cfr. *infra*, parag. 41.2.).

37 Videosorveglianza

Il parere del Gruppo dei garanti europei

Il Gruppo dei garanti europei, nel parere n. 4/2004 (WP 89 dell'11 febbraio 2004), ha fornito specifiche indicazioni in materia di videosorveglianza e protezione dei dati personali, con l'obiettivo di fissare regole e garanzie comuni sull'installazione di telecamere, anche in vista di eventuali interventi legislativi in materia. Il parere, adottato su particolare impulso della delegazione italiana, contiene un "decalogo" sulle cautele ed i principi da osservare in materia di videosorveglianza, che si applicano anche ai trattamenti che non sono soggetti espressamente alle disposizioni della direttiva europea (ad esempio, trattamenti effettuati per scopi di sicurezza pub-

blica o per il perseguimento di reati, oppure effettuati da una persona fisica per scopi esclusivamente privati o familiari). I Garanti hanno tenuto conto in proposito anche di alcuni commenti pervenuti attraverso la consultazione pubblica conclusasi il 31 maggio 2003.

37.1. La videosorveglianza in ambito pubblico

L'incremento delle risorse finanziarie a disposizione degli enti locali derivanti da fonti comunitarie, dal Piano operativo nazionale sulla sicurezza e dalle leggi regionali tese a finanziare gli investimenti per promuovere legalità e sicurezza sociale ha probabilmente contribuito a determinare un incremento nell'utilizzo di sistemi di rilevazione di immagini in ambito pubblico.

Ancora numerosi sono stati i reclami e le segnalazioni pervenuti al Garante in merito a possibili violazioni delle norme sulla protezione dei dati personali derivanti dall'installazione di sistemi di videocontrollo ad opera, in particolare, di amministrazioni locali, attivati per finalità di sicurezza urbana, tutela del patrimonio, monitoraggio del traffico, asserite competenze in tema di prevenzione e repressione dei reati, disciplina dei rifiuti urbani. Numerosi sono stati pure i reclami e le segnalazioni nei confronti di impianti installati dagli esercenti attività commerciali o artigianali per ridurre il "rischio criminalità".

Parallelamente, sono stati posti al Garante moltissimi quesiti sul tema da parte di soggetti pubblici titolari del trattamento (enti locali, aziende sanitarie locali, istituti scolastici e prefetture).

Il Garante ha ricordato in primo luogo che l'installazione di sistemi di videosorveglianza non è subordinata ad una formale autorizzazione preliminare. Non è quindi stabilito alcun termine decorso il quale i progetti sottoposti all'Autorità dai titolari possano ritenersi conformi alla normativa sulla protezione dei dati personali o comunque autorizzati dal Garante, poiché al riguardo non è previsto il formarsi del cd. silenzio-assenso. Ciò, tenuto oltretutto conto che i progetti trasmessi all'Autorità spesso non descrivono tutte le caratteristiche che permetterebbero di verificare l'applicazione del principio di proporzionalità nei singoli aspetti del trattamento.

Già in passato, con il provvedimento generale del 29 novembre 2000 (cd. decalogo sulla videosorveglianza), l'Autorità aveva fornito alcune prime indicazioni per garantire un equo contemperamento tra le esigenze di sicurezza ed il rispetto della normativa sulla protezione dei dati personali nella rilevazione di immagini e suoni.

Le prescrizioni, gli accertamenti e le garanzie indicate in tale documento dovevano essere necessariamente aggiornate, in ragione dell'evoluzione delle tecnologie disponibili, dei nuovi strumenti giuridici elaborati in sede comunitaria ed internazionale e del nuovo Codice.

Il Garante ha perciò portato a compimento un nuovo procedimento, adottando nell'aprile 2004 un ulteriore provvedimento generale per individuare principi e cautele più specifici da rispettare in materia di videosorveglianza a pena di illiceità del trattamento, in vista del relativo codice deontologico.

L'art. 134 del d.lg. n. 196/2003 impegna infatti l'Autorità a definire a breve i lavori preparatori di un apposito codice deontologico per disciplinare il trattamento dei dati personali effettuato con strumenti automatizzati di rilevazione di immagini.

Nel merito delle questioni analizzate dall'Autorità nel 2003, va tra l'altro evidenziato il quesito formulato da un'agenzia investigativa sulla possibilità di installare telecamere in luoghi pubblici in connessione con il mandato ricevuto da un comune e finalizzato alla raccolta di prove di eventuali atti di vandalismo, danneggiamenti o altri atti criminosi, affinché si potessero perseguire penalmente e civilmente i relativi autori. In proposito, l'Autorità ha rilevato la mancanza del presupposto della proporzionalità nell'uso dello strumento rispetto alla finalità perseguita. Si è pure notato che l'ente pubblico committente (un comune) era privo di funzioni istituzionali in materia di prevenzione ed accertamento dei reati. L'adozione di un sistema di videosorveglianza avrebbe potuto giustificarsi solo in presenza di una comprovata inidoneità di altri sistemi o cautele (impianti di allarme, specifica vigilanza, ecc.) e con un ruolo ben diverso del titolare del trattamento, ovvero con l'attivazione delle forze di polizia.

Il Garante è intervenuto a richiesta affinché la realizzazione di un "sistema integrato di sicurezza territoriale" presso il quartiere Eur di Roma avvenga in piena conformità a quanto previsto dalla normativa sulla protezione dei dati personali e, in particolare, in stretto ossequio al principio di proporzionalità tra mezzi impiegati e scopi perseguiti (che si specifica nei principi di pertinenza e non eccedenza) e nel rispetto delle competenze degli organi coinvolti. Sotto questo aspetto, saranno perciò oggetto di ulteriore e preventivo esame le modalità di registrazione delle immagini, il tempo della loro conservazione, nonché la predisposizione di un'adeguata informativa alla cittadinanza.

37.2. La videosorveglianza nel settore privato

Anche nel settore privato l'utilizzo di impianti di videosorveglianza ha dato luogo, nel 2003, a frequenti interventi del Garante, a conferma della progressiva diffusione del fenomeno e della crescente attenzione e sensibilità dei cittadini al riguardo.

Nei numerosi casi analizzati, in attesa della definizione del codice di deontologia previsto dall'art. 134 del d.lg. n. 196/2003, sono stati ribaditi i principi già affermati nel provvedimento generale del 29 novembre 2000.

Videosorveglianza per fini di sicurezza individuale

Diverse sono state le istanze riguardanti l'installazione di impianti per finalità di sicurezza in ambito condominiale e in spazi antistanti le porte d'ingresso ad abitazioni private. Al riguardo, fermo restando il divieto sanzionato penalmente di interferire illecitamente nella vita privata altrui, si è nuovamente constatata l'inapplicabilità della vigente normativa sulla protezione dei dati personali ai trattamenti di dati effettuati per fini esclusivamente personali (art. 5, comma 3, d.lg. n. 196/2003): tuttavia, si è rilevato che questa esclusione per le apparecchiature di videosorveglianza installate al solo fine della sicurezza individuale non riguarda quelle attivate da condomini o più gruppi familiari e presuppone, comunque, che le immagini registrate non siano oggetto di successiva comunicazione sistematica o diffusione (*Provv.* 22 dicembre 2003).

Nei casi in cui la legge non sia applicabile perché ad esempio il sistema è attivato da un solo condomino che non registra i dati, ciò non comporta che i terzi siano

privati di garanzie in sede civile e penale. A parte la possibilità di ottenere tutela sulla base dell'art. 615-*bis* c.p., i terzi devono essere comunque salvaguardati nei loro diritti (riservatezza, tranquillità individuale) attraverso la delimitazione dell'angolo visuale, in modo da non riprendere l'uscio altrui o da attivare indebite forme di controllo su aree comuni.

Varie segnalazioni e reclami hanno poi riguardato il trattamento di dati effettuato tramite sistemi di videosorveglianza più complessi, installati ad opera, ad esempio, di studi professionali, esercizi commerciali, società ed enti *no-profit*, per i quali si è reso necessario eseguire accertamenti *in loco* in collaborazione con la Guardia di finanza (per il protocollo d'intesa siglato dalle due istituzioni il 26 ottobre 2002, v. *Relazione* 2002).

In un caso, poi, di installazione da parte di una farmacia, a seguito di alcuni episodi criminosi, di apparecchiature di videosorveglianza a protezione dei dipendenti e delle cose custodite nei relativi locali, si è reso necessario richiamare il titolare ad una più scrupolosa osservanza dei principi del cd. decalogo.

In altre ipotesi sono state invece contestate sia l'omessa notificazione al Garante del trattamento effettuato mediante impianti di videosorveglianza installati dai titolari per motivi di protezione del patrimonio e delle persone, sia la mancata adozione di un'idonea informativa agli interessati circa la presenza di tali impianti. In questi casi è stato infatti accertato che la qualità delle immagini consentiva l'identificazione delle persone che entravano nel campo di visuale delle telecamere e che i relativi titolari avevano completamente disatteso gli obblighi vigenti in materia, soprattutto per quanto concerne l'omessa informativa, comprovata dall'assenza di avvisi o cartelli recanti le indicazioni prescritte dalla normativa.

Altri procedimenti, scaturiti da reclami proposti da organismi sindacali aziendali (Rsa o Rsu) di diverse società avverso l'installazione di sistemi di videosorveglianza potenzialmente configurabili come strumenti di controllo a distanza dell'attività dei lavoratori, sono sfociati anch'essi nel richiamo al rispetto delle prescrizioni di cui all'art. 4 della legge n. 300/1970 (la cui vigenza è fatta salva dal d.lg. n. 196/2003).

Videosorveglianza sui treni

Di particolare interesse è risultato inoltre un progetto sperimentale di Trenitalia S.p.A. per installare sistemi di videosorveglianza su taluni vagoni di treni che transitano su specifiche tratte ferroviarie oggetto di ripetuti atti vandalici e di episodi di microcriminalità a danno dei passeggeri. Al riguardo la società ha dichiarato di aver già adottato taluni primi accorgimenti per la protezione dei dati, come ad esempio l'effettuazione delle riprese con modalità volte ad escludere sia un avvicinamento dell'immagine sia (per quanto riguarda le carrozze–cuccette) la ripresa degli scompartimenti dei passeggeri, nonché la memorizzazione delle immagini riprese in forma criptata e la predisposizione di un'informativa agli interessati.

Dopo un approfondito esame, l'Autorità ha richiamato l'attenzione di Trenitalia S.p.A. sui seguenti punti: necessità di individuare con precisione e nell'ambito di una ristretta cerchia di persone i responsabili e gli incaricati del trattamento; riduzione al minimo, ove tecnicamente possibile, dei tempi di conservazione giornaliera delle immagini prima della loro cancellazione; adozione di idonee misure di sicurezza dei sistemi e dei dati raccolti. Il Garante ha inoltre chiesto di conoscere, entro il mese di giugno 2004, l'esito della prima sperimentazione del progetto e lo stato di attuazione delle misure di protezione dei dati.

38 Rilevazioni biometriche

I dati biometrici recano informazioni particolarmente delicate ed il loro uso, se, da un lato può svolgere un ruolo utile nella previsione di misure di sicurezza per l'accesso a dati, apparecchiature e sistemi, riducendo il ricorso ad altri dati personali più direttamente identificativi quali nome, indirizzo o domicilio, dall'altro, può comportare gravissimi rischi legati all'uso indebito o indiscriminato di informazioni desunte da connotati particolari quali le impronte digitali lasciate dalla persona interessata.

La posizione dei garanti europei

La diffusione crescente dei sistemi biometrici ha spinto il Gruppo dei garanti europei ad adottare uno specifico documento di lavoro sul tema (WP 80 del 1° agosto 2003).

Secondo il Gruppo, l'impiego di tecniche biometriche è ammissibile solo se realmente proporzionato agli scopi che si vogliono raggiungere e se non comporta di regola la creazione di archivi centralizzati e l'utilizzazione di informazioni desunte da "tracce fisiche" (come le impronte digitali) che una persona può lasciare anche senza rendersene conto. I garanti si sono riservati di tornare sul tema in futuro per far sì che le imprese, le pubbliche amministrazioni e i soggetti interessati all'impiego di sistemi biometrici sviluppino dispositivi realmente rispettosi della *privacy*; in particolare, il Gruppo ha richiamato l'attenzione sull'opportunità di redigere anche appositi codici deontologici che fissino i criteri da seguire nello sviluppo e nell'utilizzo di sistemi biometrici.

Il Wpisp

Anche il *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse ha rivolto particolare attenzione al tema delle tecnologie biometriche, in considerazione del notevole interesse che tali tecnologie stanno assumendo in svariati ambiti, quali il settore bancario, l'istruzione, i servizi pubblici, la sicurezza dei viaggi ed il controllo dell'immigrazione. Il gruppo, coadiuvato da consulenti esperti in materia di *privacy*, ha pertanto elaborato un documento che, dopo un'introduzione generale in cui vengono esaminate le differenti tecnologie biometriche, analizza le diverse possibili configurazioni e funzionalità dei sistemi biometrici, evidenziandone le implicazioni in materia di protezione dei dati e sicurezza dell'informazione.

38.1. Dati biometrici: gli interventi del Garante

In considerazione dei rischi connessi all'utilizzo di sistemi biometrici, l'Autorità ha potenziato la propria attività di verifica e di vigilanza in tale settore. Attenzione particolare è stata dedicata ad esempio alla possibilità di installare questi sistemi a fini di controllo degli accessi ai luoghi di lavoro o a servizi di mensa universitaria.

Tramite tali verifiche, il Garante intende accertare se l'uso di un sistema così invasivo, come quello di rilevazione delle impronte digitali, sia effettivamente e obiettivamente proporzionato rispetto alle finalità che si vogliono perseguire.

Le pubbliche amministrazioni nei cui confronti sono stati avviati accertamenti, sono state chiamate a documentare le ragioni dell'inidoneità di altri sistemi o procedure da cui deriverebbero minori pericoli o rischi per i diritti e le libertà fonda-

mentali degli interessati, nonché le finalità perseguite con l'impiego di tali sistemi di rilevazione.

Inoltre, è stato chiesto di indicare le modalità di concreta rilevazione e/o registrazione dei dati biometrici ed il successivo confronto delle impronte digitali eventualmente registrate con quelle rilevate dai lettori ottici. Ancora, i destinatari degli accertamenti sono stati invitati a specificare i tempi di conservazione, le misure di sicurezza adottate e le modalità di consultazione dei dati da parte dei soggetti autorizzati.

Tra gli accertamenti effettuati va in particolare evidenziato quello nei confronti di un ente regionale per il diritto allo studio universitario che, secondo notizie di stampa, intendeva bandire una gara di appalto per 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 (ad esempio, studenti vincitori di borse di studio o in particolari condizioni di reddito). A seguito dell'intervento del Garante, l'ente ha comunicato la rinuncia a realizzare il progetto in quanto non conforme al principio di proporzionalità tra i mezzi impiegati e le finalità di controllo della spesa perseguite.

Il progetto *S-Travel*

Con riferimento all'utilizzo di dati biometrici da parte di operatori privati, merita di essere poi ricordato l'esame di un progetto pilota, curato da un gruppo di organizzazioni e società operanti a livello internazionale (cd. *S-Travel Consortium*).

Attraverso tale progetto si intendeva avviare, presso gli aeroporti di Atene e di Milano Malpensa, la sperimentazione dell'uso di tecniche di autenticazione biometrica (impronte digitali e/o immagine dell'iride) nel settore del trasporto aereo, con particolare riguardo alle operazioni di *check-in* e di imbarco. Il progetto, seguito in Italia da Alitalia-Linee Aeree Italiane S.p.A., avrebbe coinvolto, in una prima fase, i dipendenti Alitalia e avrebbe dovuto essere esteso in una seconda fase ai passeggeri abituali della medesima compagnia che vi avessero aderito spontaneamente.

Dopo un primo contatto con tale compagnia, il Garante ha richiamato l'attenzione sulle cautele imposte dalla normativa comunitaria e nazionale in materia, ed in particolare sull'opportunità di un formale interpello al Garante stesso (ai sensi dell'art. 24-*bis*, legge n. 675/1996; v. ora, art. 17, d.lg. n. 196/2003) per permettergli di effettuare gli approfondimenti del caso e di prescrivere le necessarie garanzie, anche in vista dell'ipotizzata estensione della sperimentazione ai passeggeri abituali.

Il progetto poneva, infatti, delicati problemi in merito al rispetto dei principi di necessità e proporzionalità del trattamento, nonché di pertinenza e non eccedenza dei dati. L'utilizzo di tecniche di sperimentazione biometriche di riconoscimento rispondeva solo in parte al perseguimento dell'obiettivo di rafforzamento della sicurezza nei controlli aeroportuali, mirando anche alla semplificazione degli attuali adempimenti ed all'accelerazione del flusso dei passeggeri negli aeroporti.

La raccolta di dati biometrici relativi sia alle impronte digitali, sia all'immagine dell'iride di entrambi gli occhi è risultata eccedente e sproporzionata rispetto alle finalità del trattamento anche all'Autorità greca per la protezione dei dati personali, la quale, nel novembre 2003, è intervenuta bloccando lo sviluppo del progetto.

Dopo un ulteriore incontro con l'Ufficio del Garante nel quale sono stati illustrati questi punti problematici, il Consorzio e Alitalia non hanno fornito ulteriori notizie circa l'intenzione di avviare in Italia la sperimentazione.

Rilevazioni biometriche in banca

Nel corso dell'anno sono inoltre pervenute all'Ufficio numerose richieste da parte di cittadini relative all'installazione, effettuata da alcune banche, di sistemi di rilevazione biometrica per l'accesso alle filiali. In proposito è stato ribadito l'orientamento già espresso dall'Autorità in precedenza: si è così confermato, anzitutto, che l'accesso con tali modalità deve avvenire solo ed esclusivamente sulla base di un consenso realmente libero ed informato e prevedendo modalità di ingresso alternative agevoli e non lesive della dignità della persona, anche in caso di indisponibilità al rilascio dei propri dati biometrici. Si è poi ricordato che, per il principio di proporzionalità tra gli strumenti impiegati e le finalità perseguite, resta non consentito l'utilizzo indiscriminato di sistemi di rilevazione biometrica all'ingresso di banche a fronte di una generica esigenza di sicurezza.

Sono pervenute, altresì, talune segnalazioni circa l'impiego, da parte di alcune società, di tecniche di autenticazione biometrica (impronta palmare o facciale) per la rilevazione delle presenze del personale dipendente. Si tratta di ipotesi sulle quali il Garante sta concludendo accertamenti specifici, in considerazione del fatto che il trattamento di dati biometrici in tale ambito non risulta allo stato lecito in base ai principi di necessità e proporzionalità.

È necessario, ancora, ricordare la partecipazione del Garante al cd. Gruppo passaporto elettronico costituito presso il Ministero degli affari esteri al fine di affrontare i problemi connessi all'inserimento di dati biometrici nei passaporti. L'Autorità ha fatto presente costantemente l'esigenza di individuare un'adeguata base giuridica che consentisse l'inserimento dei dati biometrici nei passaporti, sottolineando, altresì, la necessità di rispettare comunque i principi di finalità, di pertinenza e di non eccedenza nel trattamento dei dati.

Per quanto riguarda, infine, l'attività consultiva svolta dall'Autorità su richiesta del Ministero dell'interno in merito al nuovo modello elettronico per i permessi di soggiorno, specifiche indicazioni sono state formulate relativamente alla necessità di un'adeguata base giuridica per l'utilizzo di dati biometrici, alle tecniche di registrazione dei dati (verificazione o autenticazione), nonché alla conservazione separata dei dati biometrici rispetto a quelli raccolti ai sensi del testo unico delle leggi di pubblica sicurezza per persone pericolose o sospette (cfr. sul punto anche *infra*, parag. 45.2.).

39 Attività di polizia

Anche nel 2003 sono pervenute a questa Autorità alcune segnalazioni, a volte presentate direttamente al Garante, ovvero a seguito di istanze di accesso rivolte al Dipartimento della pubblica sicurezza, con le quali gli interessati lamentano la registrazione, nel C.e.d. (Centro elaborazione dati) di tale Dipartimento, di dati inesatti, incompleti o non aggiornati, per lo più in riferimento a provvedimenti giudiziari o amministrativi adottati e non registrati (art. 10 legge n. 121/1981, modificato dall'art. 42 legge n. 675/1996 e, da ultimo, dall'art. 175, comma 3, d. lg. n. 196/2003).

Il C.e.d. del Dipartimento della pubblica sicurezza

L'Autorità aveva già sottolineato in passato (*Provv.* 17 gennaio 2002) che anche i trattamenti effettuati da organi o uffici di polizia concernenti dati memorizzati nel predetto C.e.d., ovvero trattati per finalità di prevenzione, accertamento o repressione dei reati, devono essere comunque effettuati nel rispetto dei principi di liceità, pertinenza e non eccedenza previsti dall'art. 9 della legge n. 675/1996 (ora, art. 11 d.lg. n. 196/2003). Si era poi richiamata l'attenzione degli uffici sulla necessità di verificare con cadenza periodica la rispondenza a tali principi dei dati trattati, apportando senza ritardo le modifiche richieste o necessarie e cancellando i dati detenuti, specie in ragione degli esiti processuali eventualmente documentati dagli interessati.

In linea con le indicazioni del Garante, questi profili hanno trovato ulteriore rafforzamento nel Codice.

Il d.lg. n. 196/2003 ha infatti previsto che il C.e.d. del Dipartimento della pubblica sicurezza debba assicurare in maniera più incisiva l'aggiornamento periodico, la pertinenza e la non eccedenza dei dati trattati anche attraverso interrogazioni del casellario giudiziale e di quello dei carichi pendenti del Ministero della giustizia o di altre banche di dati di forze di polizia, al fine di garantire la costante rispondenza delle informazioni registrate nel C.e.d. a quelle conservate in altri archivi (art. 54, comma 3, d.lg. n. 196/2003).

Analogamente, la verifica periodica del rispetto dei principi dettati dall'art. 11 del Codice è prevista come specifico obbligo per i singoli organi, uffici e comandi di polizia, i quali potranno avvalersi anche delle risultanze del C.e.d. (aggiornate come appena precisato) procedendo pure, in caso di trattamenti di dati effettuati con mezzi diversi da quelli elettronici, ad annotare o integrare i documenti cartacei che li contengono (art. 54, comma 4, d.lg. n. 196/2003).

L'importanza di queste garanzie è testimoniata anche dalla disposizione del Codice che demanda ad un regolamento governativo lo sviluppo di taluni principi applicabili ai trattamenti effettuati per finalità di polizia. In un regolamento previsto dovranno essere infatti contemplati, fra l'altro, appositi e più specifici termini di conservazione dei dati, nonché determinate modalità per il loro aggiornamento periodico, per la comunicazione degli aggiornamenti ad altri soggetti cui le informazioni sono state, eventualmente, comunicate in precedenza, e per la verifica della pertinenza dei dati rispetto alla specifica finalità perseguita (art. 57 d.lg. n. 196/2003).

Il Codice ha inoltre chiarito che la disciplina vigente in materia di accesso ai dati conservati nel C.e.d. (art. 10, commi 3, 4 e 5, legge n. 121/1981) si applica anche

ai dati trattati da organi o uffici di polizia con l'ausilio di strumenti elettronici, nonché a quelli –già espressamente considerati in passato– destinati a confluire nel C.e.d. (art. 56 d.lg. n. 196/2003).

Particolare attenzione dovrà essere prestata ai trattamenti di dati che presentano maggiori rischi di danno all'interessato (trattamenti riferiti a dati genetici, biometrici o effettuati mediante tecniche basate su dati relativi all'ubicazione) per i quali l'Autorità intende individuare, anche su comunicazione degli organi interessati, particolari misure ed accorgimenti a garanzia dell'interessato (artt. 55 e 17 d.lg. n. 196/2003). L'Autorità ha già segnalato la necessità di determinare tali misure, anche in conformità alle indicazioni che potranno pervenire dalle stesse amministrazioni interessate, in relazione alla raccolta dei rilievi dattiloscopici effettuata in occasione del rilascio o del rinnovo del permesso di soggiorno agli stranieri ed all'eventuale inserimento dei dati biometrici nel documento di soggiorno elettronico.

L'Autorità è, poi, intervenuta nuovamente sulla diffusione da parte di organi di polizia di immagini e, specialmente, di foto segnaletiche di persone coinvolte in attività di polizia, in relazione ad una recente vicenda giudiziaria, che ha coinvolto anche alcuni personaggi del mondo dello spettacolo.

In merito a tale caso, già ricordato in un'altra parte della *Relazione* (cfr. parag. 15.2.), il Garante ha rilevato che la diffusione di immagini di persone coinvolte in indagini o altri accertamenti è consentita agli organi di polizia solo per finalità di giustizia o di polizia e comunque nel rispetto della dignità della persona arrestata o altrimenti detenuta.

40 Problemi applicativi e possibili sviluppi del sistema di informazione Schengen

Il Sistema di informazione Schengen (su cui, v. pure *infra*, parag. 49.) è assoggettato ad un'attività di verifica e controllo del suo funzionamento da parte dell'Autorità comune di controllo (Acc), alla quale compete vigilare sull'applicazione della Convenzione di Schengen. Nel biennio 2002-2003 tale Autorità è stata presieduta dal segretario generale del Garante, che aveva già ricoperto la carica di vice presidente nel precedente biennio.

Il sesto Rapporto dell'Acc

Nel dicembre 2003 l'Autorità comune ha approvato il sesto Rapporto, in cui sono evidenziate le attività intraprese per una nuova campagna di informazione nei confronti dei cittadini, per l'apertura di un sito *web* della stessa Autorità comune *(http://www.schengen-jsa.dataprotection.org)* e per l'attuazione di una *newsletter*.

Il Rapporto è dedicato, in particolare, al potenziamento degli strumenti di indagine attraverso le modifiche proposte al sistema informativo attuale. Si tratta del cd. Sis II, che prevede un significativo ampliamento delle categorie di informazioni registrabili nel sistema, il possibile inserimento di dati biometrici e la modifica di alcuni meccanismi di accesso e utilizzazione dei dati.

Il Rapporto sottolinea i vari sforzi compiuti dall'Autorità di controllo per far sì che tali modifiche siano pienamente conformi alla Convenzione di applicazione dell'Accordo di Schengen. In particolare, nel rispondere alle sollecitazioni di alcuni Stati membri rispetto agli sviluppi del Sis, si è evidenziato che le modifiche proposte (il Sis II dovrebbe essere attuato entro il 2006) comporterebbero un sostanziale mutamento della natura del sistema informativo. Dando a strutture come Europol o Eurojust la possibilità di accedere direttamente ai dati in esso contenuti, il Sis verrebbe utilizzato per scopi investigativi leciti senza, però, una revisione complessiva delle sue finalità: invece, la Convenzione del 1990 aveva previsto un'utilizzazione "più statica" del Sis, sostanzialmente per vietare l'ingresso nella cd. Area Schengen a soggetti segnalati come indesiderabili dalle competenti autorità nazionali e quale strumento utile per alcune misure cd. compensative.

Alle proposte di modifica del Sis l'Autorità comune ha dedicato nel biennio 2002-2003 diversi pareri, nei quali si è sottolineata la necessità di chiarire le nuove modalità di accesso di altri organismi (Europol, Eurojust) e si è ribadita l'inopportunità di inserire dati biometrici nel sistema (ad esempio, rilievi dattiloscopici) qualora tali dati non siano effettivamente indispensabili ai fini della specifica segnalazione. In merito alla proposta di inserire nel Sis le informazioni contenute nel cosiddetto "mandato di arresto europeo", l'Autorità comune, in un altro parere, ha sollecitato chiarimenti da parte del competente Comitato presso il Consiglio Ue, sottolineando che l'utilizzo del Sistema informativo Schengen quale veicolo di trasmissione delle informazioni contenute nel mandato di arresto europeo comporterebbe, ancora una volta, una modifica sostanziale della natura del Sis e dei suoi meccanismi di funzionamento, che va previamente discussa ed impostata organicamente sul piano normativo. Tra le diverse altre questioni riassunte nel Rapporto vi è quella dell'integrazione con altre banche dati.

Anche il Parlamento europeo ha sollecitato un riesame della questione, attraverso alcune audizioni pubbliche e seminari tenuti a Bruxelles, cui è stato chiamato a partecipare il segretario generale del Garante, in qualità di presidente dell'Autorità comune di controllo.

L'art. 96 della Convenzione Schengen

Sotto altro profilo, è stato avviato dall'Autorità comune uno studio per verificare le discrepanze eventualmente esistenti fra i vari Paesi nell'interpretazione ed applicazione dell'art. 96 della Convenzione Schengen, relativo alle segnalazioni ai fini della non ammissione sul territorio comune. In base ai criteri previsti da tale norma, nessuna segnalazione relativa ad una persona può essere inserita nel Sis se non in base ad una richiesta delle competenti autorità nazionali successiva all'adozione di un formale provvedimento (in genere di espulsione) delle autorità amministrative o giudiziarie concernente la medesima persona. Si è quindi avviata una verifica comune in tutti i Paesi, che dovrà portare entro breve termine anche in Italia a controlli almeno a campione sulle migliaia di interessati segnalati dal nostro Paese e sulle procedure di immissione di tali informazioni.

In merito, infine, ai tempi di conservazione delle segnalazioni inserite nel Sis, l'Autorità comune ha ritenuto, in un parere, che il termine di tre anni previsto dall'art. 112 della Convenzione Schengen per il riesame delle singole segnalazioni si applichi a tutti i dati personali contenuti nel Sis, indipendentemente dalle specifiche finalità (reperimento di una persona, divieto di ingresso nei confronti di tale persona).

41 Gli interventi dell'Ocse in materia di sicurezza

41.1. Attuazione delle linee-guida sulla sicurezza

Ad un anno dall'approvazione delle linee-guida sulla sicurezza, l'Ocse ha organizzato un seminario internazionale cui ha partecipato anche questa Autorità, per mettere a confronto le esperienze applicative nei singoli Paesi.

Le relazioni hanno evidenziato una notevole difformità nelle misure attuative a livello nazionale ed hanno fatto emergere la mancanza di chiarezza sui soggetti che dovrebbero promuovere l'attuazione dei principi contenuti nelle linee-guida. Tutti i partecipanti hanno affermato la necessità di incrementare lo scambio di *best practice* e di sviluppare metodologie capaci di valutare l'impatto delle misure di sicurezza informatica. Altre esigenze assai sentite sono quelle di sviluppare ulteriormente la condivisione delle informazioni *(Warning, Advice and Reporting WARP)* e di incoraggiare le industrie a conformare sempre di più i loro *hardware* e *software* alla sicurezza ed alla *privacy*, individuando soluzioni che evitino di far affidamento solo sui consumatori finali.

Particolare attenzione è stata rivolta anche alla necessità di promuovere politiche di istruzione e formazione per i Paesi non membri dell'Ocse, anche in ragione dell'interdipendenza crescente fra Paesi sviluppati e Paesi in via di sviluppo, che obbliga a pensare la sicurezza in termini "globali". È stata inoltre sottolineata la necessità di passare dal concetto di sicurezza a quelli di responsabilità e affidabilità.

La discussione si è conclusa con la decisione di creare un *Global Culture of Security Web Site (www.oecd.org/sti/cultureofsecurity)*, che possa costituire uno strumento di scambio di esperienze reciproche fra i Paesi membri e, allo stesso tempo, una fonte di informazione per i Paesi non membri.

41.2. Sicurezza dei viaggi internazionali **(Travel Security)**

Alla luce dei numerosi dibattiti non solo europei, l'Ocse ha deciso di rivolgere particolare attenzione a tale argomento, ritenendolo un importante terreno di confronto tra le rinnovate esigenze di sicurezza ed i principi di protezione dei dati personali.

Nel settembre del 2003, l'Ocse e l'Icao (Organizzazione internazionale dell'aviazione civile) hanno organizzato a Londra un incontro, cui ha partecipato anche questa Autorità, volto ad esaminare i tipi di controlli e di sistemi che potrebbero migliorare la sicurezza dei viaggi internazionali, garantendo al contempo un elevato grado di tutela dei dati personali.

L'esame dei metodi sottoposti alla discussione, tra i quali figurano l'inserimento di dati biometrici nei passaporti e la previsione di sistemi di trasmissione dei dati dei passeggeri, ha confermato che questa materia costituirà un elemento cruciale del dibattito anche futuro su sicurezza e *privacy*.

Per tali ragioni il *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse, avendo competenze in materia di sicurezza, *privacy* e biometria –i tre ele-

menti centrali della *travel security*– ha recentemente dato vita ad un gruppo di esperti che, unitamente a rappresentanti dell'Icao, si occuperà del tema. Il gruppo, basandosi sulle raccomandazioni dell'Icao e sulle linee guida dell'Ocse, avrà come compito principale l'elaborazione di indicazioni agli Stati membri sugli aspetti di sicurezza dell'informazione e di tutela della *privacy* nella raccolta e scambio dei dati relativi ai passeggeri che intraprendono viaggi internazionali. Di tale gruppo farà parte anche un rappresentante del Garante.

Le informazioni genetiche

42 I compiti e gli interventi del Garante

Con riferimento ai dati genetici, il Codice ha confermato il principio stabilito dalla disciplina previgente secondo cui il trattamento di queste informazioni, da chiunque effettuato, dovrà essere oggetto di un'apposita autorizzazione del Garante (art. 90).

Tale autorizzazione sarà rilasciata nel 2004 sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità. Nelle more di questa nuova ed apposita autorizzazione, che avrà carattere generale, i trattamenti di dati genetici possono essere allo stato iniziati o proseguiti osservando le prescrizioni contenute nell'autorizzazione n. 2/2002, come ad es. il divieto di comunicare le informazioni genetiche a terzi.

Sempre in tema di dati genetici, il Garante è intervenuto a seguito di una segnalazione proveniente dall'estero rispetto ad una vicenda che aveva avuto eco anche sulla stampa straniera. Il caso riguarda un'articolata ricerca genetica su popolazioni isolate in Alto Adige. L'Autorità, avvalendosi dell'esperienza acquisita a seguito di analoghi accertamenti svolti in merito a ricerche attivate in altre regioni, ha curato ispezioni *in loco*, ottenendo informazioni e documenti relativamente alle modalità di raccolta dei dati bio-genetici e all'osservanza delle garanzie a tutela della riservatezza degli interessati in materia di informativa e consenso.

Dal procedimento svolto con la collaborazione dei professionisti preposti alla ricerca è già scaturita, pur in presenza del rispetto di parte dei principi di legge, una denuncia di reato per violazione di norme in materia di misure di sicurezza e un connesso provvedimento di prescrizione di misure idonee ai sensi dell'art. 169 del Codice.

È poi attualmente allo studio dell'Autorità il trattamento di dati personali connesso alla realizzazione di *test* genetici. L'esame avviato dal Garante concerne i *test* finalizzati alla prevenzione, diagnosi o terapia di malattie genetiche, quelli di paternità e/o maternità utilizzati per scopi probatori in sede civile o penale, nonché quelli di tipo "informativo" o "confidenziale", basati cioè su una mera comparazione dei profili genetici ottenuti da due o più tracce biologiche anonime, al fine di fornire indicazioni sulla loro compatibilità genetica.

Procreazione assistita

Per quanto riguarda la materia della procreazione assistita, si è parlato in altra parte della *Relazione* dell'audizione del presidente del Garante nell'ambito dei lavori preparatori della legge n. 40/2004 (cfr. parag. 2.). Va aggiunto che l'Autorità è stata investita da numerosi interpelli e segnalazioni a proposito delle modalità inizialmente ipotizzate per attuare l'art. 17 di tale legge, nella parte in cui prevede che le strutture e i centri in cui si praticano tecniche di procreazione medicalmente assistita trasmettano al Ministero della salute *"un elenco contenente l'indicazione numerica degli embrioni prodotti … nonché, nel rispetto delle vigenti disposizioni sulla tutela della riservatezza dei dati personali, l'indicazione nominativa di coloro che hanno fatto ricorso alle tecniche medesime a seguito delle quali sono stati formati gli embrioni"*.

Di seguito alla prima circolare del Ministro della salute del 10 marzo 2004, l'Ufficio del Garante ha curato alcuni approfondimenti in collaborazione con il Ministero.

All'esito di tali approfondimenti, con nota ministeriale del successivo 25 marzo, si è ottenuta conferma che non si sarebbe più sollecitata una comunicazione nominativa di tutti gli interessati che avevano fatto ricorso alla procreazione assistita presso i centri, ma che, al contrario, si sarebbe proceduto alla sola richiesta di inviare al Ministero una serie di codici numerici indicanti il centro, la regione di riferimento e un numero sequenziale per ogni embrione congelato, in collegamento con i dati identificativi (che rimarranno in possesso dei soli centri). La vicenda ha trovato così un giusto punto di bilanciamento di cui il Governo ha anche dato atto nella successiva risposta ad alcuni atti di sindacato ispettivo in Parlamento.

43 Il documento di lavoro del Gruppo art. 29

Sul trattamento dei dati genetici deve essere ricordato, inoltre, il documento di lavoro adottato il 17 marzo 2004 dal Gruppo dei garanti europei costituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

L'inarrestabile progresso tecnologico nel settore della genetica ha indotto il Gruppo ad occuparsene, viste le sue ripercussioni nel campo della riservatezza. In particolare si è cercato di individuare i settori in cui il trattamento dei dati genetici determina maggiori preoccupazioni, considerando comunque la protezione dei dati genetici un presupposto indispensabile del principio di uguaglianza e del diritto alla salute.

Dopo aver fornito le definizioni di dato genetico ed elaborato il concetto di "gruppo biologico", in linea con quanto stabilito in materia dal Consiglio d'Europa e dall'Unesco, vengono descritti il campo di applicazione della direttiva n. 95/46/CE, nonché le caratteristiche che rendono unici questi dati e le finalità più rilevanti per le quali vengono trattati negli ordinamenti dei quindici Paesi membri (tra le quali l'assistenza sanitaria e la terapia medica, l'occupazione, le assicurazioni, la ricerca medica e scientifica e l'identificazione). In tutti questi casi è necessario raggiungere un approccio uniforme e un punto di vista condiviso, al fine di stabilire adeguate garanzie.

Qualsiasi trattamento di dati genetici non connesso alla salvaguardia della salute dell'interessato e alla ricerca scientifica può avvenire solo se previsto da una norma di legge conforme alla direttiva e, in particolare, al principio di finalità e proporzionalità. Ne discende il divieto di *screening* genetici generalizzati.

Nei settori dell'occupazione e delle assicurazioni il trattamento dovrebbe essere consentito solo in casi eccezionali e comunque previsti da norme di legge.