SENATO DELLA REPUBBLICA

XIV LEGISLATURA

Doc. CXXXVI
n. 4

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 2003)

(Articolo 31, comma 1, lettera n, *della legge 31 dicembre 1996, n. 675)*

Presentata dal Garante per la protezione dei dati personali

(RODOTÀ)

Comunicata alla Presidenza il 29 aprile 2004

ATTI PARLAMENTARI

XIV LEGISLATURA

Doc. **CXXXVI**
n. **4**

RELAZIONE

SULL'ATTIVITÀ SVOLTA DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

(Anno 2003)

(Articolo 31, comma 1, lettera n, della legge 31 dicembre 1996, n. 675)

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

INDICE

V – La privacy e le sfide del futuro

Reti di comunicazioni:

Il trasferimento di dati personali all'estero:

La sicurezza pubblica e privata:

Le informazioni genetiche:

ALLEGATI

Allegato A

Codici di deontologia

Allegato B

Misure di sicurezza

Allegato C

Elenco delle abbreviazioni

La presente Relazione è riferita al 2003 e contiene talune notizie già anticipate nella precedente Relazione, nonché alcune ulteriori informazioni, aggiornate al 24 aprile 2004, relative a sviluppi significativi che si è ritenuto opportuno menzionare.

art.	articolo
Bollettino	Bollettino del Garante per la protezione dei dati personali « *Cittadini e Società dell'Informazione* »
c.c.	codice civile
c.p.c.	codice di procedura civile
c.p.p.	codice di procedura penale
cd.	cosiddetto/a
cfr.	confronta
Cost.	Costituzione
d.l.	decreto legge
d.lg.	decreto legislativo
d.m.	decreto ministeriale
d.P.C.M.	decreto del Presidente del Consiglio dei ministri
d.P.R.	decreto del Presidente della Repubblica
G.U.	Gazzetta Ufficiale
l.	legge
lett.	lettera
n.	numero
p.	pagina
Pa	Pubblica amministrazione
parag.	paragrafo
Provv.	provvedimento
Relazione	Relazione del Garante per la protezione dei dati personali
r.d.	regio decreto
reg.	regolamento
S.p.A.	società per azioni
T.U.	testo unico
u.s.	ultimo scorso
Ue	Unione europea
v.	vedi

Relazione2003

Discorso del Presidente **Stefano Rodotà**

Signor Presidente della Repubblica,

un anno, quello passato, in cui la corsa delle tecnologie si è fatta ancor più impetuosa, ma pure l'anno in cui Governo e Parlamento hanno messo a punto il Codice in materia di protezione dei dati personali, poi entrato in vigore il 1° gennaio 2004, che contiene strumenti che assicurano proprio l'adeguamento della disciplina giuridica ad una realtà perennemente mobile.

Il Codice, infatti, ha un impianto nel quale assume specifica rilevanza la trama dei principi, da adattare poi alla molteplicità delle situazioni concrete. Irrobustisce il sistema della protezione dei dati personali, ormai solidamente collocata nel quadro dei diritti fondamentali. Fa così crescere le garanzie per la libertà delle persone. Rappresenta il primo esempio, su scala internazionale, di riordino generale di una materia complessa e mutevole.

Un nuovo quadro di principi

L'innovazione sul piano dei principi si coglie fin dal primo articolo del Codice, che riproduce il primo comma dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea (ora presente anche nell'articolo 50 del Progetto di Trattato che istituisce una Costituzione per l'Europa): "Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Il trasferimento di questa norma nel sistema italiano rende non più proponibili interpretazioni riduttive della protezione dei dati personali, e stabilisce un legame solido tra ordinamento italiano e ordinamento europeo. E il legislatore ha voluto ulteriormente ribadire la sua volontà di considerare la protezione dei dati come un diritto fondamentale, nominandola esplicitamente nell'articolo 2 del Codice.

È stata così fatta una scelta impegnativa, che richiede coerenza. Le norme sulla protezione dei dati personali non sono certo incise sul bronzo, ma neppure possono essere considerate come pezzi di una leggina che può essere smontata appena i portatori di un interesse settoriale alzano la voce o al semplice annuncio di una possibile emergenza. Il Codice segna il passaggio da una situazione di frammentazione legislativa ad un sistema unitario. Ha dato vita ad un quadro di riferimento di medio periodo, che consente di seguire il cambiamento, ma al tempo stesso vuole offrire certezze. Se dovesse farsi strada la sensazione che si tratta di un testo manipolabile sotto la spinta dell'emozione o del piccolo interesse, diverrebbero labili le garanzie per i cittadini, sarebbero incentivati i comportamenti volti ad aggirare il Codice, verrebbero scoraggiate le iniziative volte ad adeguare alla nuova disciplina le strutture pubbliche e private, che esigono investimenti e non possono, quindi, essere assoggettate ad un regime di precarietà.

Inoltre, proprio perché ci troviamo in presenza di diritti fondamentali, non sono ammissibili cedimenti a logiche localistiche. Il Garante seguirà con attenzione la legislazione regionale, per evitare che venga incrinato il principio della parità di trattamento dei cittadini, indipendentemente dal luogo in cui si trovino a vivere.

Di tutto questo bisogna esser consapevoli perché il Codice è parte essenziale di un progetto più complessivo, fondato su riferimenti nazionali e sopranazionali, affidato anche ad una molteplicità di codici di deontologia e buona condotta che sviluppano i suoi principi in specifici settori. Questo è già avvenuto per l'attività giornalistica, la ricerca storica, la ricerca nell'ambito del sistema statistico nazionale. Si sono appena conclusi i lavori dei codici dedicati alle centrali rischi private ed al trattamento di dati statistici da parte di soggetti che non fanno parte del Sistan. Presto vedranno la luce i codici dedicati alle indagini investigative ed alla videosorveglianza, ai quali altri se ne aggiungeranno nel corso dell'anno, in particolare quelli

riguardanti Internet, i rapporti di lavoro, il *direct marketing*. Il nostro paese, dunque, si sta dotando di un significativo *corpus* legislativo sui rapporti tra l'organizzazione sociale e l'innovazione scientifica e tecnologica, terreno sul quale si misura ormai la capacità innovativa dei sistemi giuridici.

Proprio per rafforzare la trama dei principi, al fondamentale principio di dignità, e ai ben noti principi di finalità, pertinenza e proporzionalità si affiancano ora quelli di "semplificazione, armonizzazione ed efficacia" (art. 2.2 Codice) e di "necessità" (art. 3 Codice). Quest'ultimo merita una sottolineatura particolare. L'articolo 3 stabilisce che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità".

Si enuncia così una linea di politica del diritto particolarmente impegnativa, che mette anche in guardia contro pericolose derive tecnologiche. Si tratta di una indicazione importante, perché la protezione dei dati rischia ogni giorno d'essere compressa dalla crescente offerta sul mercato di tecnologie che rendono più agevole forme generalizzate di raccolta delle informazioni. Il principio di necessità diviene così un ineludibile *test* legislativo per valutare la legittimità delle raccolte di informazioni personali.

In ciò non è difficile scorgere la volontà di misurare l'accettabilità sociale e politica delle tecnologie anche dal punto di vista del rapporto tra mezzi e fini in una società democratica, come, peraltro, prescrive l'art. 8 della Convenzione europea dei diritti dell'uomo (1950), dove si subordina la possibilità di limitare la protezione della vita privata e familiare solo attraverso misure coerenti con il carattere "democratico" di una società. Il Codice rafforza il legame tra *privacy* e democrazia.

Il ricorso alle tecnologie e gli "allarmi" del Garante

Abbiamo ricordato, in passato, che non tutto ciò che è tecnologicamente possibile è anche socialmente desiderabile, eticamente accettabile, giuridicamente legittimo. Oggi dobbiamo aggiungere che le derive tecnologiche possono produrre gravi effetti distorsivi. Distorsioni nell'uso delle risorse quando, ad esempio, queste vengono investite in impianti di videosorveglianza privi di vera utilità per la sicurezza. Distorsioni nell'organizzazione degli interventi quando, ad esempio, ci si affida a grandi banche dati centralizzate, tecnicamente difficili da gestire, vulnerabili agli attacchi, accompagnate da affidamenti in *outsourcing* spesso inadeguati, soprattutto tali da distogliere l'attenzione dalla necessità di raccolte e di indagini mirate. Distorsioni nella percezione e nell'analisi della realtà quando, ad esempio, le raccolte di informazioni vengono adoperate per frettolose traduzioni di un fenomeno in termini di ordine pubblico, invece di indagarne le ragioni sociali e di avviare, quindi, politiche più adeguate.

Le regole di *privacy* divengono così anche fattore di efficienza, e si rivelano strumenti indispensabili per una analisi dei rapporti tra società e tecnologia. Una valutazione d'"impatto *privacy*" dovrebbe ormai accompagnare molti interventi legislativi ed organizzativi. Altrimenti, la corsa verso raccolte sempre più imponenti di dati personali non produce strumenti migliori di conoscenza della realtà, ma un assordante "rumore di fondo tecnologico" che può addirittura rendere più complessa l'azione pubblica. L'affidarsi cieco alle tecnologie, ritenendo che in esse risieda ormai la soluzione di ogni problema, può risolversi in una delega in bianco, con la politica che rischia di farsi espropriare dei suoi compiti di scelta e di decisione su gravi questioni sociali.

Il Garante, fin dalle sue prime relazioni, ha sempre indicato casi concreti in cui

i rapporti tra società e innovazioni scientifiche e tecnologiche si presentavano in forme particolarmente critiche. Sono quelli che, nelle cronache giornalistiche, vengono definiti gli "allarmi" del Garante. E che allarmi sono davvero, nel senso che non si tratta di grida senza fondamento, ma di segnalazioni precoci di dinamiche che, poi, rivelano tutta la loro portata. Videosorveglianza, conservazione di enormi volumi di traffico telefonico, rilevanza dei dati genetici, *spamming*, controlli capillari sulle persone: questi sono alcuni dei temi sui quali negli anni passati abbiamo richiamato l'attenzione e che, poi, si sono rivelati fenomeni socialmente pervasivi, con problemi ineludibili a livello interno ed internazionale.

Questo lavoro prospettico rimane essenziale, non solo per attrezzarsi a fronteggiare il futuro, ma anche per non cadere nella *routine* burocratica. Ma non sappiamo fino a quando il Garante potrà tener fede a questo impegno se continuerà la lenta riduzione delle sue risorse. Questo stillicidio non pregiudica soltanto l'efficienza: rischia di minare la nostra autonomia. Raccogliendo una indicazione contenuta nella relazione dell'anno scorso, la Camera dei deputati ha votato all'unanimità una mozione nella quale si sottolinea appunto la necessità di attribuire al Garante le risorse necessarie. Su questa base ci siamo rivolti al Governo e speriamo che, in attesa di una più attenta considerazione nella prossima legge finanziaria, alcuni interventi siano già possibili attingendo al fondo di riserva.

Il futuro è già tra noi – si usa dire. Per questo il Garante dedica la sua attenzione anche a novità apparentemente minori, ad innovazioni ancora d'incerta applicazione. Solo così, infatti, si può evitare d'essere colti in flagrante peccato di distrazione, intervenendo quando la forza delle cose rende più difficile regolare situazioni in parte già consolidate.

Il sistema delle telecomunicazioni è quello che più visibilmente incorpora il

futuro. Si trasforma, offre agli utenti grandi opportunità, ma crea anche nuove vulnerabilità individuali e sociali. Dopo aver adottato provvedimenti sui messaggi di posta elettronica non desiderati *(spamming)* e sui messaggini telefonici *(Sms)* promozionali, il Garante sta per intervenire in tre direzioni. Quella della televisione interattiva, dove il continuo flusso di informazioni dall'utente al fornitore del servizio può consentire controlli continui sulle abitudini delle persone, ricavandone profili personali e di gruppo ed esponendo i singoli al rischio di nuovi controlli, se viene consentito ad autorità pubbliche di accedere a questi dati. Quella delle videochiamate, che possono coinvolgere una molteplicità di soggetti e richiedono, quindi, regole precise sull'utilizzazione delle immagini. Quella, infine, di un rigoroso controllo del modo in cui i diritti dell'utente vengono rispettati nell'ambito della telefonia, dove riscontriamo inadempimenti riguardanti questioni alle quali i cittadini sono assai sensibili, come le chiamate di disturbo e l'identificazione della linea chiamante.

Etichette "intelligenti" e controlli sulle persone

Un anno fa sottolineavamo i problemi nascenti da tecniche di localizzazione che rendono possibile un controllo continuo delle persone, creando una sorta di guinzaglio elettronico. Su questa strada non ci si è fermati e, anzi, la tecnologia delle radiofrequenze *(Rfid)* ha portato alla creazione di "etichette intelligenti" che, sostituendo i codici a barre, permetteranno di seguire i prodotti nei loro spostamenti, creando così le condizioni per controllare anche chi ha acquistato ed usa quel prodotto.

Molti impieghi della *Rfid* sono sicuramente utili e benefici: migliore gestione delle merci, possibilità di rintracciare l'origine di prodotti particolarmente delicati (come i medicinali), rapidità di operazioni commerciali (lettura istantanea dei prezzi

di tutti gli oggetti posti nel carrello di un supermercato). Se, tuttavia, le etichette intelligenti non vengono disattivate nel momento in cui il prodotto passa nelle mani dell'acquirente, diventa reale il rischio di una sorveglianza generalizzata di persone e comportamenti.

Ma lo stesso corpo può essere tecnologicamente modificato, predisposto per essere seguito e localizzato permanentemente. Braccialetti elettronici sono stati proposti anche per controllare i bambini sulle spiagge. Ora la possibilità di inserire sotto la pelle un *chip*, contenente ad esempio informazioni sulla salute o tale da permettere in ogni momento la localizzazione di persone rapite, di criminali pericolosi, di detenuti in libertà provvisoria o più semplicemente l'identificazione di una persona, ha indotto una società americana a lanciare il servizio *VeriChip* con lo slogan *"Get chipped"*. Questa società ha poi presentato il servizio *VeriPay*, consistente sempre in un *chip* sotto la pelle, che dovrebbe prendere il posto di una comune carta di credito, rendendo così più sicuri e veloci i pagamenti. Il controllo diventa poi ancora più agevole se ci si affida alle etichette intelligenti, adoperandole per contrassegnare non solo prodotti, ma anche esseri viventi: oggi gli animali di un gregge, come già accade, in prospettiva anche le persone.

Siamo ormai di fronte alla concreta possibilità di vere e proprie modificazioni del corpo. Se, ad esempio, si considera la possibile sostituzione del braccialetto elettronico con le tecnologie *Rfid* per controllare i detenuti in regime di semilibertà o le persone agli arresti domiciliari, non assistiamo ad un innocente passaggio da una tecnologia all'altra. Per quanto odioso possa essere, il braccialetto non modifica il corpo. Ma quando si inserisce un *chip* o si applica una etichetta intelligente, l'integrità del corpo è violata, la dignità lesa, sì che l'impianto dovrebbe essere ritenuto illegittimo anche se la persona interessata abbia dato il suo consenso.

Si tratta, dunque, di stabilire quando la *Rfid* possa essere adoperata per raccogliere informazioni personali. Poiché la nuova tecnologia è in fase di decollo, il Garante interverrà nelle prossime settimane precisando le condizioni per il suo legittimo uso. Ferma restando l'inammissibilità di applicazioni dirette sul corpo, tutti i soggetti ai quali vengono trasferiti prodotti così "etichettati" dovranno ricevere una informazione adeguata ed essere messi nella condizione di ottenere prodotti per i quali sia stata disattivata la *Rfid* o di procedere direttamente alla disattivazione.

Tecniche biometriche e libertà del corpo

Se questi usi del corpo possono sembrarci meno vicini, e più controllabili, lo stesso non può dirsi per le tecniche biometriche. Per documenti di identificazione d'ogni tipo, dai passaporti alle semplici carte d'identità, si esige sempre più largamente che in essi siano inseriti dati biometrici, ritenuti indispensabili per assicurare la certezza dell'identificazione.

Si dà così rilevanza, in modo nuovo, al corpo, che diventa fonte diretta di informazioni, oggetto di un continuo *"data mining"*, davvero una miniera a cielo aperto dalla quale attingere dati ininterrottamente. Lo ripetiamo: il corpo in sé sta diventando una *password*. La fisicità prende il posto delle astratte parole chiave, sostituite da impronte digitali, geometria della mano o delle dita o dell'orecchio, iride, retina, tratti del volto, odori, voce, firma, uso di una tastiera, andatura, *Dna*.

L'insistenza sui dati biometrici si è fatta particolarmente martellante per la loro associazione con le esigenze di sicurezza. Ma qui valgono le considerazioni sulle derive tecnologiche e sulla necessità di riferirsi sempre ai principi del Codice.

Il principio di necessità impone di accertare se la finalità perseguita non possa essere realizzata utilizzando dati che non coinvolgano il corpo. Il principio di proporzionalità esige una considerazione rigorosa della legittimità di raccolte generalizzate rispetto a raccolte mirate, di una conservazione centralizzata o decentrata dei dati raccolti. Il principio di dignità fa emergere la necessità di rispettare l'autonomia delle persone di fronte a particolari raccolte di dati (quelle riguardanti la salute, in primo luogo).

Non ci si può limitare ad una generica analisi costi-benefici. Quando si incide su libertà personale, integrità e dignità, non si può agire come se il bisogno di sicurezza o il fine dell'efficienza potessero prevalere su ogni altra considerazione. Difendendo la persona e il suo corpo si difendono valori fondamentali dei sistemi democratici, che non possono essere limitati o sacrificati senza avviare pericolose derive di tipo totalitario.

L'utilizzazione dei dati biometrici offre certamente nuove forme di sicurezza, semplificazioni delle attività quotidiane. Aumenta la certezza delle identificazioni e delle verifiche dell'identità. Può facilitare attività investigative.

Ma non ci si può limitare a registrare il contributo tecnico della biometria alle attività di identificazione e verifica. È indispensabile assicurarsi della loro accuratezza, poiché le tecniche utilizzate possono determinare percentuali elevate di falsi positivi e negativi. Questo accade per il carattere ancora sperimentale di alcune tecniche o dipende dalle particolari condizioni in cui vengono impiegate (come le condizioni di luce o l'angolo di ripresa per l'identificazione facciale).

Il ricorso ai dati biometrici, quindi, esige un approccio tecnicamente prudente, senza gli entusiasmi e le definitive certezze che spesso vengono proclamate soprat-

tutto da chi ha interesse a collocare sul mercato le relative tecnologie. In un documento dell'Ocse del marzo di quest'anno *(Biometric-based Technologies)* si osserva che una rassegna delle informazioni disponibili dà "al lettore la sensazione che la biometria non sia ancora 'pronta per la prima serata'". Questo vuol dire che, mentre queste tecnologie sembrano funzionare adeguatamente in impieghi ridotti e limitati, "la loro accuratezza, affidabilità e adeguatezza non sono ancora sufficientemente raffinate per una loro utilizzazione in sistemi di identificazione personale su larga scala".

Da questo tipo di analisi si traggono due indicazioni. Una riguarda il periodo breve-medio, e consiglia una valutazione rigorosa dell'uso dei dati biometrici con riferimento alla loro affidabilità: si tratta, evidentemente, di indicazioni destinate a variare a seguito dei perfezionamenti tecnici. L'altra ha carattere generale e si riferisce al *test* di compatibilità con i valori di libertà e democrazia al quale anche le utilizzazioni dei dati biometrici devono essere sottoposte, secondo le indicazioni desumibili anche da un parere del Gruppo europeo dei garanti.

Si sono già ricordati i principi di necessità e proporzionalità, rilevanti anche per valutare la legittimità di raccolte di dati riferiti ad un gran numero di persone. Le raccolte generalizzate, infatti, soprattutto se giustificate genericamente con ragioni di sicurezza, modificano la percezione sociale di tali raccolte e trasformano tutti i cittadini in potenziali sospetti. Fanno crescere la vulnerabilità sociale, essendo difficile eliminare il rischio di abusi o difendere le grandi banche dati da violazioni operate anche da gruppi terroristici o criminali. Diversi studi propongono in modo persuasivo argomenti sull'inefficienza e sui limiti delle grandi raccolte d'informazioni.

Il ricorso massiccio alle soluzioni basate sulla biometria può essere presentato e percepito come una panacea tecnologica, sì che l'opinione pubblica tende a

sopravvalutare la loro accuratezza, associando impropriamente tali tecnologie con una protezione assoluta contro il terrorismo. A questa falsa certezza può associarsi una crescente "mitridatizzazione" sociale. Il diffondersi del ricorso alla biometria oltre le situazioni di stretta necessità rischia di far progressivamente perdere ai cittadini la sensibilità necessaria per avvertire i rischi per la loro libertà personale. La società può essere anestetizzata attraverso la progressiva cancellazione delle percezioni legate alla perdita del controllo esclusivo sul proprio corpo.

Cogliamo un'inquietudine sociale di fronte ad invasive forme di appropriazione del corpo attraverso i dati sulla salute. Possono farlo soggetti pubblici: per questo abbiamo segnalato l'improprietà e la pericolosità di raccolte centralizzate di dati sulla salute per finalità di controllo sulla spesa sanitaria e siamo intervenuti per evitare improprie comunicazioni sull'identità delle persone in materia di procreazione assistita. Possono farlo soggetti privati: per questo continuiamo a controllare l'offerta su Internet di *test* genetici, e in generale le questioni della genetica, alle quali ha recentemente dedicato un parere il Gruppo europeo dei garanti.

Trasformazioni della persona

Davanti a noi sono mutamenti che toccano l'antropologia stessa delle persone. Siamo di fronte a slittamenti progressivi: dalla persona "scrutata" attraverso la videosorveglianza e le tecniche biometriche si può passare ad una persona "modificata" dall'inserimento di *chip* ed etichette "intelligenti", in un contesto che sempre più nettamente ci mostra come stiamo diventando *"networked persons"*, persone perennemente in rete, via via configurate in modo da emettere e ricevere impulsi che consentono di rintracciare e ricostruire movimenti, abitudini, contatti, modificando così senso e contenuti dell'autonomia delle persone.

I servizi di localizzazione si diffondono e si diversificano, utilizzando la telefonia cellulare, la tecnologia delle radiofrequenze, i sistemi di rilevazione satellitare (che diverranno più efficienti con l'entrata in funzione del sistema Galileo). La localizzazione può riguardare lo stesso interessato o soggetti terzi; può interessare aree vaste o luoghi circoscritti; può essere momentanea o protratta nel tempo; può fornire servizi che vanno dal controllo di veicoli allo spostamento di persone. Riflettendo sui loro diversi effetti, si può dire che le tecnologie elettroniche, dopo aver contribuito in modo essenziale all'annullamento della distanza e creato le condizioni per controlli capillari, stanno anche facendo riscoprire la "prossimità". Infatti, quando i servizi di localizzazione sono solo quelli richiesti dall'interessato e riguardano l'area in cui egli stesso si muove, mettono la persona nella condizione di valorizzare la vicinanza fisica con altre persone o con specifici servizi.

Il rimanere perennemente in rete, peraltro, può modificare, o cancellare del tutto, il "diritto all'oblio". Fino a ieri una notizia apparsa anni prima su un giornale locale, una vecchia foto pubblicata in un remoto gazzettino, non seguivano implacabilmente la persona alla quale si riferivano. Oggi è sufficiente che quella notizia o quella foto si riferiscano ad una persona appena nota, o abbiano fatto parte di una vicenda di qualche rilevanza, ed ecco che basta digitare un nome su un motore di ricerca per farle riaffiorare, rendendo estremamente difficile il ricorso agli strumenti che possono consentire ad una persona di non rimanere prigioniera di un passato che non passa. E lo stesso divieto d'indagine sulle opinioni dei lavoratori, importantissima conquista sancita dall'articolo 8 dello Statuto dei lavoratori, rischia d'essere aggirato da esplorazioni in rete che non lasciano traccia.

A questo mutamento non assistiamo passivamente, e di esso non parliamo soltanto perché possa aversene pubblica consapevolezza. Interventi del Garante italiano, del Gruppo europeo sulla protezione dei dati personali, di molte autorità nazionali indicano le strade di una concreta strategia.

Abbiamo appena approvato un nuovo, ampio provvedimento sulla videosorveglianza, dove si individuano i modi per combinare correttamente libertà delle persone, esigenze di controllo, efficienza amministrativa. Per quanto riguarda le impronte digitali, abbiamo stabilito condizioni rigorose per eventuali e limitati trattamenti da parte dei privati, opponendoci, ad esempio, ad una loro utilizzazione per il semplice controllo dell'accesso a mense universitarie; ed attendiamo la relazione del Governo al Parlamento, come previsto da una mozione approvata dalla Camera dei deputati, per quanto riguarda le modalità della loro raccolta generalizzata a fini di identificazione, sulle quali esprimeremo il nostro parere. Registriamo positivi contatti con il Dipartimento per la pubblica sicurezza del ministero dell'Interno in materia di impronte digitali sui permessi di soggiorno e per la distinzione tra impronte dei comuni cittadini e impronte di persone sospettate. Sui diversi progetti di costituzione di banche dati del *Dna* diciamo fin da ora che esse devono essere limitate a finalità di particolare rilevanza e specificamente individuate, devono riguardare categorie assai circoscritte di soggetti, devono raccogliere i soli dati rilevanti per l'identificazione (con esclusione, quindi, di tutto quel che ha valenza predittiva o consente di risalire ad altri soggetti), devono precisare i rapporti tra i dati raccolti ed il materiale genetico dal quale sono estratti. No, in ogni caso, a tutto ciò che si presenta come schedatura di massa o ad utilizzazioni anche solo potenzialmente discriminatorie. Né finalità di sicurezza, e tanto meno interessi economici, possono mettere in discussione l'ineludibile principio d'eguaglianza. Pure in un ambiente come quello degli Stati Uniti, dove la forza della *business community* è persino straripante, il Senato ha approvato all'unanimità un progetto di legge che vieta ogni utilizzazione dei dati genetici da parte di assicuratori e datori di lavoro *(Genetic Non-Discrimination Act)*.

Questa strategia, oltre a ribadire il rigoroso riferimento ai principi di necessità, finalità, pertinenza e proporzionalità, sottolinea la necessità di una precisa distinzione tra finalità di identificazione e di verifica. Manifesta una preferenza per i

sistemi decentrati rispetto a quelli centralizzati e per una identificazione su base strettamente individuale (1:1) piuttosto che facendo riferimento a banche dati contenenti informazioni su una molteplicità di soggetti (1:M). Diverse autorità di controllo europee, infatti, sostengono già che i dati biometrici non dovrebbero essere raccolti in banche dati centralizzate, ma inseriti in un oggetto nella disponibilità diretta dell'interessato, come una carta con *microchip*, un telefono cellulare, una carta di credito. L'identificazione e la verifica, in altri termini, dovrebbero essere effettuate comparando il dato contenuto in quell'oggetto con il dato fornito dall'interessato al momento dell'identificazione e/o della verifica.

Libertà, sicurezza, diritti fondamentali

Si tratta di una strategia volta a mostrare l'improprietà delle tesi che vogliono identificare la tutela della sicurezza con la compressione della protezione dei dati personali, dunque di diritti fondamentali. Non solo sono possibili bilanciamenti tra i diversi interessi, ma è comunque indispensabile che ogni eventuale limitazione venga accompagnata da nuove garanzie, adeguate alla diversa situazione che si è creata. Un esempio può essere tratto proprio da una vicenda che ha comportato una modificazione dell'articolo 132 del Codice. Ritenendosi inadeguato il termine di trenta mesi per lo svolgimento delle indagini su reati particolarmente gravi, si è portato questo termine a quarantotto mesi. Ma questa "perdita" è stata, almeno in parte, "compensata" da modalità ancor più garantite di custodia "sotto chiave" dei dati, dalla riduzione a ventiquattro mesi del termine generale di conservazione, di cui si giovano tutti i cittadini, e dalla limitazione dell'utilizzabilità solo per una serie di reati gravi dei dati conservati per i successivi ventiquattro mesi.

Non siamo, evidentemente, insensibili ai temi della sicurezza. Ma operiamo

perché essi vengano affrontati in modo razionale, depurando le proposte dal tasso di emotività o improvvisazione che finiscono col renderle inefficienti, sottolineando sempre che il rispetto dei diritti e delle libertà fondamentali non è solo un dovere imposto dalle leggi, ma un formidabile "valore aggiunto" per la democrazia nella lotta contro chi, terroristi in primo luogo, negano con i loro atti proprio i suoi valori.

Lavoriamo per questo non soltanto in Italia. Un virtuoso circuito istituzionale ha ben funzionato nell'Unione europea. Infatti, solo grazie all'azione congiunta del Parlamento europeo e del Gruppo europeo dei garanti è stato finora possibile porre un argine alla pretesa dell'amministrazione americana di ottenere praticamente senza condizioni decine di milioni di dati sui passeggeri delle linee aeree in viaggio verso gli Stati Uniti, mentre altri paesi, come l'Australia e il Canada, hanno accettato le richieste di garanzie avanzate dall'Unione europea. Lo abbiamo detto in passato, e lo ripetiamo oggi: non si tratta di una vicenda circoscritta, ma di un confronto tra modelli di tutela dei diritti. E la sensibilità per il diritto e per i diritti, che la vecchia Europa continua a dimostrare, si conferma come una riserva di saggezza per tutti.

Per questo, dopo aver mostrato ieri che attraverso la protezione dei dati personali si giunge ad una vera "costituzionalizzazione della persona", richiamiamo oggi l'attenzione sulla necessità di una rilettura di molti tradizionali diritti. Il costante riferimento alla necessità di "rispetto dei diritti e delle libertà fondamentali" (art. 2.1 Codice) non implica soltanto un confronto concreto tra le specifiche forme di trattamento dei dati personali e i singoli diritti e libertà. Impone ormai una ricostruzione di libertà e diritti aderente all'ambiente tecnologico nel quale vengono esercitati: dalla considerazione come "formazioni sociali" delle comunità virtuali alla libertà di circolazione in luoghi videosorvegliati, dalla segretezza delle comunicazioni in Internet all'estensione della promessa della *Magna Charta* – "non metteremo mano su di te" – dal corpo fisico al corpo elettronico.

Consapevoli di tutto questo, abbiamo ritenuto che molte proposte di conservazione dei dati di traffico su Internet siano in conflitto con la dimensione dei diritti fondamentali. Ma non abbiamo mai considerato la rete come uno spazio senza regole. Basta ricordare i nostri interventi in materia di *spamming*, che hanno preso le mosse proprio dalla considerazione che la semplice reperibilità su Internet di un indirizzo di posta elettronica non implica la sua libera appropriabilità da parte di chiunque. In questo senso, il recente provvedimento in materia di propaganda elettorale, oltre a costituire un *vademecum* per i candidati, contribuisce a chiarire la differenza tra i diversi strumenti – posta tradizionale, stampa, telefono, comunicazione elettronica. Quest'ultima crea uno spazio del tutto nuovo, dove i cittadini devono poter esercitare una duplice libertà: quella d'essere al riparo da ogni comunicazione indesiderata e quella di potersi esprimere liberamente, nella forma della comunicazione e del collegamento. Questo spazio di libertà, non comparabile a quello individuato dagli altri mezzi di comunicazione e dove già si scambiano ogni giorno 300 milioni di messaggi elettronici, esige un grado di tutela particolarmente intenso.

Garante, istituzioni, cittadini

Il Codice ha aperto al Garante nuove possibilità di azione con l'articolo 154, estendendo il suo potere di segnalazione anche al Parlamento, e non più al solo Governo. Nasce così un nuovo circuito istituzionale, che si spera virtuoso quanto quello europeo.

Questo potere è già stato esercitato, in particolare nelle delicatissime materie della tutela dei dati sulla salute e della conservazione dei dati del traffico in rete. Da qui ha preso le mosse una collaborazione complessivamente assai positiva, testimo-

niata anche da alcuni voti unanimi con i quali la Camera dei deputati ha assunto posizioni che sottolineano l'importanza della tutela di questa nuova dimensione della libertà.

Il legame con il Parlamento, peraltro, riflette la specifica legittimazione del Garante, che vede i suoi quattro componenti scelti da un voto delle Camere. E il rafforzamento del Garante è in linea con l'emersione sempre più netta della sua natura di istituzione di garanzia, confermata anche dalla Carta dei diritti fondamentali dell'Unione europea e dal Progetto di Trattato per una Costituzione europea. Solo per i dati personali, infatti, è qui prevista la necessaria presenza di una autorità indipendente, che assume così una rilevanza "costituzionale". Per queste ragioni, perdurando la discussione sulla riforma delle autorità indipendenti, siamo dell'opinione che sarebbe preferibile il mantenimento delle attuali modalità di nomina dell'intero collegio che, proprio perché affidate al Parlamento, ne garantiscono meglio l'indipendenza. Lo ricordiamo anche perché davanti alla Commissione europea è stato sollevato un dubbio sulle modalità di nomina di alcune autorità europee, con l'argomento che il peso esercitato dall'esecutivo farebbe venir meno i requisiti di indipendenza richiesti della Direttiva 95/46.

L'azione del Garante non si esaurisce nei pur ricchi circuiti istituzionali interni ed internazionali. Vive sulla lunga frontiera del rapporto con il singolo cittadino, nel dialogo con l'opinione pubblica. Quello che oggi sta davanti a voi è un Garante più aperto e attento, non prigioniero di una banale logica di "comunicazione", ma consapevole della necessità di parlare e di essere compreso.

Prendendo sul serio il principio di semplificazione, è stato messo a punto un sistema di notificazioni elettroniche che non teme confronti con i sistemi degli altri paesi. Per gli obblighi di notificazione è stato delineato un percorso che offre più

ampi margini per adottare le misure di sicurezza. Abbiamo avviato una innovativa attività di formazione rivolta al mondo privato e a quello pubblico. Si svolgeranno nelle prossime settimane un seminario sullo *spamming* e un convegno sulle innovazioni tecnologiche. Con il codice di deontologia sulle centrali rischi private ci rivolgiamo ad una vastissima platea di cittadini, in un momento in cui il credito al consumo assume specifica rilevanza. Sono state rese più efficienti le strutture di rapporto con l'esterno. E tutti i componenti del Garante si sono recati in varie città, per illustrare direttamente i temi della protezione dei dati.

Segni, tutti, di una attenzione per le situazioni reali. Esattamente l'opposto di quella *"buroprivacy"* che qualcuno impugna come argomento contro il Codice e che, quando non è segno di cattiva coscienza, si traduce nella pretesa di annullare garanzie di tutti i cittadini per l'interesse magari di un gruppo ristretto.

Abbiamo reso più agevole la conoscenza e l'utilizzazione del nostro lavoro con le newsletter, e soprattutto con la pubblicazione di un Massimario riassuntivo di tutta la nostra "giurisprudenza", seguito con particolare attenzione dal nostro Vicepresidente, Giuseppe Santaniello. È imminente l'uscita di una raccolta di scritti su *privacy* e attività produttive, voluta da Gaetano Rasi. In un altro volume, "*Privacy* e giornalismo", Mauro Paissan ha sistemato i nostri interventi nel settore sensibilissimo dei mezzi di comunicazione. Senza mai cedere a tentazioni censorie, a paternalismi o a rigurgiti di moralismo, il Garante ha cercato di rendere effettiva una tutela di cui hanno bisogno, proprio per l'invadente spettacolarizzazione d'ogni momento della vita quotidiana, soprattutto i cittadini "comuni". E su questi temi è in corso un lavoro con l'Ordine dei giornalisti.

Sono aumentate le ispezioni, sono divenute più penetranti, hanno portato anche alla segnalazione all'autorità giudiziaria di ipotesi di reato. Rafforzeremo que-

sta attività, anche grazie all'eccellente collaborazione con la Guardia di finanza. Non sorprenda questo riferimento alle ispezioni, dunque ad un'attività repressiva, in una parte dedicata all'apertura all'esterno del Garante. Basta leggere le frequenti lettere ai giornali, per rendersi conto che nulla infastidisce i cittadini più dei casi in cui la legge sulla *privacy* è violata con intenzione, se non con protervia.

Ma, come sempre, sono le nude cifre ad avere la più forte eloquenza. Abbiamo deciso ben 775 ricorsi (erano stati 500 nel 2002), un impressionante dato quantitativo che rende immediatamente evidente una scelta preferenziale per la risoluzione delle controversie ad opera del Garante piuttosto che dall'autorità giudiziaria. Emerge così la più vera natura del Garante, quella di essere interlocutore diretto dei cittadini, come confermano le 4914 risposte a quesiti, segnalazioni e reclami (3689 nell'anno precedente) e, soprattutto, lo spettacolare balzo in avanti delle risposte a richieste di informazioni per telefono, passate da 12.800 a 38.000. In questi dati, più che il riflesso di difficoltà interpretative e applicative, riteniamo che debba scorgersi proprio l'effetto della migliore informazione sull'accesso al Garante e della riorganizzazione dell'Ufficio per le relazioni con il pubblico. Quale che sia la spiegazione più corretta di questo fenomeno, comunque, le cifre appena ricordate sono un segno di efficienza e, se scomposte nelle molteplici materie a cui si riferiscono, rivelano quanto sia larga l'area che la nostra attività deve coprire ogni giorno – salute, credito, telecomunicazioni, genetica, informazione, sicurezza, assicurazioni, pubblica amministrazione. Qui, in questo continuo confronto con il mondo, è il fascino del nostro lavoro.

Di fronte a tutti questi compiti, le forze di cui disponiamo sono inadeguate. Ma riusciamo a farcela lo stesso – tra mille difficoltà, e magari con qualche ritardo o conflitto. Per questo è grande il ringraziamento di tutto il Collegio, e il mio personale, a questa piccola e operosa comunità di lavoro, qui rappresentata dal segretario generale, Giovanni Buttarelli.

Vita privata e presenza pubblica

Lavorando così come facciamo, ci troviamo di fronte ad un altro problema. Spesso ai cittadini viene promesso un futuro pieno di efficienza amministrativa e occultato un presente in cui si moltiplicano gli strumenti di un controllo sempre più invasivo e capillare. Sembra quasi che si stiano costruendo due mondi non comunicanti, e che l'*e-government*, l'amministrazione elettronica, possa evolversi senza tener conto dei diritti individuali e collettivi. Noi proviamo a tenere insieme questi due aspetti, per restituire ai cittadini una immagine unitaria dell'ordinamento, così come ci preoccupiamo dell'unità della persona.

Si giunge così ad un altro punto di paragone, per noi ineludibile – quello del rapporto tra pubblico e privato. Una ventina d'anni fa, Albert Hirschman scriveva che "l'inversione verso la vita privata può essere considerata come un movimento verso la realtà, verso la sincerità, addirittura verso l'umiltà. Come la vita pubblica può consolarci della noia della vita privata, così la vita privata ci offre un riparo contro il parossismo e la futilità degli impegni pubblici". L'intimità come fattore di equilibrio, e dunque come possibilità di liberazione da altre tirannie.

A condizione, però, che non diventi disincanto, o distacco. Per ciò interpretiamo sempre più nettamente la protezione della vita privata non come un ritrarsi dalle brutture del mondo, non come un impossibile rifiuto del mutamento tecnologico, ma come una precondizione per l'esercizio pieno delle libertà e dei diritti. Lo diciamo ancora una volta: come un elemento prezioso della personalità e della cittadinanza.

IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI E LE NUOVE GARANZIE NEL CODICE

Premessa

La Relazione per il 2003 presenta una struttura in parte innovativa rispetto alle precedenti edizioni, allo scopo di dare un quadro ancora più adeguato dei principali problemi concreti che, nel presente e nell'immediato futuro, contraddistinguono la protezione dei dati personali.

La Relazione è quindi, in primo luogo, incentrata sul ruolo fondamentale che nel settore in esame hanno avuto nel 2003 le innovazioni normative.

Quello appena trascorso può infatti ben definirsi un anno "storico" per la privacy, in quanto ha visto ultimare il processo di armonizzazione delle molteplici fonti normative regolanti tale materia in un testo unico di rango legislativo, emanato con il d.lg. 30 giugno 2003, n. 196 (cd. Codice, citato nella Relazione con la maiuscola anche per distinguerlo dai codici deontologici di settore).

Tale fondamentale sviluppo normativo, la cui attuazione a livello amministrativo ha assorbito e sta assorbendo una consistente parte dell'attività dell'Autorità, è analizzato nel capitolo iniziale della Relazione in cui si dà conto anche del complessivo stato di recepimento delle direttive comunitarie in materia di dati personali negli Stati membri.

Il secondo capitolo, invece, riassume i diritti attribuiti agli interessati dalla normativa, come delineati da provvedimenti del Garante intervenuti nel 2003, nonché i principali doveri dei soggetti che trattano i dati personali, con particolare riferimento alle misure di sicurezza ed alla notificazione, anche alla luce dei recenti interventi dell'Autorità in proposito.

Nel terzo capitolo, poi, viene analizzata la ricca casistica relativa ai rapporti tra la privacy ed i diritti tutelati a livello costituzionale che con essa vengono continuamente a confrontarsi: in particolare, vengono prese in considerazione la libertà associativa (in cui si è fatto rientrare pure il fenomeno religioso e quello politico), la libertà di informazione e quella di iniziativa economica (art. 41, secondo comma, Cost.).

Nel quarto capitolo viene affrontato il delicato tema dell'applicazione della normativa sulla protezione dei dati personali nelle pubbliche amministrazioni centrali e locali: i provvedimenti del Garante mettono qui in luce il carattere solo parziale ed ancora insoddisfacente di tale applicazione e il perdurare, anche per il 2003, della necessità di interventi chiarificatori dell'Autorità sui rapporti tra la normativa in materia di privacy e le specifiche discipline di settore che regolano l'agire delle pubbliche amministrazioni.

Il quinto capitolo, che chiude la prima parte della Relazione, guarda a quei settori nei quali, in un prossimo futuro, la privacy dovrà fronteggiare le sfide più importanti che l'evoluzione tecnologica porta al necessario rispetto dei diritti della persona, secondo la prospettiva –costantemente seguita dal Garante nei suoi interventi– di una giusta sinergia tra la diffusione delle nuove tecnologie e l'elevato livello della tutela dei dati personali ora assicurato dal Codice.

La seconda parte della Relazione, infine, è dedicata all'Ufficio del Garante, visto sotto i due profili dell'attività e della gestione amministrativa.

IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

I - Il quadro normativo
Normativa nazionale

1 Il Codice in materia di protezione dei dati personali

1.1. Il percorso per arrivare al Codice

Nel 2003 è stato completato l'*iter* normativo di integrazione e razionalizzazione della disciplina in materia di protezione dei dati personali: con il d.lg. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), per la prima volta nel panorama internazionale, viene riunita in un unico corpo normativo una materia, quella della protezione dei dati, la cui disciplina si era formata nel tempo con vari interventi integrativi e modificativi della l. 31 dicembre 1996, n. 675, apportati in attuazione della delega originariamente contenuta nella legge n. 676/1996 e, successivamente, nella l. 24 marzo 2001, n. 127 (v. art. 1, comma 4).

Il delicato lavoro preparatorio di ricognizione e di studio delle norme da riunire nel testo unico, svolto da un'apposita commissione istituita presso il Dipartimento per la funzione pubblica della Presidenza del Consiglio dei ministri e presieduta dal prof. Cesare Massimo Bianca, si è concluso nei primi mesi del 2003 con una scelta orientata per l'adozione di un testo unico di rango legislativo, anziché misto, in linea con i nuovi orientamenti della legge di semplificazione per il 2001 (l. 29 luglio 2003, n. 229), all'epoca in fase di approvazione. Il doppio vaglio da parte del Consiglio dei ministri, i pareri delle competenti commissioni parlamentari e di questa stessa Autorità hanno evidenziato una positiva convergenza di intenti e un'obiettiva sinergia di apporti diretti a mantenere ed innalzare il livello di garanzia dei diritti delle persone (in alcuni casi anche sviluppato in nuovi settori di disciplina) ed al tempo stesso a semplificare adempimenti e modalità di esercizio dei diritti.

1.2. La sistematica del Codice

Il Codice, che ha anche recepito la direttiva n. 2002/58/CE in tema di tutela della vita privata nel settore delle comunicazioni, e del quale è possibile indicare in questa sede solo alcuni tratti essenziali, si compone di tre parti: la prima, recante le disposizioni generali applicabili a tutti i trattamenti ed alcune ulteriori regole specifiche per i trattamenti effettuati da soggetti pubblici o privati; la seconda, nella quale sono riunite disposizioni particolari esclusive per alcuni trattamenti, che integrano o in qualche caso derogano alle disposizioni generali della parte prima; la terza, concernente la tutela amministrativa e giurisdizionale dell'interessato, i controlli ed il sistema delle sanzioni.

1.3. I principi: il diritto alla protezione dei dati personali e il rafforzamento delle garanzie

Sul piano generale delle garanzie, il Codice reca il solenne riconoscimento, nel nostro ordinamento, dell'autonomo diritto alla protezione dei dati personali (art. 1, d.lg. n. 196/2003), in armonia con quanto già previsto nella Carta dei diritti fondamentali dell'Unione europea e nel progetto di Costituzione europea.

Pur essendo informato ai canoni di semplificazione, armonizzazione ed efficacia, il Codice prescrive che il trattamento dei dati personali si svolga in un quadro di elevata tutela (art. 2, comma 2, d.lg. n. 196/2003) per i diritti delle persone e nel rispetto del "principio di necessità" nel trattamento stesso (art. 3, d.lg. n. 196/2003), principio esteso ai sistemi informativi ed ai *software*, anche per ciò che riguarda la loro configurazione, affinché i dati personali o identificativi siano utilizzati solo se indispensabili per raggiungere le finalità consentite nei singoli casi.

1.4. Le novità normative in tema di accesso ai dati

In materia di accesso ai dati personali, il Codice contiene alcune novità di rilievo sul piano pratico-applicativo.

Accesso ai dati valutativi

In particolare, si conferma espressamente che la richiesta di accesso ai dati personali e l'esercizio degli altri diritti connessi possa riguardare anche i dati di tipo valutativo, salvo per quanto attiene alla loro rettifica o integrazione (art. 8, comma 5, d.lg. n. 196/2003). In relazione ai limiti all'esercizio dei diritti dell'interessato, resta poi significativa la qualificazione di quel pregiudizio per lo svolgimento di investigazioni difensive o per l'esercizio di un diritto, che legittima il "differimento" dell'accesso e, sotto altro profilo, rende possibile accedere ai dati relativi a chiamate telefoniche in entrata, altrimenti non accessibili, in termini di pregiudizio "effettivo e concreto".

Altra novità importante in materia di accesso è contenuta nell'art. 7, comma 2, lett. *e)*, del Codice, secondo cui l'interessato ha il diritto di ottenere dal titolare anche l'indicazione dei soggetti che, in qualità di responsabili o di incaricati, possono venire a conoscenza dei dati che lo riguardano.

Conoscibilità delle informazioni relative a terzi

Infine, sono previste particolari modalità di riscontro alla richiesta di accesso, allo scopo di facilitarne la comprensione sotto il profilo espositivo, come pure la possibilità, per l'interessato, di conoscere informazioni relative a terzi quando la scomposizione dei dati personali renderebbe incomprensibili i dati richiesti (art. 10, commi 4, 5 e 6, d.lg. n. 196/2003).

1.5. Tutela dei diritti

Ampliamento dei termini del riscontro

In chiave di maggiore tutela per l'interessato, nonché di semplificazione anche per il titolare del trattamento, devono essere lette alcune disposizioni del Codice che snelliscono l'esercizio dei diritti e favoriscono la soluzione preventiva delle potenziali controversie direttamente fra l'interessato e il titolare o responsabile del trattamento. Viene perciò previsto un termine più ampio rispetto al passato per completare il riscontro all'esercizio dei diritti stessi (quindici giorni dal ricevimento della richiesta) e si pone a disposizione del titolare un possibile ampliamento di tale termine sino a trenta giorni quando le operazioni necessarie per un integrale riscontro sono di particolare complessità, ovvero ricorre altro giustificato motivo (art. 146 d.lg. n. 196/2003).

Per quanto riguarda poi la tutela in sede giudiziaria dei diritti, il Codice armonizza i vari riti innanzi al giudice ordinario, ora ricondotti opportunamente ad un'unica procedura intentata mediante ricorso al solo tribunale (art. 152 d.lg. n. 196/2003).

1.6. Semplificazioni: notificazione, informativa, consenso

Non mancano, nel Codice, altri interventi di snellimento delle modalità di esercizio dei diritti e degli adempimenti cui sono tenuti i titolari del trattamento, pubbliche amministrazioni e imprese. Nel solco del processo di semplificazione (senza intaccare le garanzie) già intrapreso con il d.lg. n. 467/2001, vengono individuati in modo espresso i casi, più ridotti rispetto al passato, in cui è previsto l'obbligo di notificazione del trattamento al Garante (che può ora essere effettuata solo in via telematica) in relazione ai soli trattamenti che possono presentare rischi per l'interessato (artt. 37 e 38 d.lg. n. 196/2003). Con le modifiche apportate, si è così individuato un insieme più circoscritto di trattamenti oggetto di notificazione, capovolgendo il precedente impianto della normativa nei limiti consentiti dalla specifica disciplina comunitaria. Ulteriori trattamenti possono peraltro essere sottratti all'obbligo di notificazione con provvedimento del Garante (come quello, di cui si dirà oltre, adottato il 31 marzo 2004), provvedimento che, del pari, può individuare eventuali altri trattamenti da notificare, benchè non inclusi nella lista normativa di cui all'art. 37 del Codice.

Semplificazioni sono state previste anche in materia di informativa all'interessato: si prevede, infatti, che il Garante possa individuare modalità semplificate per fornire l'informativa, in particolare in assenza di una relazione diretta con l'interessato (si pensi ad un *call-center*: art. 13, comma 3, d.lg. n. 196/2003). Il Codice, inoltre, introduce modalità semplificate per l'informativa e per la manifestazione del consenso dell'interessato in relazione al trattamento di dati in ambito sanitario.

Infine, notevole valenza semplificativa, sempre nel mantenimento di un elevato livello di tutela, ha l'estensione dei casi in cui il trattamento può essere effettuato da soggetti privati ed enti pubblici economici in assenza del consenso dell'interessato. Così è per il trattamento di dati "comuni" effettuato da organismi *no-profit*, a condizione che il trattamento riguardi dati degli associati e non preveda la comunicazione ad altri soggetti e la diffusione, analogamente a quanto disposto per i dati sensibili (art. 24, comma 1, lett. *h)*, d.lg. n. 196/2003). La norma, tuttavia, a garanzia degli interessati, condiziona questo presupposto equipollente al consenso all'individuazione, da parte dei titolari del trattamento, delle specifiche modalità di utilizzo dei dati, da rendere note agli associati con l'informativa (analoga condizione è stata inserita per i trattamenti di dati sensibili nell'art. 26, comma 4, lett. *a)*, del d.lg. n. 196/2003).

Dal consenso si può parimenti prescindere quando il trattamento di dati sensibili è necessario per adempiere a specifici obblighi previsti dalla normativa in materia di gestione del rapporto di lavoro, sempre che siano rispettati i limiti previsti dall'autorizzazione del Garante (art. 26, comma 4, lett. *d)*, d.lg. n. 196/2003).

1.7. Diritto nazionale applicabile e flussi transfrontalieri

Principio di "stabilimento"

Con il Codice viene completato il recepimento del principio comunitario di "stabilimento" del titolare del trattamento (art. 4, direttiva n. 95/46/CE) quale criterio principale per individuare la disciplina nazionale applicabile. In linea con il principio di semplificazione nelle operazioni di esportazione dei dati, si esclude poi l'obbligo di notificare specificatamente al Garante il trasferimento dei dati personali verso Paesi non appartenenti all'Ue (con la conseguente soppressione dell'obbligo di attendere il decorso del termine previsto dall'art. 28, comma 2, della legge n. 675/1996 prima di poter procedere al trasferimento), consentendo

di indicare tale operazione nell'unica notificazione cui eventualmente il titolare del trattamento sia tenuto (art. 37 d.lg. n. 196/2003).

1.8. Misure di sicurezza

Misure idonee e minime

In tema di misure di sicurezza il Codice conferma il "doppio binario" per gli obblighi cui sono tenuti i titolari già in base alla legge n. 675/1996, prevedendo, sul piano della liceità del trattamento e della stessa responsabilità civile, l'obbligo di adottare tutte le misure "idonee" a ridurre al minimo i rischi di danni per l'interessato (artt. 15 e 31 d.lg. n. 196/2003), e, per quanto concerne quella penale, l'obbligo di adottare quanto meno quelle cd. "misure minime" (artt. 33-36 e 169 d.lg. n. 196/2003).

Disciplinare tecnico

Le "misure minime" di sicurezza, già contenute nel d.P.R. 28 luglio 1999, n. 318, sono state peraltro aggiornate anche sulla base del progresso tecnologico degli ultimi anni e sono indicate in un apposito disciplinare tecnico allegato al Codice (all. B), modificabile con decreto ministeriale onde consentirne agevolmente il costante adeguamento.

1.9. I trattamenti in ambito pubblico

L'impianto della parte generale di disciplina relativa ai trattamenti effettuati da soggetti pubblici non ha subito rilevanti mutamenti, salvo alcuni interventi comunque significativi, anche di chiarimento, riguardanti in specie le comunicazioni al Garante ed il trattamento di dati sensibili.

I soggetti pubblici possono continuare a trattare dati sensibili solo se la legge o, in via transitoria il Garante, abbiano previamente individuato le rilevanti finalità di interesse pubblico perseguite con un determinato trattamento, e i soggetti pubblici stessi abbiano, parimenti, individuato e previamente reso conoscibili i tipi di dati e di operazioni eseguibili (art. 20 d.lg. n. 196/2003, già art. 22, comma 3-*bis*, legge n. 675/1996).

Ora, il Codice consente alle pubbliche amministrazioni, che non abbiano ancora provveduto in proposito, di adempiere al più tardi entro il 30 settembre 2004 (art. 181, comma 1, lett. *a)*, d.lg. n. 196/2003). In ragione della natura sensibile dei dati trattati, che richiede in ogni caso elevate garanzie, l'atto con il quale i soggetti individuano i tipi di dati e di operazioni eseguibili deve avere natura regolamentare, in linea con quanto ritenuto dal Garante già sotto la previgente normativa; al fine di assicurarne la più ampia omogeneità si prevede, inoltre, che i regolamenti possano essere redatti anche sulla base di schemi-tipo (art. 20, comma 2, d.lg. n. 196/2003).

1.10. I codici di deontologia e di buona condotta

Al fine di rendere il dato normativo sempre più aderente alla realtà, con il d.lg. n. 196/2003 si è rafforzata l'importanza dei codici di deontologia e di buona condotta in materia di protezione dei dati personali, prevedendone la sottoscrizione in molteplici e significativi settori: si pensi ai trattamenti di dati effettuati tramite Internet, ovvero per la gestione del rapporto di lavoro, per fini di *direct marketing* come pure da parte delle "centrali rischi" private o, ancora, con riguardo alla videosorveglianza. A tutti i codici deontologici viene ora esteso il principio secondo cui il rispetto delle norme in essi contenute è condizione essenziale per la liceità dei trattamenti (previsione originariamente riferita solo ai codici indicati nell'art. 20 del

d.lg. n. 467/2001, nonché a quelli in materia di ricerca statistica e storica).

Codici di deontologia di imminente sottoscrizione

Per taluni di essi, in particolare quelli riferiti ai trattamenti effettuati nell'ambito di sistemi informativi gestiti da "centrali rischi" private, come pure per quelli concernenti l'attività di investigazione privata o relativi agli scopi statistici e di ricerca scientifica perseguiti in ambito privato, i lavori sono sostanzialmente terminati o in fase di avanzata elaborazione.

1.11. La conservazione dei dati di traffico

D.l. 24 dicembre 2003, n. 354

Nonostante la sua recente approvazione, il Codice ha subito un intervento modificativo in un settore di rilievo, quello dei trattamenti effettuati per ragioni di giustizia. Con il d.l. 24 dicembre 2003, n. 354, convertito, con modificazioni, dalla l. 26 febbraio 2004, n. 45, è stata, tra l'altro, introdotta una modificazione all'art. 132 del Codice, che disciplina la conservazione dei dati di traffico per finalità di accertamento e repressione di reati.

Nella sua formulazione originaria, l'art. 132 del Codice prevedeva che i fornitori di servizi di comunicazione elettronica dovessero conservare i "dati relativi al traffico telefonico" per trenta mesi, per finalità di accertamento e repressione di reati.

Sulla base di alcuni successi investigativi in delicate inchieste riguardanti atti di terrorismo, si è avviato uno specifico dialogo tra il Garante e alcuni uffici giudiziari, in particolare la Direzione nazionale antimafia, che ha portato ad approfondire alcune possibili nuove soluzioni di disciplina, le quali sono state doverosamente segnalate alle autorità di governo.

Modifiche all'art. 132 del Codice

Intendendo garantire l'efficacia di tali investigazioni su delitti di particolare gravità che possono richiedere indagini lunghe ed articolate, il decreto legge in esame aveva però drasticamente soppresso il riferimento al traffico telefonico (riferendosi in modo più ampio ai "dati di traffico"), introducendo anche un'ulteriore fase di conservazione dei dati per altri trenta mesi per il perseguimento dei delitti di cui all'art. 407, comma 2, lett. *a)*, c.p.p., nonché di quelli in danno di sistemi informatici o telematici. Inoltre, modificando l'originaria versione dell'art. 132, il decreto legge aveva previsto una disciplina più dettagliata delle modalità di acquisizione dei dati da parte dell'autorità giudiziaria; si era altresì demandata ad un successivo decreto interministeriale, da adottarsi su conforme parere del Garante, l'individuazione delle modalità di conservazione e di trattamento dei dati, in base a taluni criteri-guida normativamente prefissati (individuazione di talune misure di sicurezza; conservazione separata dei dati per i successivi trenta mesi; garanzia del diritto di accesso e degli altri diritti previsti dall'articolo 7 del d.lg. n. 196/2003; distruzione periodica dei dati decorsi i periodi di conservazione).

Le soluzioni prefigurate dal decreto legge hanno suscitato un ampio dibattito.

Rischi segnalati dal Garante

Al fine di assicurare il pieno rispetto dei diritti fondamentali della persona, subito dopo l'emanazione del decreto legge e durante i lavori per la sua conversione (AC 4594), anche nel corso dell'audizione del presidente dell'Autorità innanzi alla Commissione giustizia della Camera (tenutasi il 20 gennaio scorso), il Garante ha segnalato al Parlamento che le formule ipotizzate per prolungare i tempi di conservazione dei dati (tornati, dagli originari trenta mesi del Codice, ad un periodo mas-

simo di cinque anni) e, soprattutto, l'estensione delle nuove regole al traffico su Internet, avrebbero determinato una forte compressione delle garanzie della persona, anche in relazione ai principi costituzionali in materia di libertà delle comunicazioni e segretezza della corrispondenza.

L'approvazione delle mozioni

Anche alla luce del dibattito svoltosi il 14 gennaio 2004 nell'aula della Camera, dove, con orientamenti unanimi, sono state approvate due convergenti mozioni della maggioranza e dell'opposizione (le quali hanno impegnato il Governo a *"rimuovere tutte le norme potenzialmente lesive dei diritti di riservatezza"* previsti, fra l'altro, *"dall'articolo 15 della Costituzione"* e a *"regolamentare in modo più efficace il trattamento dei dati di traffico della telefonia mobile, al fine di tutelare il diritto degli individui"*), la Commissione ha approvato alcune prime modifiche al decreto legge fra le quali, in particolare:

Modifiche al decreto legge:
• in commissione

a) il riferimento non già, genericamente, ai dati inerenti al traffico, ma ai *"dati relativi al traffico telefonico o alla corrispondenza in via telematica"*;

b) la riduzione dei tempi di conservazione dei dati, dai cinque anni complessivi (trenta mesi più altri trenta mesi), a quattro anni (ventiquattro mesi più altri ventiquattro mesi);

c) l'attribuzione al Garante, con proprio provvedimento da adottare ai sensi dell'articolo 17 del Codice (cd. *prior checking*) del compito di disporre particolari misure a garanzia dell'interessato.

• in assemblea

Nel corso della discussione in Assemblea è poi emersa la più ampia scelta di sopprimere ogni riferimento ai dati di traffico diversi da quello telefonico, stante la particolare delicatezza di una *data retention* sistematica dei dati di traffico in Internet. Si è ritenuto infatti necessario procedere ad una valutazione più approfondita, e sulla base di un dibattito pubblico, delle implicazioni che ciò avrebbe sullo sviluppo delle reti. Si sono altresì considerate le importanti implicazioni che il trattamento di quei dati può avere sulla riservatezza e sugli altri diritti e libertà fondamentali degli interessati, come pure l'oggettiva complessità e difficoltà della loro conservazione e gestione.

L'Assemblea ha, invece, confermato la scelta della Commissione circa la riduzione dei tempi di conservazione a quattro anni complessivi ed ha eliminato il rinvio ad un apposito decreto interministeriale per la determinazione delle modalità di trattamento e di conservazione dei dati.

Il Senato ha, infine, approvato definitivamente il testo licenziato dalla Camera.

2 Altre attività normative

Nel corso dell'anno sono stati approvati numerosi altri provvedimenti riguardanti aspetti d'interesse per la materia del trattamento dei dati personali rispetto ai

quali, schematicamente, si segnalano i profili più rilevanti:

a) l'art. 50 del d.l. 30 settembre 2003, n. 269, convertito, con modificazioni, dalla l. 24 novembre 2003, n. 326, "collegato" alla legge finanziaria 2004, con cui sono state introdotte disposizioni per il controllo della spesa sanitaria.

L'art. 50 del d.l. n. 269/2003)

Il Garante, nel corso dei lavori di conversione del decreto legge, ha richiamato l'attenzione delle Camere sui delicati problemi sollevati da tale disposizione, che prevede, fra l'altro, la costituzione di banche dati a fini di controllo della spesa sanitaria. Tale finalità, pur essendo ispirata dall'esigenza di incentivare il monitoraggio della spesa pubblica è però, allo stato, perseguita attraverso strumenti che (senza fermi accorgimenti che potrebbero essere introdotti, almeno in parte, nei vari decreti attuativi previsti) rischiano di compromettere il diritto dei cittadini alla protezione dei dati e in particolare di quelli riguardanti lo stato di salute, protetti da particolari garanzie. Attraverso i farmaci prescritti e le prestazioni specialistiche ottenute può essere infatti ricostruita analiticamente la storia sanitaria di ciascun soggetto.

Le preoccupazioni manifestate dal Garante

L'Autorità ha ricordato che la legislazione vigente prevede già procedure per il monitoraggio della spesa sanitaria che non presuppongono la costituzione di banche dati centralizzate sulla salute. Tali procedure possono essere rese più efficienti, ma non possono tradursi in una compressione del diritto alla protezione dei dati personali. Le finalità di contenimento della spesa possono essere egualmente perseguite con altre modalità basate su una verifica della genuinità di dichiarazioni e attestazioni relative al reddito, sull'uniformità dei *software* utilizzati e con un accesso particolarmente selettivo ad altri dati, effettuato solo localmente e laddove vi sia un'effettiva e concreta necessità, escludendo un accumulo sistematico di milioni e milioni di posizioni.

L'Autorità ha sottolineato, peraltro, che il sistema disegnato dal decreto legge potrebbe anche discriminare i cittadini in base al reddito, in quanto chi può permettersi di pagare direttamente i farmaci e le prestazioni specialistiche non verrebbe inserito nelle banche dati. Infine, il Garante ha sottolineato che la previsione di una tessera sanitaria rischierebbe di favorire la confusione nel settore della carte elettroniche identificative, dove un'ulteriore tessera andrebbe ad aggiungersi a quelle già in fase di sperimentazione.

Le preoccupazioni manifestate dal Garante non sono state fugate dall'ulteriore testo dell'art. 50 convertito in legge, anche tenendo conto della previsione del progressivo assorbimento della tessera sanitaria nella carta d'identità elettronica o nella Carta nazionale dei servizi (art. 50, comma 13, d.l. n. 269/2003). Sul piano applicativo, poi, si è determinata una sovrapposizione fra il decreto legge e il Codice per la messa a punto del modello di ricetta medica, in quanto anche il decreto legislativo n. 196 del 2003 reca disposizioni in proposito (art. 87). Il dibattito parlamentare sviluppatosi sul punto è sfociato in un ordine del giorno della Camera, con cui si impegna il Governo *"ad adottare le adeguate iniziative normative al fine di escludere il trattamento dei dati sensibili degli assistiti"*. Il Garante, in ogni caso, continuerà a seguire attivamente queste tematiche anche in sede di formulazione dei necessari pareri sugli schemi dei decreti di attuazione dell'art. 50 (art. 154, comma 4, d.lg. n. 196/2003), come pure nell'esprimere il necessario parere ai fini del trattamento dei dati sensibili (art. 20);

L'ordine del giorno della Camera

b) la l. 19 febbraio 2004, n. 40, recante disposizioni in materia di procreazione assistita: nel corso dell'esame del disegno di legge si è tenuta alla Camera un'audizione del presidente dell'Autorità, prof. Stefano Rodotà, nella quale sono stati segnalati alcuni aspetti d'interesse in materia di protezione dei dati personali. Successivamente, in sede di prima applicazione della legge, si è ottenuto, in accordo con il Ministro della salute, che le comunicazioni (che i centri autorizzati ad applicare le tecniche di procreazione assistita dovevano trasmettere ai sensi del relativo art. 17) fossero effettuate utilizzando codici numerici in luogo dell'indicazione nominativa delle persone che si erano rivolte ai medesimi centri;

Le nuove norme in materia di occupazione e mercato del lavoro

c) il d.lg. 10 settembre 2003, n. 276, recante "Attuazione delle deleghe in materia di occupazione e mercato del lavoro, di cui alla legge 14 febbraio 2003, n. 30": contiene alcune disposizioni in materia di trattamento di dati personali effettuati nell'ambito del rapporto di lavoro (artt. 8-10, 15, 16 e 73 d.l. n. 276/2003) che sarebbe stato più opportuno inserire nel Codice. In relazione a queste disposizioni, il Garante fornirà comunque alcune indicazioni in occasione dell'espressione del parere sugli schemi di decreto ministeriale cui spetta individuare alcune modalità di trattamento dei dati e definire flussi informativi volti ad agevolare l'incontro tra domanda ed offerta di lavoro (artt. 8, comma 2, e 16, comma 2, d.lg. n. 276/2003). Il decreto prevede anche alcune garanzie a fini di informazione agli interessati in caso di annunci di lavoro pubblicati su giornali o effettuati mediante reti di comunicazione elettronica (art. 9 d.lg. n. 276/2003). Sono poi vietate le discriminazioni che possono derivare dal trattamento di dati sensibili o di dati non pertinenti ed eccedenti rispetto alle finalità tipiche del rapporto di lavoro, divieto esteso alle agenzie per il lavoro e agli altri soggetti abilitati alla selezione del personale o all'effettuazione di indagini (art. 10 d.lg. n. 276/2003);

La legge di semplificazione per il 2001 e le norme del Codice sulla diffusione *on line* delle sentenze (artt. 51 e 52)

d) la l. 29 luglio 2003, n. 229, cd. legge di semplificazione per il 2001: ha riflessi sulla materia della protezione dei dati, da un lato per la delega di riordino della normativa concernente il documento informatico, la firma elettronica e digitale, la sicurezza dei dati e dei sistemi e l'accesso informatico (in relazione alla quale l'Autorità ha già fornito una prima collaborazione nell'ambito della commissione istituita su iniziativa del Dipartimento per la funzione pubblica); dall'altro, in ragione di una disposizione in tema di riproduzione e diffusione mediante strumenti telematici delle sentenze e delle altre decisioni del giudice amministrativo e contabile (art. 19 legge n. 229/2003) che dovrà essere applicata, come peraltro segnalato dall'Autorità, nel rispetto dei principi di protezione dei dati. Il Codice contiene, infatti, alcune disposizioni per favorire la conoscenza sia dei dati identificativi dei giudizi pendenti, sia delle decisioni giudiziarie adottate, attraverso la loro disponibilità *on line* nei siti Internet delle autorità giudiziarie interessate (art. 51). Al tempo stesso, però, il Codice prevede in favore delle parti alcune situazioni di anonimato nel caso in cui la sentenza sia riprodotta su riviste giuridiche, mediante *compact disk*, o tramite Internet, senza intaccare le vigenti disposizioni processuali sulla pubblicazione delle sentenze e sulla conoscibilità di atti giudiziari secondo le regole dei codici di rito (art. 52). Si prevede infatti che ciascun interessato possa richiedere "per motivi legittimi" alla cancelleria o alla segreteria competenti l'apposizione, sull'originale della decisione, di un'annotazione per precludere, in caso di riproduzione della sentenza, l'indicazione

delle proprie generalità o di altri dati identificativi. L'annotazione può essere altresì apposta d'ufficio dal giudice, a garanzia della dignità dell'interessato. Anche a prescindere da tale annotazione, chiunque diffonda provvedimenti giudiziari deve omettere i dati personali dai quali possa desumersi anche indirettamente l'identità di minori (art. 52, comma 5, d.lg. n. 196/2003): è qui evidente l'intento di assicurare più ampie garanzie di riservatezza a soggetti particolarmente meritevoli di protezione, in linea con altri strumenti già presenti nell'ordinamento (cfr. art. 734-*bis* c.p.). Una disposizione transitoria limita l'obbligo di omettere i dati identificativi dell'interessato per le sentenze adottate prima dell'entrata in vigore del Codice, prevedendolo solo nel caso in cui l'interessato medesimo ne faccia espressa richiesta e, comunque, per i documenti pubblicati mediante Internet o diffusi su nuovi supporti, informatici o cartacei (art. 181, comma 5, d.lg. n. 196/2003).

Come già ricordato, poi, la legge n. 229/2003 sostituisce il ricorso ai testi unici, anche misti, con la distinta codificazione della normativa primaria e secondaria: a questa modifica si è tempestivamente ispirato il Governo includendo, nel Codice in materia di protezione dei dati personali, norme aventi tutte rango primario;

e) la l. 20 giugno 2003, n. 140, che reca disposizioni in materia di intercettazioni e di acquisizione di tabulati concernenti conversazioni o comunicazioni di parlamentari intercettate nel corso di procedimenti riguardanti terzi, prevedendo la distruzione dei verbali e delle registrazioni relative alle intercettazioni irrilevanti (art. 6). Tale normativa ha effetti in materia di protezione dei dati personali: infatti, la sua eventuale violazione può comportare l'inutilizzabilità dei dati personali trattati (artt. 11, comma 2, 47 e 53 d.lg. n. 196/2003);

f) il d.l. 27 giugno 2003, n. 151, convertito dalla l. 1 agosto 2003, n. 214, recante modifiche al codice della strada, che contiene nuove disposizioni in materia di "accertamenti qualitativi non invasivi" e di ulteriori verifiche sullo stato delle persone da parte degli organi di polizia, in relazione al divieto di guida in stato di ebbrezza o di alterazione psico-fisica per uso di sostanze stupefacenti;

g) il d. l. 9 maggio 2003, n. 105, convertito dalla l. 11 luglio 2003, n. 170, il cui art. 1-*bis* istituisce l'anagrafe nazionale degli studenti e dei laureati delle università: sul tema, l'Autorità sta collaborando con il Ministero dell'istruzione, dell'università e della ricerca per la messa a punto del decreto di attuazione dell'anagrafe, con il quale vengono individuati i dati personali che possono esservi inseriti;

h) la l. 16 gennaio 2003, n. 3, recante "Disposizioni ordinamentali in materia di pubblica amministrazione" (c.d."collegato" alla finanziaria 2002): ha previsto alcuni interventi mediante regolamenti governativi in materia di innovazione tecnologica nella pubblica amministrazione, con riguardo, in particolare, alla diffusione della Carta nazionale dei servizi (Cns) e all'accesso telematico agli atti della pubblica amministrazione (art. 27); rispetto ad essa il Garante ha espresso il parere di competenza sullo schema di regolamento recante disposizioni per la diffusione e l'uso della Carta nazionale dei servizi (v. *infra*, parag. 45.2.).

3 Lavori parlamentari

Oltre ai provvedimenti normativi sin qui descritti, vanno segnalati i lavori parlamentari relativi ad altre iniziative legislative ugualmente d'interesse per la tematica della protezione dei dati personali. In proposito si ricordano:

a) alcune proposte di legge in materia di vigilanza privata (AC 4209 del Governo e proposte abbinate, all'esame della Commissione affari costituzionali della Camera) e di investigazione privata (AS 490, presso la Commissione giustizia del Senato) per gli aspetti che riguardano il trattamento dei dati personali, anche ai fini della sottoscrizione da parte delle categorie interessate del codice di deontologia e di buona condotta in materia di investigazione privata e indagini difensive, in fase di avanzato approfondimento (art. 135 d.lg. n. 196/2003);

Protesti bancari

b) due disegni di legge in materia di cancellazione dei dati personali dagli elenchi dei protesti bancari e di omonimia nei protesti bancari (AS 1368 ed AS 839, esaminati congiuntamente dalla Commissione giustizia del Senato). Tali proposte di legge assumono rilievo anche in vista dell'adozione del codice deontologico in materia di informazioni commerciali, nell'ambito del quale devono essere individuati termini armonizzati di conservazione dei dati personali contenuti in banche di dati pubbliche e private riferite al comportamento debitorio dell'interessato, diverse dalle "centrali rischi" private (artt. 117, 118 e 119 d.lg. n. 196/2003);

c) alcuni disegni di legge che recano modifiche al codice di procedura civile (AS 2430 ed abb. presso la Commissione giustizia del Senato), per i quali appare opportuno un coordinamento con le disposizioni introdotte dal Codice in materia di notificazioni di atti giudiziari (art. 174 d.lg. n. 196/2003);

d) il disegno di legge del Governo recante disposizioni per l'attuazione della decisione del Consiglio dell'Unione europea che istituisce Eurojust (AC 4293, all'esame della Commissione giustizia della Camera);

e) tre proposte di legge di iniziativa parlamentare, sostanzialmente identiche, che prevedono l'istituzione del Difensore dei diritti delle persone private della libertà personale (AC 411, Pisapia ed altri, AC 3229, Mazzoni e AC 3344, Finocchiaro ed altri, all'esame della Commissione affari costituzionali della Camera).

Il Garante o Difensore civico nelle carceri è già conosciuto ed operante in molti Paesi europei, ma non è allo stato previsto dalla legislazione nazionale: recentemente, invece, è stata sottoposta all'attenzione dell'Autorità una legge regionale che ha istituito tale autorità in ambito locale. In base a quanto previsto dal testo unificato delle tre proposte di legge, recentemente elaborato, al Difensore civico è riconosciuto il compito di tutelare i diritti fondamentali delle persone detenute o comunque private della libertà personale, in conformità ai principi ed alle disposizioni contenuti nella

Costituzione, nelle leggi e nelle convenzioni internazionali sui diritti umani; gli è inoltre riconosciuto il diritto di accesso presso tutte le pubbliche istituzioni nelle quali la legge prevede sia limitata la libertà personale, nonché il diritto di incontrare chiunque senza restrizioni;

Il progetto sull'accesso della polizia ai dati detenuti dai vettori

f) una proposta di legge in materia di accesso delle forze di polizia ai dati detenuti da vettori aerei e navali (AC 2630), della quale si è già data notizia nella precedente *Relazione* annuale. Nell'ambito dei lavori presso la Commissione affari costituzionali della Camera si è tenuta, il 14 gennaio 2003, un'audizione del presidente del Garante, il quale ha espresso l'esigenza che il progetto normativo rispetti i principi in materia di protezione dei dati personali applicabili ai trattamenti effettuati per finalità di polizia, prevedendosi, in ogni caso, richieste di informazioni circostanziate, selettive e finalizzate unicamente al perseguimento di gravi reati di terrorismo o di criminalità organizzata.

Il recepimento delle direttive comunitarie

4 Stato di recepimento delle direttive comunitarie negli Stati membri

4.1. Il recepimento della direttiva n. 95/46/CE

Gli attuali quindici Paesi dell'Ue hanno provveduto in tutto o in parte all'attuazione della direttiva n. 95/46/CE. La Francia, pur non avendo ancora completato l'*iter* parlamentare per l'adozione della legge nazionale di recepimento, ha comunicato alla Commissione europea l'approvazione della legge "Informatica e libertà", la quale, nonostante risalga al gennaio del 1978, contiene principi analoghi a quelli introdotti dalla direttiva.

Presentiamo di seguito la tabella riassuntiva delle normative nazionali adottate dai Paesi dell'Unione.

Tabella di recepimento della direttiva 95/46/CE – aprile 2004

Stato	Normativa nazionale di recepimento	Entrata in vigore
AUSTRIA	Datenschutzgesetz 2000 (legge sulla tutela dei dati 2000) del 17 agosto 1999	1° gennaio 2000
BELGIO	Legge dell'8 dicembre 1992 sulla tutela della *privacy* nel trattamento di dati personali, come modificata dalla legge 11 dicembre 1998 di trasposizione della direttiva n. 95/46/CE	1° settembre 2001
DANIMARCA	Legge n. 429 del 31 maggio 2000	1° luglio 2000
FINLANDIA	Legge n. 523/99	1° giugno 1999
GERMANIA	Bundesdatenschutzgesetz (legge federale sulla protezione dei dati) del 23 maggio 2001 e successive modificazioni	23 maggio 2001
FRANCIA	Legge su informatica e libertà del 6 gennaio 1978 e successive modificazioni (sono previsti emendamenti per recepire integralmente la direttiva)	Progetto di legge (Petite Loi) di recepimento approvato dalla Assemblea Nazionale il 30 gennaio 2002, modificato dal Senato il 1° aprile 2003
GRECIA	Legge n. 2472 del 10 aprile 1997 (Protezione delle persone rispetto al trattamento di dati personali)	10 novembre 1997
IRLANDA	Data Protection (Amendment) Act 2003 del 10 aprile 2003, che modifica il Data Protection Act (legge sulla protezione dei dati) del 13 luglio 1988. (Gli artt. 4, 17, 25 e 26 della direttiva erano stati attuati con regolamento approvato il 19 dicembre 2001)	1° luglio 2003 (alcune norme sono entrate in vigore successivamente) 1° aprile 2002

/ segue

Stato	Normativa nazionale di recepimento	Entrata in vigore
ITALIA	Legge 31 dicembre 1996, n. 675, e successive modificazioni (abrogata dal 1° gennaio 2004); decreto legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali")	8 maggio 1997 1° gennaio 2004
LUSSEMBURGO	Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel	1° dicembre 2002
PAESI BASSI	Wet bescherming persoonsgegevens (legge per la tutela dei dati personali) del 6 luglio 2000	1° marzo 2001
PORTOGALLO	Legge sulla protezione dei dati n. 67/98, del 26 ottobre 1998	27 ottobre 1998
REGNO UNITO	Data Protection Act 1998 (legge sulla protezione dei dati 1998) e legislazione secondaria (regolamenti di attuazione)	1° marzo 2000
SPAGNA	Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (legge organica 15/1999, del 13 dicembre, sulla protezione dei dati personali)	14 gennaio 2000
SVEZIA	Personuppgiftslagen (1998:204) (legge sui dati personali del 29 aprile 1998) integrata dall'ordinanza sui dati personali (1998:1191) del 3 settembre 1998	24 ottobre 1998

4.2. Il recepimento delle direttive n. 97/66/CE e n. 2002/58/CE

La direttiva n. 2002/58/CE relativa alla vita privata ed alle comunicazioni elettroniche (i cui tratti salienti sono già stati rappresentati nella *Relazione* per il 2002, p. 106 s.), con la quale si è sostituita la direttiva n. 97/66/CE sulla protezione dei dati nel settore delle telecomunicazioni, è stata tempestivamente recepita con il d.lg. n. 196/2003 (Titolo X, artt. 121-132. Delle modifiche all'art. 132 apportate con il d.l. n. 354 del 24 dicembre 2003, convertito in l. 26 febbraio 2004, n. 45, si è già ampiamente fatto cenno *supra*, a parag. 1.11.).

Altri cinque Paesi dell'Ue hanno emanato norme nazionali di recepimento entro il termine del 31 ottobre 2003 (Austria, Danimarca, Irlanda, Regno Unito e Spagna).

L'art. 13 della direttiva n. 2002/58/CE

Il 5 dicembre 2003 la Commissione europea ha attivato le iniziative preliminari all'avvio della procedura di infrazione nei confronti di alcuni Stati (Belgio, Finlandia, Francia, Germania, Grecia, Lussemburgo, Paesi Bassi, Portogallo, Svezia), per la mancata comunicazione delle norme nazionali adottate nel settore delle comunicazioni elettroniche. Il Portogallo ha successivamente emanato un decreto legge (n. 7/2004 del 7 gennaio 2004) con cui ha recepito la disposizione (art. 13) della predetta direttiva che fissa il principio del consenso preventivo per le comunicazioni indesiderate; inoltre, l'iniziativa avviata nei confronti della Svezia si riferisce esclusivamente al mancato recepimento del medesimo art. 13, dal momento che le altre disposizioni erano già state attuate nell'ordinamento interno e la relativa comunicazione era pervenuta alla Commissione nei termini stabiliti.

Il 1° aprile 2004 la Commissione ha emesso un parere motivato (seconda fase del procedimento di infrazione) nei confronti dei suddetti Paesi, ad eccezione della Svezia, che ha nel frattempo provveduto a recepire l'art. 13. Il parere prevede un termine di due mesi per l'adeguamento, scaduto il quale la Commissione procede alla presentazione del ricorso alla Corte di giustizia.

Tabella di recepimento della direttiva n. 2002/58/CE - aprile 2004

Stato	Normativa nazionale di recepimento
AUSTRIA	Art. 107 Telekommunikationsgesetz 2003 (legge sulle telecomunicazioni: introduce, in particolare, l'obbligo del consenso preventivo) Artt. 6-8 E-Commerce-Gesetz 2001 (legge sul commercio elettronico: prevede la possibilità per l'abbonato di farsi inserire in un elenco di soggetti che rifiutano la ricezione di messaggi commerciali) Art. 12 Wertpapieraufsichtsgesetz 1996 (legge per il controllo sui titoli monetari)
DANIMARCA	Marketing Practices Act (n. 699 del 17 luglio 2000, modificato dalla legge 428 del 6 giugno 2002 e, per quanto riguarda parte della direttiva n. 2002/58/CE, dalla legge 450 del 10 giugno 2003)
IRLANDA	European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003 (entrato in vigore il 6 novembre 2003)
ITALIA	Decreto legislativo n. 196 del 30 giugno 2003 ("Codice in materia di protezione dei dati personali")
REGNO UNITO	Privacy and Electronic Communications (EC Directive) Regulations 2003 (entrato in vigore l'11 dicembre 2003)
SPAGNA	Ley 32/2003 del 3 novembre 2003 (Legge generale sulle telecomunicazioni)

5 Il primo rapporto sull'attuazione della direttiva europea in materia di protezione dei dati

Il 15 maggio 2003 la Commissione europea ha pubblicato il primo rapporto sullo stato di attuazione della direttiva n. 95/46/CE. Il documento, sulla base della consultazione pubblica tenutasi nel 2002 (nella quale oltre diecimila soggetti hanno fatto pervenire le proprie osservazioni), nonché delle osservazioni giunte dagli Stati membri e dalle autorità nazionali di controllo, traccia un bilancio positivo dell'applicazione della direttiva escludendo, allo stato attuale, l'opportunità di una sua revisione; posizione, questa, che la Commissione sottolinea essere condivisa dalla maggioranza degli Stati e delle predette autorità.

Difficoltà segnalate

Nel rapporto sono anche evidenziate alcune difficoltà di applicazione omogenea dei principi della direttiva che sarebbero riconducibili a talune divergenze nelle legislazioni di recepimento, ad una ridotta sensibilizzazione dell'opinione pubblica (come risulta da una recente indagine condotta da Eurobarometro), ad un'imperfetta osservanza delle disposizioni nazionali da parte dei titolari del trattamento e all'asserita onerosità di talune disposizioni nazionali sulla notificazione e sul trasferimento dei dati verso Paesi terzi.

Trattamento dei dati in forma di immagini e suoni

Infine, si mettono in luce alcuni profili problematici rispetto al trattamento dei dati in forma di suoni ed immagini. Per ciascun aspetto, il rapporto propone alcune strategie di intervento nell'ambito di un vero e proprio "Piano di lavoro" la cui attuazione è prevista per la fine del 2004. Nel 2005 la Commissione intende esaminare nuovamente lo stato di applicazione della direttiva valutando anche, alla luce della maggiore esperienza acquisita, l'eventuale necessità di introdurre misure ulteriori.

6 La protezione dei dati nell'Ue secondo l'Eurobarometro

Come appena accennato, nel febbraio del 2004 sono stati resi noti i risultati dell'indagine condotta da Eurobarometro per conto della Commissione, riguardante l'applicazione delle norme sulla *privacy* previste dalla direttiva n. 95/46/CE.

Il documento comprende due sezioni dedicate l'una ad aziende e imprese quali titolari di trattamento e, l'altra, ai cittadini interessati dal trattamento di dati personali.

Aziende e imprese

I risultati dell'indagine (tra i quali si evidenzia la posizione positiva dell'Italia) offrono un panorama vario della protezione dei dati personali in Europa. Oltre il 60% dei cittadini dell'Ue afferma di nutrire preoccupazioni forti o molto forti sulla tutela della *privacy*. Tutte le imprese che raccolgono, utilizzano e conservano dati personali giudicano positivamente l'esistenza di norme comunitarie e nazionali in materia, ma quasi la metà ritiene insufficiente l'armonizzazione a livello comunitario. Diversa è anche la valutazione riferita al livello di tutela offerto dalla rispettiva legge nazionale ed agli obblighi che quest'ultima impone. Dal lato degli utenti, invece, si lamenta un rispetto insufficiente delle disposizioni sull'informativa da parte delle imprese e la scarsa conoscenza delle norme fra piccole imprese.

Cittadini

Per quanto riguarda i cittadini interpellati, un terzo degli intervistati è a conoscenza dei diritti loro riconosciuti dalle discipline di protezione dei dati e degli obblighi di trasparenza in capo ai titolari del trattamento. Nonostante ciò, la stragrande maggioranza degli interpellati ritiene che sia giusto ottenere queste informazioni e, soprattutto, conoscere se i dati che li riguardano siano diffusi o comunicati a terzi e per quali finalità.

La situazione italiana

In relazione al livello di conoscenza e di applicazione delle norme sulla protezione dei dati, i cittadini italiani risultano essere i più informati sui propri diritti e sull'esistenza di un'autorità indipendente; le imprese italiane ritengono più delle altre (61%) che sia stata raggiunta un'effettiva armonizzazione a livello comunitario e risultano più rispettose delle prescrizioni legate al dovere di informativa degli interessati. Ancorché oltre il 75% di esse si identifichi chiaramente come titolare del trattamento e rappresenti agli interessati le finalità del trattamento posto in essere, molte imprese manifestano ancora la necessità di maggiori chiarimenti sull'applicazione delle norme. Altro elemento importante è che la percentuale dei cittadini particolarmente preoccupati per la propria *privacy* è scesa in Italia dal 47% del 1991, quando mancava una legislazione specifica nazionale, al 14% del 2003.

II - I diritti dell'interessato I doveri del titolare

I diritti

7 Diritto di accesso

7.1. Rapporto di lavoro

Con due decisioni del 28 marzo 2003, il Garante ha esaminato i ricorsi di due lavoratori che si erano rivolti all'Autorità lamentando l'incompletezza del riscontro fornito dal loro ex datore di lavoro ad istanze di accesso ai dati personali riguardanti, tra l'altro, le ragioni del loro trasferimento ad altro reparto. Il titolare del trattamento ha risposto in entrambi i casi di aver comunicato ai richiedenti tutti i dati personali detenuti nei propri archivi e di non considerarsi obbligato a creare appositamente altri dati, per soddisfare ulteriori e diverse esigenze informative dei richiedenti stessi.

L'Autorità ha ritenuto la risposta della società conforme alla disciplina vigente in tema di tutela dei dati personali, che attribuisce al lavoratore il diritto di accedere ai propri dati personali detenuti dal datore di lavoro e di ottenerne la comunicazione in forma intelligibile e completa, ma non di ottenere la creazione di dati inesistenti o la loro approfondita rielaborazione secondo criteri indicati dal lavoratore medesimo.

Un'altra pronuncia del Garante (*Provv.* 2 luglio 2003) ha avuto origine dal ricorso di un ex dipendente che ha lamentato il mancato riscontro da parte del datore di lavoro ad un'istanza di accesso ai dati personali che lo riguardavano contenuti in documenti riferiti ad un intervallo temporale di circa trenta anni. Rilevato che il riscontro da fornire all'interessato era particolarmente complesso (i dati richiesti riguardavano sia un periodo risalente nel tempo, sia un rapporto di lavoro cessato da diversi anni, sia, infine, un datore di lavoro che aveva subito numerose trasformazioni nel proprio assetto societario), il titolare del trattamento si era limitato a manifestare solo una generica disponibilità a fornire i dati richiesti. L'Autorità ha ritenuto che la società resistente avrebbe dovuto adoperarsi per un riscontro più idoneo e tempestivo e le ha quindi assegnato un termine breve per provvedere a quanto non correttamente omesso.

Dati riferibili a persone identificate o identificabili

Sempre con riferimento al diritto di accesso del lavoratore ai dati che lo riguardano, il Garante ha stabilito (*Provv.* 29 ottobre 2003) che non rientra nell'ambito di applicazione della normativa sulla protezione dei dati personali la richiesta di conoscere unicamente mere notizie di carattere contrattuale o professionale (ad es. gli accordi collettivi nazionali o aziendali), che non sono in nessun modo riferibili a persone identificate o identificabili.

Il diritto di accesso consente, infatti, al lavoratore di conoscere tutti i dati che lo riguardano detenuti dal proprio datore di lavoro, ma non può essere esercitato per

apprendere notizie impersonali che non siano riferibili ad un interessato identificato o identificabile.

7.2. Accesso ai dati per ragioni di giustizia

Il Garante ha nuovamente rilevato, in occasione di una decisione su un ricorso presentato nei confronti di un ufficio giudiziario (procura della Repubblica), che ai trattamenti effettuati per "ragioni di giustizia" (v., ora, art. 47 d.lg. n. 196/2003) alcune disposizioni in materia di protezione dei dati personali non sono applicabili o sono applicate con alcuni adattamenti.

Modalità di esercizio dei diritti

In particolare, non è previsto l'esercizio in forma diretta del diritto di accesso e degli altri diritti degli interessati, né la presentazione di un ricorso all'Autorità. È invece possibile esercitare tali diritti in forma diversa dalla richiesta rivolta al titolare o al responsabile del trattamento, presentando un'istanza al Garante per sollecitare la verifica della conformità del trattamento ai requisiti stabiliti (*Provv.* 5 novembre 2003).

Il Codice ha poi confermato l'inesperibilità del ricorso al Garante, prevedendo che il diritto di accesso e gli altri diritti degli interessati possano essere esercitati anche nei confronti dei trattamenti effettuati per "ragioni di giustizia" attraverso una segnalazione a questa Autorità. Le diverse modalità di esercizio dei diritti non incidono, quindi, sul sostanziale livello di tutela garantito agli interessati, poiché il Garante mantiene il potere di verificare la liceità e la correttezza dei trattamenti, con modalità peraltro adeguate alla specificità del contesto in cui questi sono effettuati, ovvero nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo giudiziario procedente (artt. 8, 47 e 160 d.lg. n. 196/2003).

7.3. Associazioni

Nel 2003 sono pervenute numerose segnalazioni relative all'accesso, da parte di soci o iscritti, a dati personali di altri aderenti ad un ente o associazione.

Dati non sensibili degli associati

Come in passato, l'Ufficio del Garante ha evidenziato che il trattamento dei dati personali non sensibili degli associati è consentito senza il loro consenso quando persegue finalità lecite sulla base di quanto previsto dall'atto costitutivo o dallo statuto dell'associazione o ente, oppure se ricorre uno degli ulteriori presupposti del trattamento equipollenti al consenso, previsti dalla normativa vigente (ad esempio, per adempiere ad un obbligo di legge o per esigenze di difesa di un diritto in sede giudiziaria).

Tale impostazione è stata ribadita dal Codice con riferimento al trattamento dei dati effettuato da associazioni od organismi senza scopo di lucro, anche non riconosciuti, in riferimento agli aderenti ed ai soggetti che con essi hanno contatti regolari (artt. 24, comma 1, lett. *b)* e 26, comma 4, lett. *a)*, d.lg. n. 196/2003).

7.4. Dati di traffico: fatturazione dettagliata

Il Garante ha ribadito la piena applicabilità dell'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) alle informazioni incluse nella fatturazione, trattandosi di dati di carattere personale. In particolare, con una decisione del 30 aprile 2003

l'Autorità, nell'accogliere un ricorso, ha ordinato ad un fornitore di servizi di telecomunicazione di comunicare gratuitamente al ricorrente i dati di traffico "in uscita" con l'indicazione integrale delle cifre dei numeri chiamati, che nel caso di specie erano relativi ad una carta prepagata intestata all'interessato.

Chiamate "in uscita"

Non possono, invece, trovare accoglimento le richieste, rivolte ai gestori telefonici, di conoscere gli estremi identificativi e gli indirizzi dei soggetti cui corrispondono i numeri telefonici riportati nel tabulato delle chiamate "in uscita" (*Provv.* 22 settembre 2003). Esercitando il diritto di accesso, l'interessato può infatti conoscere i dati personali che lo riguardano, ma non può chiedere di acquisire dati e informazioni relativi a terzi, come ora precisa espressamente il Codice (art. 10, comma 5, d.lg. n. 196/2003).

Sempre con riferimento alle chiamate "in uscita", l'Autorità ha precisato che il titolare deve fornire idoneo riscontro soltanto alle istanze di accesso formulate dalla persona cui si riferiscono i dati personali oggetto della richiesta. In un caso è stato, pertanto, ritenuto illecito il riscontro fornito dal titolare ad un'istanza di accesso presentata da una persona che non risultava essere il reale utilizzatore dell'utenza telefonica (*Provv.* 30 dicembre 2003).

Con decisione del 13 novembre 2003, il Garante ha altresì chiarito che l'accesso dell'interessato deve essere garantito anche nei confronti dei dati relativi a chiamate verso numeri a tariffazione speciale (ad es., quelli che iniziano con il prefisso "709").

7.5. Dati di traffico: chiamate in entrata e chiamate di disturbo

La problematica dei giusti limiti da porre all'esercizio del diritto d'accesso ai dati identificativi delle cd. chiamate in entrata ha trovato una soluzione di conferma nel Codice, il quale precisa che l'accesso a tali dati non è previsto per esercitare un diritto in sede civile ed è lecito soltanto quando, omettendo di darne comunicazione, si determinerebbe un pregiudizio "effettivo e concreto" per lo svolgimento delle investigazioni difensive in ambito penale (art. 8, comma 2, lett. *f)*, d.lg. n. 196/2003; l. 7 dicembre 2000, n. 397).

Questa previsione del Codice, come ha nuovamente constatato l'Autorità con una decisione del 18 febbraio 2004, traccia un bilanciamento tra il diritto dell'interessato ad accedere ai dati che lo riguardano e il diritto alla riservatezza di terzi (gli utenti-persone fisiche chiamanti e i soggetti chiamati), circoscrivendo il diritto di accesso alle sole comunicazioni "in entrata" di cui sia realmente necessaria la conoscenza, negando le quali si arrecherebbe un pregiudizio reale per lo svolgimento delle investigazioni difensive, che deve risultare comprovato, in concreto, caso per caso.

Anche con riferimento alle chiamate in entrata, è stato ribadito che il diritto d'accesso può essere esercitato dall'interessato soltanto nei confronti dei dati che lo riguardano. Nel decidere su un ricorso, il Garante ha pertanto dichiarato inammissibile la richiesta volta ad identificare utenze diverse da quella dell'interessato (e le relative coordinate delle chiamate), da cui erano originate alcune chiamate effettuate a nome di quest'ultimo verso il *call-center* di una società di telefonia mobile (*Provv.* 5 novembre 2003).

Riguardo, invece, all'accesso alle chiamate di disturbo, specie quando non sia possibile identificare sull'apparecchio la linea chiamante, il Codice conferma il diritto dell'abbonato di richiedere al fornitore del servizio di rendere temporaneamente inefficace la soppressione dell'identificazione della linea chiamante (e di conservare i dati relativi alla provenienza della chiamata ricevuta) e riconosce espressamente il diritto di venirne a conoscenza (art. 127 d.lg. n. 196/2003).

7.6. Messaggi di posta elettronica indesiderati

Anche al destinatario di messaggi di posta elettronica non sollecitati sono riconosciuti i diritti di cui all'art. 7 del Codice, fra i quali il diritto di conoscere da quale fonte siano stati ricavati i propri dati, di far interrompere in qualsiasi momento la loro ulteriore utilizzazione a fini commerciali o pubblicitari e, ancora, di far cancellare quelli trattati in violazione di legge.

Ferma restando la tutela che su un altro piano, quello penalistico, è data dalla natura di reato dello *spamming* (art. 167 del Codice), l'interessato può, gratuitamente e senza particolari formalità, rivolgere comunque un'esplicita richiesta al mittente del messaggio indesiderato e, ove non riceva un soddisfacente riscontro nel termine di quindici giorni (o di trenta giorni, se sono necessarie operazioni di particolare complessità), può rivolgersi all'autorità giudiziaria ordinaria oppure proporre ricorso al Garante (che resta incompetente riguardo ad eventuali pretese risarcitorie del danno subito).

Accesso ai dati relativi ai terzi

Negli innumerevoli ricorsi esaminati in materia di *spamming* l'Autorità ha peraltro precisato che l'esercizio del diritto di accesso e la successiva proposizione di un ricorso al Garante non sono consentiti con riferimento a dati personali relativi a terzi. Sono stati pertanto dichiarati inammissibili alcuni ricorsi, una volta accertata la loro proposizione da parte di soggetti privi della relativa legittimazione, in quanto si trattava di persone diverse da quelle cui erano riferiti i dati concernenti gli indirizzi di posta elettronica dei quali era stato lamentato l'illecito trattamento (*Provv.* 25 luglio, 5 e 16 dicembre 2003).

7.7. Credito

Con riferimento al trattamento dei dati personali in ambito bancario, un profilo delicato ha riguardato l'esercizio del diritto di accesso ai dati personali di persone decedute, il quale è qui approfondito in un apposito paragrafo (cfr. subito parag. 7.10.).

Gratuità del riscontro all'interessato

Per quanto concerne la disciplina del diritto di accesso dell'interessato ai dati personali che lo riguardano detenuti da istituti di credito, va ricordato che il titolare è tenuto ad assicurare un riscontro gratuito alle richieste di accesso rivoltegli dagli interessati.

In alcune occasioni, taluni istituti di credito hanno invece subordinato tale riscontro al versamento, da parte del cliente, di somme occorrenti per ricercare e mettere a disposizione i documenti richiesti: ciò per far fronte alle spese che gli istituti sostenevano di dover affrontare per il reperimento dei dati e la loro comunicazione all'interessato.

Tale comportamento è stato giudicato illegittimo dal Garante in alcune decisioni su ricorsi (*Newsletter* n. 199, 3-9 novembre 2003; v. anche *Provv.* 10 dicembre 2003) poiché, nel vigore della legge n. 675/1996, il contributo spese poteva essere richiesto all'interessato solo nel caso in cui presso il titolare non fosse risultata confermata l'esistenza di suoi dati personali. Pertanto, si è affermato che l'esercizio del diritto di accesso vantato dal ricorrente doveva essere garantito gratuitamente e non poteva essere condizionato, nelle sue modalità di esercizio, a quanto stabilito, a ben altri fini, dal testo unico in materia bancaria e creditizia (d.lg. n. 385/1993). È stato quindi ordinato alle banche resistenti di estrarre dagli atti e dai documenti da essa detenuti tutte le informazioni personali richieste, concernenti le movimentazioni effettuate, e di comunicarle in breve termine agli interessati in modo intelligibile.

7.8. "Centrali rischi" private

Al Garante sono pervenute ancora numerose richieste da parte di cittadini per il tramite di associazioni e studi legali, indirizzate direttamente o per semplice conoscenza all'Autorità ed aventi ad oggetto l'esercizio dei diritti di cui all'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) in merito al trattamento dei dati da parte delle "centrali rischi" private. Sul punto si è ribadito che gli interessati possono rivolgersi direttamente al titolare o al responsabile del trattamento dei dati al fine di esercitare i diritti in esame, non risultando indispensabile, nella prima fase di questo interpello, rivolgersi subito al Garante, anche solo per conoscenza.

"Messa in chiaro" dei dati

In numerosi casi, i riscontri forniti alle richieste di accesso rivolte a banche e società finanziarie sono risultati lacunosi, in quanto limitati alla comunicazione dei dati solo per categorie od a un semplice rinvio agli estratti conto forniti mensilmente, senza nessun riferimento alle "centrali rischi". Al riguardo l'Autorità ha ripetutamente invitato le società ad integrare i riscontri già forniti in modo generico, provvedendo alla "messa in chiaro" di tutte le notizie di carattere personale oggetto di trattamento relative anche ai rapporti finanziari con i clienti, pur se provenienti da "centrali rischi". Di queste ultime, infatti, nella modulistica relativa ai contratti di finanziamento anteriori al provvedimento generale del Garante del 31 luglio 2002, spesso non sono indicati i puntuali estremi identificativi e i recapiti.

Credit scoring

Anche il riscontro fornito dalle "centrali rischi" in caso di accesso esercitato direttamente nei loro confronti è risultato in più casi parziale e insoddisfacente. Ad esempio, una società non aveva comunicato, come invece specificamente richiesto dall'interessato, i dati personali detenuti in forma di punteggi sul grado di affidabilità/solvibilità, qualificati genericamente come "indicatori numerici o punteggi diretti a fornire una rappresentazione sintetica, in termini predittivi o probabilistici, del complessivo profilo di rischio di un determinato interessato, della sua affidabilità o solvibilità". Pertanto, la società è stata invitata ad integrare la risposta fornita con riferimento all'integralità dei propri archivi, comunicando tutti gli ulteriori dati personali relativi all'interessato, anche se appunto espressi in forma di punteggio (cd. *credit scoring*, v. *Provv.* 29 dicembre 2003).

7.9. Assicurazioni

In ambito assicurativo, l'Autorità ha ribadito il principio che le informazioni personali comprese nelle valutazioni e negli altri elementi di giudizio riportati nelle perizie medico-legali delle compagnie di assicurazione rientrano nella sfera dei dati

personali e vanno pertanto comunicate all'interessato quando questi ne faccia richiesta: così nel caso del cittadino che, a seguito di un sinistro di cui era rimasto vittima, si era rivolto all'impresa assicuratrice della controparte per avere conferma dell'esistenza di dati personali che lo riguardavano.

L'art. 8, comma 4, del Codice ha, poi, individuato opportune soluzioni in riferimento all'accesso a dati di tipo valutativo, relativi a giudizi, opinioni o altri apprezzamenti di tipo soggettivo, confermando però il diritto di accesso, che trova riconoscimento anche nel successivo regolamento sull'accesso agli atti delle imprese di assicurazione (art. 5 comma 2, d.m. 20 febbraio 2004, n.74).

Comunicazione all'interessato di dati sulla salute

Il Garante aveva inoltre riaffermato in passato che in caso di comunicazione all'interessato di dati che riguardano la sua salute acquisiti nell'ambito di una visita medica dal consulente sanitario della compagnia, tale comunicazione doveva avvenire per il tramite di un medico designato dall'interessato o dalla compagnia assicuratrice titolare del trattamento (*Provv.* 7 maggio 2003; *Newsletter* n. 195, 8-21 dicembre 2003); la questione è ora diversamente disciplinata dall'art. 84 del Codice.

Differimento temporaneo dell'accesso

Per altro verso, la normativa consente ancora al titolare del trattamento di differire temporaneamente l'esercizio del diritto di accesso, per il periodo durante il quale potrebbe derivargli un pregiudizio per lo svolgimento delle cd. indagini difensive o, comunque, per far valere o difendere un diritto in sede giudiziaria (*Provv.* 21 marzo 2003; *Provv.* 29 dicembre 2003). Come già osservato, la valutazione dell'esistenza di un effettivo pregiudizio, tale da giustificare il temporaneo differimento dell'accesso, deve essere effettuata caso per caso sulla base di elementi concreti allegati dal titolare del trattamento o comunque presenti in atti (v. ora art. 8, comma 2, lett. *e)*, del Codice).

7.10. Accesso ai dati di persone decedute

Uno degli aspetti più delicati affrontati nella materia dell'accesso ai dati personali è stato quello dell'accesso ai dati del defunto.

Settore bancario

La questione si è posta in primo luogo, come accennato, nel settore bancario. L'art. 13, comma 3, della legge n. 675/1996, riconosceva tale diritto a chiunque vi avesse interesse: in base a tale disposizione, si è ammesso il diritto degli eredi di accedere ai dati personali del defunto, inclusi eventuali dati riferiti a terzi (ad es., cointestatari del conto corrente o soggetti delegati ad operare sul conto medesimo), nel caso in cui quelli relativi all'interessato e le notizie relative a terzi fossero intrecciati al punto da rendere i primi, se presi isolatamente, incomprensibili, oppure snaturati nel loro contenuto (v. *Provv.* 8 ottobre 2003 e *Provv.* 10 dicembre 2003, che richiamano sul punto il *Provv.* 23 giugno 1998). Al contrario, non poteva essere accolta la richiesta di accesso a dati personali trattati da una banca e riferiti ad una persona deceduta, se volta a conoscere specificamente e direttamente l'identità della persona delegata dal defunto ad effettuare determinate operazioni bancarie (*Provv.* 13 novembre 2003).

La disposizione, come modificata dal Codice (v. l'art. 9, comma 3), specifica ora l'ambito dei soggetti legittimati ad accedere ai dati personali di persone decedute in favore di chi ha un interesse proprio, o agisce a tutela dell'interessato, o per ragioni familiari meritevoli di protezione.

Settore assicurativo

Nel 2003, il Garante è stato chiamato a pronunciarsi sulla questione dell'accesso ai dati relativi al defunto anche in ambito assicurativo: in proposito si è affermato che il diritto di accesso ai dati personali di un defunto non riguarda le informazioni relative a terzi, come ad es. i terzi beneficiari di polizze assicurative (*Provv.* 31 marzo 2003; *Provv.* 22 settembre 2003; *Provv.* 13 novembre 2003): pertanto, sebbene all'erede legittimo spetti il diritto ad accedere a tutte le informazioni personali che riguardano il defunto, non è tuttavia consentito alla società assicuratrice di comunicargli il nome del beneficiario della polizza.

Nei casi a suo tempo esaminati, l'Autorità ha riconosciuto legittima la richiesta di alcuni eredi di accedere ai dati personali riconducibili ai familiari deceduti, benché impropriamente formulata (sul piano della protezione dei dati personali), nella parte in cui si chiedeva l'accesso ad interi documenti detenuti dalle imprese di assicurazioni. La messa a disposizione dell'intera documentazione da parte del titolare del trattamento, in copia o in visione, può essere infatti disposta dal Garante, in applicazione del Codice, qualora sussistano reali, oggettive difficoltà di estrapolazione dei dati richiesti all'interno di documenti, ed avendo comunque cura di oscurare i dati personali eventualmente riferiti a terzi. È stato quindi intimato alle società di estrarre dagli atti e dai documenti detenuti, comprese le eventuali polizze sottoscritte, tutte le informazioni personali relative al defunto, comunicandole in modo intelligibile all'erede legittimo, con esclusione di tutte le informazioni non direttamente riferite al medesimo defunto (e, quindi, nello specifico, non comunicando i dati personali relativi al beneficiario della polizza).

La tematica va ora considerata anche da un diverso angolo visuale, alla luce dell'ulteriore diritto di accesso agli atti delle imprese di assicurazione, disciplinato innovativamente dal già citato d.m. 20 febbraio 2004, n.74.

Un'altra questione ha riguardato la legittimità del rifiuto, opposto da un ufficio delle imposte, di rilasciare copia della dichiarazione dei redditi presentata, a suo tempo, da un parente deceduto del richiedente. In questo caso, il Garante ha riconosciuto al richiedente stesso il diritto di accedere ai dati personali relativi al congiunto deceduto contenuti nella dichiarazione dei redditi di quest'ultimo, ribadendo che tale diritto può essere esercitato da chiunque vi abbia interesse (*Nota* 12 febbraio 2004).

7.11. Giornalismo

Il Garante ha riaffermato il principio in base al quale i diritti di accesso e gli altri diritti ora previsti dall'art. 7 del Codice –esercitabili pure nei confronti degli editori e dei direttori responsabili delle testate giornalistiche (cfr. *Provv.* 26 marzo e 23 aprile 2003)– possono essere fatti valere anche in riferimento a fotografie e ad altri dati personali diffusi attraverso pubblicazioni consultabili via Internet (*Provv.* 8 ottobre 2003 e 8 gennaio 2004).

7.12. Rai

Con la decisione del 19 novembre 2003 è stata dichiarata inammissibile la richiesta dell'interessato volta a conoscere il nominativo della persona incaricata dalla Rai –Radiotelevisione Italiana S.p.A.– di effettuare una visita presso il domicilio dell'interessato stesso nell'ambito delle attività relative alla gestione e riscossione del canone di abbonamento. In proposito, va ricordato che l'art. 7, comma 2, lett. *e)*,

del Codice consente ora, all'interessato, di ottenere dal titolare anche l'indicazione dei soggetti che in qualità di responsabili o incaricati possono venire a conoscenza dei dati che lo riguardano.

8 Cancellazione dei dati

8.1. Cancellazione dei dati trattati dalla pubblica amministrazione

Il diritto ad ottenere la cancellazione dei dati personali trattati da una pubblica amministrazione ha formato oggetto di numerosi ricorsi.

Delibera di giunta comunale

Va ricordata in particolare la decisione su un ricorso con il quale era stata domandata la cancellazione di dati personali contenuti in una deliberazione di giunta comunale, affissa all'albo pretorio, che faceva riferimento ad una controversia in cui era coinvolto il ricorrente (*Provv.* 12 gennaio 2004).

L'Autorità non ha accolto la richiesta dell'interessato, ritenendo la diffusione dei dati che lo riguardavano necessaria allo svolgimento delle funzioni istituzionali dell'ente e conforme alle vigenti disposizioni sullo svolgimento dei procedimenti amministrativi e sulla pubblicazione degli atti (cfr. art. 124 d.lg. n. 267/2000). Nella deliberazione, peraltro, non venivano riportati dati di carattere giudiziario e le informazioni contenute risultavano esatte e non eccedenti rispetto all'esigenza di trasparenza delle deliberazioni comunali. Il Garante ha però riaffermato la necessità di rispettare i principi di pertinenza e non eccedenza, nel bilanciare le esigenze di riservatezza e di trasparenza dell'attività amministrativa.

Quesito referendario

Analogamente, è stata ritenuta infondata la richiesta volta ad eliminare dal testo di un quesito referendario (concernente il progetto di ristrutturazione di una scuola elementare), le generalità del ricorrente, lì indicate in quanto si trattava dell'autore di un progetto che era contestato nella vicenda referendaria. I dati in questione non sono stati ritenuti eccedenti rispetto alla finalità di illustrare l'iniziativa alla popolazione, considerata pure l'esattezza e l'obiettività con cui essi erano stati riportati, come anche l'ampia conoscibilità che queste informazioni avevano già avuto nella comunità locale (*Provv.* 25 settembre 2003).

8.2. Cancellazione dei dati concernenti i comportamenti debitori

La problematica dei limiti entro cui si può ottenere la cancellazione dei dati relativi ai comportamenti debitori si è posta più volte nel periodo considerato, con riferimento sia ai dati personali contenuti in banche dati pubbliche, sia a quelli registrati in banche dati private, "alimentate" peraltro con dati tratti da registri o elenchi accessibili a tutti.

Trascrizione di pignoramenti

Con riferimento all'esercizio dei diritti riconosciuti dalla normativa sulla protezione dei dati nei confronti dei pubblici registri immobiliari, l'Autorità, in una decisione del 30 dicembre 2003, ha affermato che la tutela della riservatezza non può essere invocata per ottenere la cancellazione di una trascrizione di pignoramento

immobiliare in difformità dalle specifiche ipotesi e particolari procedure previste dalla normativa di settore.

Su questa base il Garante ha giudicato infondato il ricorso presentato da un cittadino che lamentava di non aver ricevuto riscontro ad una sua istanza presentata all'Agenzia del territorio, nella quale aveva chiesto l'immediata cancellazione dei dati personali relativi una procedura esecutiva immobiliare promossa nei suoi confronti.

L'art. 2668 c.c. consente all'interessato di presentare domanda per la cancellazione delle trascrizioni quando ritiene che sussistano le condizioni per esercitare questo suo diritto. I competenti uffici possono apporre l'annotazione di cancellazione della trascrizione nel pubblico registro immobiliare solo dopo aver verificato la completezza della documentazione richiesta ed accertato la regolarità formale e sostanziale della domanda stessa.

Nel caso in esame, la richiesta di immediata cancellazione è stata quindi giudicata infondata, poiché non era emerso, da parte dell'Agenzia, un uso dei dati personali difforme dalla disciplina in materia, sia rispetto alle modalità di annotazione e tenuta dei registri immobiliari, sia rispetto alle formalità richieste dalla normativa per la cancellazione delle trascrizioni.

Banche dati private contenenti dati raccolti da elenchi pubblici

Sempre in materia di registri immobiliari, l'Autorità ha esaminato la richiesta di cancellazione di dati personali contenuti non in registri pubblici, bensì in banche di dati create e gestite da società private ed alimentate da informazioni estratte da fonti pubbliche accessibili da chiunque. La vicenda, sollevata in un ricorso, riguarda la problematica della pertinenza e completezza delle informazioni a contenuto economico in rapporto al diritto dell'interessato alla conservazione limitata nel tempo dei dati che lo riguardano, ossia per il tempo necessario al perseguimento delle finalità per le quali i dati stessi sono raccolti e successivamente trattati (art. 9 legge n. 675/1996; ora, art. 11 d.lg. n. 196/2003).

Nella decisione (*Provv.* 22 settembre 2003), il Garante ha ricordato che il trattamento di dati provenienti da pubblici registri può essere effettuato anche in assenza del consenso dell'interessato ed ha richiamato la disciplina introdotta in materia dal Codice, il quale, nel confermare la prossima adozione di un codice deontologico in materia, demanda a quest'ultimo il compito di individuare nuovi limiti temporali di conservazione dei dati relativi al comportamento debitorio (art. 119 d.lg. n. 196/2003).

Nelle more dell'adozione di tali fonti, il trattamento dei dati consistente nell'estrazione e comunicazione di informazioni accessibili a chiunque può ritenersi lecito; di qui l'infondatezza del ricorso, fermo restando il riconoscimento del diritto dell'interessato di ottenere, nei modi di legge, l'integrazione e/o l'aggiornamento delle informazioni che lo riguardano (per es., in ordine ad eventuali sentenze di riabilitazione pronunciate in suo favore).

Omonimie

Con un altro ricorso l'Autorità è stata chiamata a pronunciarsi su una richiesta di cancellazione di dati personali da un pubblico registro, motivata da una pretesa omonimia tra il ricorrente e il soggetto cui si riferivano i dati relativi ad un assegno protestato. Nel caso di specie non è stato possibile accertare inequivocabilmente nel procedimento se i dati riportati nell'elenco dei protestati corrispondessero a quelli

del ricorrente: tuttavia, nel disporre l'apertura di un autonomo procedimento, il Garante ha affermato che la situazione soggettiva dell'interessato doveva ritenersi comunque meritevole di tutela. Pertanto, l'Autorità ha disposto il blocco del trattamento effettuato dalla camera di commercio con riferimento alle informazioni che si contestava essere riconducibili al ricorrente, riservandosi ulteriori accertamenti sul punto (*Provv.* 12 gennaio 2004).

9 Opposizione al trattamento

9.1. Attività tributarie

Con importante decisione del 12 gennaio 2004, e in senso analogo a quanto disposto in passato, l'Autorità ha accolto l'opposizione di un contribuente alla comunicazione, da parte di una concessionaria provinciale del servizio riscossione tributi, di informazioni concernenti la posizione debitoria dell'interessato a terzi con i quali l'interessato stesso aveva intrattenuto rapporti professionali. La comunicazione veniva effettuata tramite l'invio a questi ultimi di una "richiesta di dichiarazione stragiudiziale" circa l'esistenza di eventuali crediti vantati dall'interessato nei loro confronti. Poiché tale particolare procedura è risultata non legittimata da alcuna specifica previsione normativa e non rispondente ai principi di pertinenza e non eccedenza dei dati rispetto alle finalità perseguite, nelle more degli ulteriori accertamenti (in corso) sulla questione è stato disposto, quale misura cautelare, il blocco dei dati oggetto di trattamento (cfr. *infra*, parag. 26.).

Diffusione degli elenchi dei contribuenti

In merito al regime di pubblicità dell'elenco dei contribuenti l'Autorità ha ribadito che non vi è incompatibilità tra la protezione dei dati personali e determinate forme di pubblicità di dati previste per finalità di interesse pubblico o della collettività. In particolare, con decisione del 2 luglio 2003, il Garante ha rilevato che la disciplina contenuta nel d.P.R. n. 600/1973 (art. 69), in base alla quale gli elenchi nominativi dei contribuenti che hanno presentato la dichiarazione dei redditi sono consultabili da chiunque presso alcuni uffici finanziari e i comuni interessati, non è stata abrogata, né modificata dalla disciplina sulle modalità di presentazione e trasmissione delle dichiarazioni per via telematica (d.P.R. 22 luglio 1998, n. 322). Pertanto, l'istanza di opposizione per motivi legittimi alla diffusione dei dati personali contenuti nelle dichiarazioni dei redditi attraverso la pubblicazione degli elenchi in questione non poteva essere accolta, poiché il regime di pubblicità previsto risponde ad una scelta normativa di carattere generale operata per favorire la trasparenza in materia di dati raccolti dalla pubblica amministrazione attraverso le dichiarazioni fiscali

9.2. Attività investigative

In una decisione dell'8 gennaio 2004 l'Autorità ha affrontato la questione della liceità del trattamento di dati personali contenuti nel materiale raccolto nell'ambito di indagini investigative e successivamente prodotto in un procedimento giudiziario.

In proposito, il Garante ha ribadito il principio in base al quale il trattamento dei dati a fini di esercizio di un diritto in sede giudiziaria è ammesso, anche in man-

canza del consenso dell'interessato, soltanto quando risulti strettamente "necessario" per la tutela del diritto esercitato. Una volta conclusa l'attività investigativa, il trattamento deve cessare in ogni sua forma, fatta salva l'immediata comunicazione dei dati al difensore o al soggetto che ha conferito l'incarico.

In particolare, nell'ambito di un procedimento di modifica delle condizioni economiche della separazione consensuale tra coniugi è stata ritenuta illecita la produzione di relazioni investigative e di fotografie, precedentemente commissionate ad un'agenzia d'investigazione, riguardanti una pretesa relazione extraconiugale mai stata oggetto di accertamento giudiziario.

9.3. Condominio

Nel 2003 sono stati esaminati dall'Autorità diversi ricorsi aventi ad oggetto il diritto di opposizione al trattamento di dati personali riguardanti situazioni di morosità di singoli condomini. Al riguardo, è stato ribadito che la normativa sulla protezione dei dati personali non ha modificato la disciplina sul condominio degli edifici prevista dal codice civile (art. 1117 s. c.c.), precisando che il condominio può tuttavia trattare solo i dati pertinenti e non eccedenti rispetto alle finalità di gestione. In particolare, i singoli condomini, che sono contitolari di un unico trattamento di cui l'amministratore ha la concreta gestione, hanno diritto di conoscere le informazioni utili riguardanti l'amministrazione ed il funzionamento del condominio, comprese quelle concernenti posizioni debitorie e creditorie dei condomini nei confronti del condominio stesso.

Comunicazione e diffusione dei dati sulle morosità dei condomini

Così, la comunicazione di informazioni relative alla morosità di un condomino nel corso dell'assemblea di condominio e la successiva trascrizione di queste informazioni in un verbale inviato ai soli condomini è stata giudicata dal Garante conforme ai principi di pertinenza e non eccedenza dei dati raccolti o successivamente trattati (*Provv.* 16 luglio 2003).

L'opposizione alla diffusione (tramite affissione nella bacheca condominiale) di dati personali concernenti presunte posizioni di morosità relative ad alcuni condomini è stata oggetto di un'ulteriore decisione dell'Autorità. In tale occasione, il Garante ha, però, ritenuto infondato il ricorso, in quanto l'istanza di opposizione era stata avanzata al titolare in un momento successivo alla rimozione dell'elenco dei morosi dalla bacheca condominiale (*Provv.* 19 novembre 2003).

I doveri

10 Rapporto di lavoro

Il Codice sulla protezione dei dati personali ha introdotto nel contesto lavorativo importanti novità ispirate, in particolar modo, alla semplificazione di alcuni adempimenti da parte del datore di lavoro. Ad esempio, per i dati sensibili, quando il trattamento è necessario per eseguire specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, non è più necessario acquisire il consenso scritto del lavoratore interessato, fermo restando il rispetto dell'autorizzazione del Garante e delle regole che saranno individuate mediante il codice di deontologia in materia di lavoro e previdenza (art. 26, comma 4, lett. *d)*, d.lg. n. 196/2003).

Raccordo con il d.lg. n. 276/2003

A prescindere dagli sviluppi a breve termine di tale codice deontologico, questo nuovo quadro normativo va peraltro raccordato con i recenti mutamenti introdotti dal d.lg. n. 276/2003 in attuazione delle deleghe in materia di occupazione e mercato del lavoro di cui alla legge n. 30/2003 (cd. riforma Biagi).

Sotto questo profilo, assume rilievo, in primo luogo, la previsione di un ulteriore divieto di indagini sulle opinioni e trattamenti discriminatori (art. 10 d.lg. n. 276/2003), sul quale sono già state avanzate all'Autorità richieste di chiarimenti da parte di talune organizzazioni sindacali. Rilevano inoltre la disposizione sull'ambito di diffusione dei dati relativi all'incontro tra domanda ed offerta di lavoro (art. 8 d.lg. n. 276 cit.) e quella sulle comunicazioni a mezzo stampa, Internet, televisione o altri mezzi di informazione (art. 9 d.lg. n. 276 cit.).

In particolare, con quest'ultima disposizione è stato recepito, a livello normativo, il consolidato orientamento dell'Autorità in materia di modalità dell'informativa ai candidati interessati ad una selezione o ricerca di personale, che deve essere in sostanza resa, sin dal momento della pubblicazione degli annunci di lavoro (cfr. *Provv.* 10 gennaio 2002).

Settori di intervento

Tra i diversi settori in cui l'Autorità è dovuta intervenire, vanno ricordati poi: il controllo a distanza dei lavoratori a mezzo di apparecchiature di videosorveglianza; le modalità di custodia e conservazione dei dati dei dipendenti a cura dei datori di lavoro; l'accesso dei lavoratori ai dati che li riguardano.

In relazione al divieto di controllo a distanza dei lavoratori, l'Autorità ha curato vari approfondimenti e si pronuncerà a breve con un provvedimento di carattere generale concernente le verifiche effettuate dai datori di lavoro sull'uso, da parte dei lavoratori, degli strumenti informatici e telematici loro assegnati per ragioni di servizio e, in particolare, sulle navigazioni in Internet e sulla gestione della posta elettronica.

Sul piano del contenzioso al riguardo merita di essere ricordata la delicata questione, portata all'attenzione del Garante, dell'impugnativa (da parte del dipendente

di una banca) di un licenziamento disciplinare motivato dall'uso irregolare delle infrastrutture informatiche fornitegli quali strumenti di lavoro.

In particolare, a fronte della domanda del lavoratore di tutela d'urgenza avverso il licenziamento, la banca ha sostenuto l'assenza di *periculum in mora* per l'avvenuta corresponsione del trattamento di fine rapporto. Tra il materiale probatorio prodotto in proposito, la banca ha tuttavia inserito anche la documentazione di cui aveva la disponibilità in qualità di parte non del rapporto di lavoro, bensì del rapporto di conto corrente che era stato instaurato con il medesimo dipendente.

L'Ufficio ha pertanto deciso di verificare in tempi brevi il rispetto, nel caso di specie, sia dei principi pertinenza e non eccedenza dei dati utilizzati e di liceità e correttezza del trattamento, sia delle norme in tema di informativa, consenso e relativi casi di esclusione (artt. 11, 13, 23 e 24 d.lg. n. 196/2003).

Eguale urgente approfondimento istruttorio è stato disposto sull'avvenuta conoscenza, da parte di alcuni dipendenti della medesima banca, dei dati personali dell'interessato emersi nell'ambito delle attività ispettive svolte nei suoi confronti, nonché sulle misure di sicurezza adottate con riferimento alle informazioni contenute nei documenti ed altri supporti presi in custodia in esito a tali attività.

Vari sono stati, poi, i reclami inviati al Garante da parte di organizzazioni sindacali (in particolare a livello aziendale), in merito all'installazione di impianti di videosorveglianza sul luogo di lavoro. In molti casi (riguardanti, soprattutto, apparecchiature installate a protezione del patrimonio aziendale, ma che riprendono anche postazioni di lavoro dei dipendenti), sono state impartite indicazioni ai datori di lavoro ai fini del pieno rispetto delle vigenti disposizioni in materia e del primo "decalogo" del Garante (v. la parte di *Relazione* inerente alla sorveglianza e ai sistemi biometrici: parag. 37.-38.).

È poi da segnalare, tra gli altri, un caso relativo alla modalità di recapito, da parte di un'azienda, di una comunicazione di contestazione disciplinare al domicilio privato di un dipendente, contenuta in un foglio ripiegato per errore in modo da rendere possibile la conoscenza dell'oggetto della lettera.

Il datore di lavoro è stato richiamato ad impartire precise istruzioni a tutti gli uffici e dipendenti incaricati di analoghi trattamenti di dati, al fine di assicurare una corretta applicazione della disciplina sulla protezione dei dati personali e garantire la riservatezza di comunicazioni contenenti dati relativi ai lavoratori interessati, in particolare per evitare la conoscenza, anche casuale, alle informazioni riportate al loro interno da parte di terzi estranei.

Cedolini delle buste paga

Il Garante è tornato ad occuparsi anche della questione relativa alla modalità di redazione e consegna dei cedolini delle buste paga ai dipendenti. Con decisione del 16 luglio 2003, l'elaborazione e la consegna dei cedolini in busta chiusa sigillata da parte di appositi incaricati del trattamento è stata ritenuta conforme ai principi della disciplina sulla protezione dei dati personali.

Indirizzo *e-mail* aziendale dell'ex dipendente

Infine, il Garante si è pronunciato sull'istanza volta a ottenere la chiusura dell'indirizzo di posta elettronica aziendale attivato a nome di un ex dipendente durante il rapporto di prestazione d'opera con una società. L'Autorità, ritenendo la

richiesta rilevante anche quale sostanziale opposizione per motivi legittimi, ha giudicato soddisfacente il riscontro fornito all'interessato da parte dell'ex datore di lavoro: quest'ultimo aveva infatti creato un nuovo indirizzo *e-mail* ed aveva inserito all'indirizzo dell'interessato un messaggio di risposta automatica che dava comunicazione dell'avvenuta disattivazione della casella di posta oggetto di contestazione (*Provv.* 22 dicembre 2003).

11 Sicurezza dei dati e dei sistemi

E-banking

Nel periodo di riferimento l'Autorità si è occupata di un caso assai significativo per la materia in esame, relativo alla sicurezza dei dati personali concernenti i rapporti bancari con i clienti, trattati da un istituto di credito nell'ambito di servizi di *e-banking*.

Il caso ha suscitato viva attenzione nel settore bancario e spiega effetti rilevanti, come caso pilota, per il livello di futuro sviluppo e di affidabilità dei servizi bancari prestati per via telematica.

È infatti accaduto che un cliente, il quale usufruiva di questi servizi via Internet, dopo un primo accesso ai dati che lo riguardavano, ricollegandosi a distanza di poco tempo al sito per controllare nuovamente la propria posizione contabile, si è trovato accidentalmente a consultare anche *file* relativi a conti correnti di altri clienti. I dati in tal modo visualizzati e memorizzati in appositi prospetti riguardavano operazioni bancarie, inclusi i numeri di conto corrente o delle carte di pagamento utilizzate per effettuare le singole transazioni (nonché, a volte, i dati dei relativi titolari), e recavano l'indicazione del pagamento di utenze domiciliate, tasse, imposte e persino emolumenti erogati da datori di lavoro. In molti casi le informazioni riguardavano anche familiari dei titolari dei conti correnti oggetto dell'accidentale consultazione, nonché terzi con i quali i correntisti avevano effettuato singole transazioni bancarie.

La banca ha fornito alcune giustificazioni sostenendo, tra l'altro, che l'unico caso di accesso indebito era stato quello oggetto di segnalazione, e che esso si era verificato solo per un breve arco temporale.

Il Garante, a conclusione di complesse verifiche, ha invece rilevato che l'erronea configurazione del sistema e dei programmi per l'accesso al servizio di *e-banking* aveva violato l'obbligo di garantire la riservatezza dei dati personali relativi a numerosi clienti e la loro protezione da accessi non autorizzati, con un abbassamento della sicurezza del sistema al di sotto della soglia minima di tutela prescritta dalla legge, rilevante non solo sul piano dell'eventuale responsabilità civile, ma anche a livello penale.

Nel caso di specie, inoltre, l'indebita comunicazione a terzi dei dati dei correntisti, realizzata mediante la messa a disposizione di informazioni caratterizzate da un'elevata confidenzialità (soprattutto in considerazione del rischio di utilizzo abusivo o illecito degli stessi dati da parte di terzi), ha configurato una violazione del cd. segreto bancario, inteso come obbligo per la banca di mantenere il riserbo su operazioni, conti e posizioni degli utenti dei servizi bancari.

Per prevenire il ripetersi delle violazioni contestate, il Garante ha segnalato alla banca l'esigenza di aggiornare l'analisi dei rischi connessi alla prestazione dei servizi di *e-banking*, in modo da adottare preventivamente misure di sicurezza idonee a garantire un livello di protezione elevato dei dati accessibili attraverso tali servizi. L'Autorità ha inoltre prescritto alla banca di verificare e di confermare l'utilizzo di codici identificativi personali e parole chiave da parte sia dei dipendenti incaricati, sia degli utenti del servizio di *e-banking*; ha poi disposto contestualmente la comunicazione all'autorità giudiziaria penale di copia degli atti. Da ultimo, a seguito dell'adempimento alle prescrizioni impartite, la banca è stata ammessa dall'Ufficio del Garante al pagamento di una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione, con conseguente dichiarazione di estinzione del reato, in conformità alla normativa vigente (cfr. ora l'art. 169 del Codice).

L'attivazione di analoghi accertamenti si è poi resa necessaria in altri due casi riguardanti la sicurezza dei dati degli utenti trattati da società concessionarie del servizio di erogazione dell'energia elettrica e del gas, mediante l'installazione di contatori per il monitoraggio dei consumi della clientela, il cui procedimento è in procinto di essere concluso.

Alla fine del 2003 sono stati inoltre instaurati alcuni procedimenti relativi alle misure adottate da datori di lavoro per la custodia di comunicazioni contenenti dati personali di lavoratori, al fine di renderne il contenuto inaccessibile ad eventuali terzi estranei alle vicende oggetto di comunicazione o di contestazione.

Da ultimo, va ricordato che, a chiarimento del nuovo quadro normativo in materia di misure di sicurezza introdotto dal Codice, e alla luce dei numerosi quesiti e richieste di proroga inviate da molte imprese, il Garante ha predisposto apposite istruzioni.

Codice e misure di sicurezza: le istruzioni del Garante (Nota 22 marzo 2004)

In particolare, il 22 marzo scorso il Garante ha fornito diverse indicazioni sui tempi e sulle modalità per una corretta applicazione delle novità normative introdotte dal Codice in materia di "misure minime" per la sicurezza dei dati e dei sistemi informatici.

L'Autorità ha sottolineato come il Codice abbia confermato la disciplina in materia di sicurezza dei dati personali introdotta nel 1996, ribadendo il principio in base al quale le "misure minime", la cui mancata adozione costituisce reato, sono solo una parte degli accorgimenti obbligatori in materia di sicurezza. Vi è, infatti, il dovere più generale, rilevante anche sul piano della responsabilità civile, di custodire i dati personali per contenere il più possibile il rischio che essi siano distrutti, dispersi, trattati in modo illecito, ovvero che diventino conoscibili fuori dei casi consentiti, come pure il dovere di introdurre ogni utile dispositivo di protezione legato alle nuove conoscenze tecniche.

L'elenco delle "misure minime" di sicurezza è stato aggiornato dal Codice, il quale ha specificato alcune modalità di applicazione in un apposito disciplinare tecnico. Analogamente a quanto avveniva in passato, le "misure minime" sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici, nonché a seconda che riguardi o meno dati sensibili o giudiziari.

Premesso che le "misure minime" obbligatorie anche in passato, devono essere ulteriormente mantenute senza attendere il decorso di termini transitori, in considerazione delle novità introdotte il Codice ha invece stabilito che, in sede di prima applicazione

del mutato quadro normativo, le nuove misure possono essere adottate entro il 30 giugno 2004. Un periodo più ampio per l'adeguamento (1° gennaio 2005) è previsto solo nel caso particolare in cui ricorrano obiettive e documentate ragioni di natura tecnica, che non consentano di installare immediatamente le nuove misure rispetto agli elaboratori e ai programmi utilizzati.

Il documento programmatico sulla sicurezza (Dps)

Con la recente comunicazione, l'Autorità ha ricordato che tra le "misure minime" di sicurezza rientra anche la redazione del documento programmatico sulla sicurezza (Dps) da parte dei soggetti che effettuano un trattamento di dati sensibili o giudiziari con l'ausilio di strumenti elettronici.

Si tratta di una misura non nuova; tuttavia, è cambiato parzialmente il contenuto del documento ed è aumentato il numero dei casi e dei soggetti destinatari dell'obbligo.

Proprio per questi motivi il Garante ha ritenuto che, solo in sede di prima applicazione della nuova disciplina, il Dps possa essere predisposto al più tardi entro il 30 giugno 2004: ciò permetterà di utilizzare il modello base semplificato predisposto dall'Autorità per effettuare, soprattutto presso realtà medio-piccole, l'analisi dei rischi che incombono sui dati personali, per individuare gli accorgimenti da adottare al fine di prevenire la loro distruzione o eventuali accessi abusivi e per pianificare gli interventi formativi nei riguardi del personale.

Dal 2005, decorso il periodo transitorio connesso all'entrata in vigore del Codice, il termine per redigere annualmente il Dps aggiornato rimarrà fissato ad un'unica scadenza, quella del 31 marzo di ogni anno, come dispone la regola tecnica n. 19 che disciplina tale misura.

Obbligo di riferire della redazione o aggiornamento del Dps

Il Garante ha inoltre precisato le modalità da seguire per l'attuazione di un'altra rilevante "misura minima" introdotta dal Codice, quella relativa all'obbligo di riferire, nella relazione di accompagnamento al bilancio di esercizio, dell'avvenuta redazione o aggiornamento del Dps. Questa misura, diretta a sensibilizzare e responsabilizzare gli organi di vertice aziendali o amministrativi sulla programmazione annuale degli adempimenti in tema di sicurezza, deve essere rispettata già nel 2004. Per questo primo anno, si è considerato il menzionato regime transitorio e la circostanza che alcuni soggetti non erano tenuti a redigere o aggiornare il Dps in base alla legge n. 675/1996. Sono state fornite varie indicazioni relative ai singoli casi, che si possono sintetizzare nel seguente specchietto riassuntivo che è stato accluso alla risposta data a Confindustria, Confcommercio e a diversi altri operatori pubblici e privati:

Disposizioni transitorie

Termini	Adempimenti
30 giugno 2004	Adozione per il 2004 di tutte le "misure minime" non previste dalla precedente disciplina. Termine ultimo di predisposizione del documento a data certa per descrivere le obiettive ragioni tecniche che non consentono di applicare immediatamente alcune nuove "misure minime" *(documento utilizzabile unicamente nel caso del tutto particolare previsto dall'art. 180, comma 2, del Codice per i soli strumenti elettronici).*
1° gennaio 2005	Adozione nuove "misure minime" su strumenti elettronici non previste in base alla precedente disciplina (solo per i soggetti legittimati a predisporre il predetto documento a data certa).

Relazione accompagnatoria del bilancio esercizio 2003

Misure	Soggetti già tenuti a redigere o aggiornare il Dps [1]	Soggetti non obbligati a redigere o aggiornare il Dps in base alla previgente disciplina
Dps 2004	Aggiornamento Dps entro il 30 giugno 2004	Redazione Dps entro il 30 giugno 2004
Relazione accompagnatoria del bilancio esercizio 2003	Riferimento al Dps redatto o aggiornato nel 2003 (con facoltà di indicazione aggiuntiva dell'aggiornamento 2004 *in itinere*), oppure menzione dell'aggiornamento eventualmente già effettuato nel 2004	Nessun riferimento se il Dps 2003 o il Dps 2004 non sono stati adottati, oppure riferimento al Dps eventualmente già adottato nel 2004. Facoltà di indicazione del Dps eventualmente predisposto nel 2003 e facoltà di indicazione dell'aggiornamento 2004 *in itinere*

Ulteriori indicazioni pratiche sono state fornite nel corso della prima edizione del ciclo di seminari di formazione curati dal Garante presso la propria sede (2 aprile 2004) e nel *Cd-Rom* multimediale in fase di predisposizione con i materiali del seminario.

12 Notificazione

Casi sottratti alla notificazione: il provvedimento del 31 marzo 2004

Con il provvedimento del 31 marzo 2004 (pubblicato in *G.U.*, Serie generale, 6 aprile 2004, n. 81 e che è riportato tra gli allegati di questa *Relazione*), il Garante ha individuato i trattamenti di dati personali che non sono oggetto di notificazione all'Autorità, in conformità a quanto stabilito dall'art. 37, comma 2, del Codice.

Come è stato già evidenziato, quest'ultimo ha introdotto una robusta semplificazione in argomento, individuando alcune specifiche categorie di trattamento per le quali vige l'obbligo di notificare preventivamente all'Autorità l'avvio di un trattamento di dati.

Fin dalle prime settimane di applicazione del Codice, e in vista del termine transitorio del 30 aprile 2004 per la presentazione delle notificazioni, il Garante ha ritenuto necessario individuare nuove semplificazioni che interessano, a date condizioni, imprese, enti locali, operatori sanitari (in particolare medici di medicina generale e pediatri), liberi professionisti, datori di lavoro e gestori di impianti di videosorveglianza.

Con tale provvedimento il Garante ha recepito diversi suggerimenti formulati, in questi primi mesi di vigenza del Codice, da alcuni operatori e associazioni di categoria, ravvisando che i trattamenti effettuati nelle predette ipotesi, specialmente in ragione delle relative modalità, potessero essere sottratti all'obbligo di notificazione, ferma restando, ovviamente, l'osservanza degli ulteriori principi ed obblighi previsti dal Codice.

(1) Titolari di un trattamento di dati sensibili o relativi a provvedimenti giudiziari di cui agli artt. 22 e 24 della legge n. 675/1996, effettuato per mezzo di elaboratori accessibili mediante una rete di telecomunicazione disponibili al pubblico

Il Garante ha invece ritenuto, allo stato, di non individuare ulteriori trattamenti di dati personali suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato oltre a quelli indicati all'art. 37, comma 1, e da sottoporre pertanto all'obbligo di notificazione. Non è comunque da escludere 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 notifica.

III - La privacy e gli altri diritti
La salute

13 Trattamento di dati idonei a rivelare lo stato di salute

Nel 2003 l'Autorità è stata nuovamente chiamata ad intervenire sul tema dei trattamenti di dati personali effettuati nell'ambito del Servizio sanitario nazionale.

Tra le questioni di maggiore rilievo affrontate si pone, in primo luogo, quella dei limiti alla comunicazione di dati sulla salute e sulla vita sessuale a soggetti diversi dall'interessato. La comunicazione di queste informazioni può, infatti, ritenersi giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti fondamentali e inviolabili. Tale principio è ora confermato dal Codice (artt. 26, comma 4, lett. *c)*, 60, 71 e 92 comma 2, d.lg. n. 196/2003).

Con un provvedimento del 9 luglio 2003, del quale ci si occupa in dettaglio nel capitolo dedicato alla pubblica amministrazione, l'Autorità ha fornito ulteriori indicazioni in ordine a tale problema (cfr. parag. 19.2.).

Recupero coattivo dei crediti affidato a società esterne

Sempre in materia di comunicazione di dati idonei a rivelare lo stato di salute, il Garante ha indicato particolari cautele che le aziende sanitarie locali devono rispettare nell'affidare a società esterne l'attività di recupero coattivo dei crediti derivanti dal mancato pagamento dei *ticket* e dal mancato ritiro dei referti medici.

In tali casi, le aziende debbono designare i soggetti che hanno accesso ai dati dei pazienti in qualità di responsabili o incaricati del trattamento ed informare preventivamente gli interessati sulla possibilità che le informazioni che li riguardano siano utilizzate per finalità di recupero dei crediti. Dovranno poi essere forniti alla società che collabora all'esterno i soli dati personali strettamente necessari al recupero della somma dovuta (dati anagrafici, indirizzo, importo, ecc.) e non anche ulteriori informazioni quali, ad esempio, quelle riguardanti il tipo di analisi effettuata o il relativo referto, in ossequio ai principi di pertinenza e non eccedenza nel trattamento dei dati (*Nota* 22 aprile 2003).

Comunicazione dei dati sulle situazioni di abbandono dei minori

Si è invece ritenuto legittimo che gli operatori di un servizio per le tossicodipendenze segnalino alla procura della Repubblica presso il tribunale dei minorenni situazioni di abbandono o di pregiudizio. La normativa di settore riconosce infatti a chiunque la facoltà di segnalare alle autorità competenti situazioni di abbandono di minori. Sui pubblici ufficiali, gli incaricati di un pubblico servizio e gli esercenti un servizio di pubblica necessità grava, poi, l'obbligo di riferire al più presto al procuratore competente per territorio sulle condizioni dei minori in situazione di abbandono di cui vengano a conoscenza in ragione del proprio ufficio (art. 9, comma 1, legge n. 184/1983).

In quanto espressamente prevista dalla legge, la comunicazione all'autorità giudiziaria di situazioni di abbandono o di pregiudizio ad opera dei servizi per le tossicodipendenze, pubblici o privati, non contrasta, perciò, con la disciplina sulla protezione dei dati. L'operatore deve tuttavia comunicare al tribunale i soli dati pertinenti e necessari ad illustrare la situazione di abbandono in cui versa il minore (*Nota* 1° luglio 2003).

Non può ritenersi invece ammessa la comunicazione, da parte della prefettura ad una amministrazione comunale che ha in assegnazione obiettori di coscienza, di provvedimenti sanzionatori relativi all'uso di sostanze stupefacenti adottati nei confronti di questi ultimi, in assenza di una specifica norma di legge che lo consenta (*Nota* 25 agosto 2003).

Sono poi all'attenzione dell'Autorità le procedure seguite da diversi comuni per controllare la legittimità degli accessi alle zone a traffico limitato (Ztl) ad opera dei medici che hanno necessità di visitare a domicilio i pazienti residenti in tale aree.

In argomento, l'indicazione del nominativo dell'assistito può risultare idonea a rivelare lo stato di salute del paziente, e come tale da trattare con l'adozione delle cautele previste per questo tipo di informazioni e nel rispetto dei principi di pertinenza e di non eccedenza. Si deve, pertanto, valutare con estrema attenzione se, per perseguire la finalità di accertamento delle infrazioni alla disciplina delle zone a traffico limitato, non sia sufficiente conoscere il recapito (via e numero civico) presso cui l'intervento medico è stato prestato.

Allo stesso modo è, poi, sotto esame la prassi seguita da alcune amministrazioni comunali di richiedere ai medici un'attestazione del consiglio dell'ordine con la quale si dichiari che il professionista si è recato nella zona a traffico limitato per ragioni legate all'esercizio della professione medica.

In base all'art. 74 del d.lg. n. 196/2003, i contrassegni rilasciati per il transito in zone a traffico limitato o per la circolazione e la sosta di veicoli a servizio di persone invalide devono contenere i soli dati indispensabili ad individuare il tipo di autorizzazione, ed essere privi di simboli o diciture da cui possa desumersi la speciale natura dell'autorizzazione, per effetto della sola visione del contrassegno.

Le generalità e l'indirizzo della persona fisica interessata, inoltre, devono essere riportati sui contrassegni con modalità tali da non permettere la loro diretta visibilità, se non in caso di richiesta di esibizione o necessità di accertamento.

Elenco dei beneficiari di assegni di cura

In applicazione del divieto di diffusione dei dati idonei a rivelare lo stato di salute, ribadito ora dal Codice (art. 22, comma 8, d.lg. n. 196/2003), il Garante ha prescritto di non affiggere, nei locali di un'azienda sanitaria locale, un elenco contenente alcuni dati personali dei beneficiari di assegni di cura. Anche l'indicazione negli elenchi delle sole iniziali dei beneficiari di tali assegni può infatti consentirne l'identificazione: quindi, le esigenze di pubblicità dell'amministrazione potevano essere ugualmente soddisfatte attraverso l'apposizione di diciture generiche o codici numerici (*Nota* 29 agosto 2003).

Si deve pure ricordare che, nell'ottobre del 2003, il Garante ha siglato un protocollo di intesa con l'Azienda ospedaliera universitaria "Policlinico Tor Vergata",

volto a sperimentare sul campo, in una struttura di recente creazione, l'applicazione della normativa a tutela della riservatezza nel settore sanitario.

A seguito dell'entrata in vigore del Codice, l'Autorità sta poi esaminando alcune questioni relative al trattamento dei dati effettuato per la tenuta e la gestione dei registri tumori: si deve, infatti, verificare in quale misura le operazioni connesse alla tenuta ed alla gestione di questi registri possano considerarsi comprese tra le attività di rilevante interesse pubblico individuate dal Codice (in particolare, dall'art. 98).

Ricerca scientifica

In materia di ricerca scientifica (oltre al codice deontologico su statistica e ricerca i cui lavori sono in fase di imminente conclusione), occorre ricordare che la disciplina di favore prevista per la ricerca in campo medico, biomedico ed epidemiologico è stata confermata dal Codice (art. 110 d.lg. n. 196/2003). Per il perseguimento di queste finalità è possibile utilizzare dati personali idonei a rivelare lo stato di salute degli interessati anche a prescindere dal consenso di questi ultimi, qualora la ricerca sia prevista da un'espressa previsione di legge che contempli specificamente il trattamento, o sia compresa in un programma di ricerca biomedica o sanitaria, e ne sia data previa comunicazione al Garante (art. 39 d.lg. n. 196/2003). A queste ipotesi il Codice aggiunge il caso in cui, per particolari ragioni, non sia possibile informare l'interessato e il programma di ricerca sia oggetto di parere favorevole da parte del competente comitato etico (nonché autorizzato dal Garante, anche con provvedimenti di carattere generale: art. 40 d.lg. n. 196/2003).

Per quanto concerne il trattamento dei dati personali dei soggetti sieropositivi, si è esaminata la questione dell'attuazione di un sistema di sorveglianza epidemiologica delle infezioni da Hiv, secondo un progetto della Commissione nazionale per la lotta contro l'Aids e le altre malattie infettive emergenti e riemergenti, sottoposto all'attenzione dell'Autorità.

Sul tema è stato costituito un gruppo di lavoro, in cui, oltre all'Autorità ed alla Commissione ora indicata, sono rappresentate le regioni, la Presidenza del Consiglio dei ministri, l'Istituto superiore di sanità e le associazioni che tutelano l'interesse delle persone affette da Hiv. Nell'ambito di questo gruppo sono stati inizialmente esaminati, in particolare, i presupposti che rendono lecito il trattamento dei dati personali dei sieropositivi, i dati utilizzati, i loro flussi e le modalità con le quali rendere l'informativa agli interessati nonché le misure di sicurezza da adottare.

Le novità introdotte dal d.l. 30 settembre 2003, n. 269 in tema di monitoraggio della spesa sanitaria hanno determinato l'attivazione dell'Autorità, con riferimento al complesso meccanismo che verrebbe basato su un modello di ricetta medica a lettura ottica e sulla costituzione di una o più banche dati.

Come già accennato, il Garante ha rilevato che la finalità di razionalizzazione del controllo della spesa sanitaria va perseguita nel pieno rispetto del diritto dei cittadini alla protezione dei dati personali, soprattutto in relazione alle informazioni riguardanti la salute. La banca (o le banche) dati di cui è prevista la realizzazione permetterebbe infatti di risalire, anche tramite il codice fiscale, all'identità dell'assistito ed all'intera sua storia sanitaria.

Ricordando che la legislazione vigente prevede già procedure di monitoraggio della spesa sanitaria che non richiedono banche dati nominative centralizzate,

l'Autorità ha precisato che l'unico sistema di controllo conforme alla normativa sulla protezione dei dati comporta l'esclusione del trattamento sistematico di qualsiasi informazione identificativa sullo stato di salute degli assistiti. Altrimenti, si correrebbe il rischio di introdurre nel sistema forme di discriminazione dei cittadini a vantaggio di chi sia in grado di pagare direttamente i farmaci e le prestazioni specialistiche (*Comunicato stampa* 28 ottobre 2003).

Anche a seguito delle indicazioni fornite dall'Autorità, il sistema di monitoraggio previsto dal decreto è stato però solo in parte modificato in sede di conversione (l. 24 novembre 2003 n. 236; cfr. *supra*, parag. 2., lett. *a)*).

L'attenzione si sposta ora, anche a seguito dei primi contatti intercorsi con il Ministero dell'economia e delle finanze, sulle modalità che verranno prescritte per la concreta applicazione del d.l. n. 269/2003.

Sono infatti previsti diversi decreti per l'attuazione delle relative disposizioni e l'Autorità svolgerà al riguardo i propri compiti istituzionali con ogni dovuta attenzione all'elevato livello di garanzia assicurato dal Codice e reso indispensabile anche dagli obblighi derivanti dal quadro comunitario e dalla giurisprudenza della Corte europea dei diritti dell'uomo a proposito dell'art. 8 della Convenzione sui diritti dell'uomo.

Tra le questioni all'avanzato studio dell'Autorità in materia di dati sulla salute, meritano di essere indicate le seguenti:

- utilizzo delle principali applicazioni telematiche (collegamenti ad Internet, *e-mail*, ecc.) e reti satellitari per i dati sulla salute, in particolare per l'offerta di servizi informativi sulle attività svolte da diverse strutture sanitarie, per la prenotazione di esami clinici e visite diagnostiche ed il rilascio dei relativi risultati, per le schede cliniche informatizzate, nonché per sistemi di teleconsulto, telediagnosi e telemedicina;

- trasmissione per via telematica all'Inps dei certificati di malattia predisposti da medici di medicina generale;

- valutazione delle procedure adottate dalle aziende sanitarie locali per il rilascio della tessera di esenzione dal pagamento del *ticket*.

Ispezioni svolte dal Garante in materia sanitaria

Tra le attività ispettive svolte dal Garante, di rilievo è anche quella effettuata in una struttura sanitaria presso cui erano state abbandonate numerose cartelle cliniche, immediatamente dopo le prime notizie di stampa e in collaborazione con la Guardia di finanza. L'Ufficio del Garante ha svolto un sostanziale ruolo di coordinamento degli interventi delle autorità locali, già avviati su indicazione della Procura della Repubblica di Lecce, allo scopo di verificare che il recupero e la conservazione delle cartelle cliniche avvenissero in modo idoneo ad evitare accessi non autorizzati ai dati personali in esse contenuti (ispezione presso un'ex colonia di Santa Maria di Leuca del 12 febbraio 2004).

Un'analoga vicenda si è verificata in Roma nel cortile di una biblioteca comunale, liberamente accessibile al pubblico, dove sono stati rinvenuti numerosi documenti sanitari (ricette e cartelle cliniche). Anche in questo caso il Garante ha otte-

nuto, subito dopo le segnalazioni di stampa, la rapida rimozione dei documenti, al fine di impedire la conoscibilità dei dati personali in essi contenuti da parte di terzi non autorizzati (ispezioni del 10 e 12 gennaio 2004).

È stato poi compiuto un terzo accertamento ispettivo nei confronti di un policlinico universitario, dove erano stati segnalati alcuni furti di *computer*. In questo caso, è stato tuttavia accertato *in loco* il rispetto della normativa sulla protezione dei dati personali e, in particolare, l'adozione delle "misure minime" di sicurezza (ispezione presso l'Azienda ospedaliera universitaria Policlinico Federico II).

Sempre con riferimento al trattamento dei dati in ambito sanitario, il Codice prevede modalità semplificate per l'informativa e l'acquisizione del consenso utilizzabili dai medici di medicina generale, dai pediatri di libera scelta e dagli organismi sanitari pubblici e privati. Al fine di agevolare l'applicazione di questa disciplina da parte degli operatori sanitari, il Garante completerà entro breve termine, in collaborazione con competenti organi rappresentativi, un modello semplificato di informativa utilizzabile anche dai medici e suggerirà formule sintetiche e colloquiali per raccogliere il consenso (lettera al Ministro della salute del 6 febbraio u.s.).

In materia di "misure minime" di sicurezza, l'Autorità presterà inoltre la propria collaborazione, all'interno di un gruppo di lavoro istituito con i rappresentanti degli operatori sanitari, per la redazione di un modello adattato di documento programmatico sulla sicurezza. Ulteriori chiarimenti e delucidazioni saranno, poi, fornite ai medici di medicina generale e ai pediatri a seguito del provvedimento del 31 marzo 2004 (su cui *supra*, parag. 12.) con cui il Garante ha introdotto alcune semplificazioni in materia di notificazione, che interessano, tra gli altri, gli operatori sanitari (*Nota* 1° aprile 2004).

Misure di carattere organizzativo

Oltre alle norme di semplificazione, il Codice detta alcune misure di carattere organizzativo intese a garantire il rispetto della dignità e degli altri diritti dell'interessato nella fornitura delle prestazioni e dei servizi sanitari, quali ad es. la cd. distanza di cortesia, la riservatezza nei colloqui e regole di condotta analoghe al segreto professionale per gli incaricati che non vi sono già sottoposti. Specifiche cautele sono poi previste per le informazioni identificative dell'assistito riportate sulle ricette mediche (art. 87 d.lg. n. 196/2003).

La necessità di rispettare tali garanzie è stata tenuta presente negli accertamenti avviati nei riguardi della prassi temporaneamente instaurata nella Regione Sicilia che, in attuazione di una legge regionale sull'introduzione di un sistema di esenzione del *ticket* basato sul reddito, ha adottato una procedura che rendeva conoscibili alcune informazioni personali relative a quanti intendessero usufruire dell'esenzione. In particolare, al momento dell'acquisto dei medicinali in farmacia, si richiedeva agli assistiti di autocertificare la propria situazione economica sul retro della ricetta.

Il Garante ha già completato le prime verifiche anche alla luce dell'analoga esperienza verificatasi in Abruzzo, che ha portato la relativa amministrazione regionale a modificare precedenti orientamenti.

Le libertà associative

14 Associazioni, movimenti politici e partiti

14.1. Associazioni

L'entrata in vigore del nuovo Codice ha interessato il settore delle associazioni con riferimento al trattamento sia dei dati comuni, sia dei dati sensibili.

Il consenso

Il trattamento di informazioni riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria non è più assoggettato alla specifica disciplina in materia di dati sensibili, fondata sul consenso scritto dell'interessato e sull'autorizzazione del Garante (art. 26, comma 3, lett. *b)*, d.lg. n. 196/2003).

Inoltre, le associazioni e gli organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale (inclusi i partiti o movimenti politici) non sono più tenuti ad acquisire il consenso degli aderenti o dei soggetti che, in relazione alle finalità statutarie perseguite, hanno contatti regolari con l'ente stesso, per poter trattare i loro dati sensibili. Tutto ciò, a patto che i dati non siano divulgati a terzi e l'associazione adotti idonee misure per la loro tutela, prevedendo modalità di utilizzo dei dati con una determinazione che deve essere resa nota agli interessati all'atto dell'informativa (art. 26, comma 4, lett. *a)*, d.lg. n. 196/2003).

Anche nel periodo considerato il Garante è stato chiamato ad occuparsi, sotto più profili, di questioni connesse al trattamento di dati personali da parte delle realtà associative.

Casistica

Tra i numerosi interventi dell'Autorità è da ricordare, in primo luogo, il caso della convenzione stipulata tra una confederazione sindacale ed un'associazione di consumatori, avente ad oggetto l'iscrizione promozionale all'associazione stessa, come soci aggregati, di persone appartenenti alle rappresentanze delle varie organizzazioni aderenti alla confederazione sindacale. Si è rilevato in proposito che la convenzione non aveva comportato una comunicazione diretta e automatica dei dati personali dei potenziali soci aggregati dalla confederazione sindacale all'associazione dei consumatori, e che la raccolta di tali dati sarebbe potuta avvenire solo su iniziativa di ciascun interessato, al momento dell'eventuale richiesta di adesione all'associazione dei consumatori. Inoltre, si è richiamata l'attenzione sulla necessità di integrare l'informativa resa agli interessati, in modo da rendere più chiari gli elementi caratterizzanti il trattamento.

Un altro caso significativo ha riguardato la richiesta, avanzata da un'associazione di categoria, di autorizzazione al trattamento dei dati sensibili relativi alla salute della clientela degli associati; in tale occasione –come già in vicende analoghe– la richiedente è stata invitata a verificare se i trattamenti effettuati non rientrassero tra quelli già autorizzati dal Garante in via generale e, in caso contrario, ad indicare le circostanze del tutto particolari o le situazioni eccezionali in base alle quali si sarebbe resa eventualmente necessaria un'autorizzazione specifica.

Infine, l'Ufficio si è occupato della richiesta di utilizzo dei dati degli associati ad una federazione sportiva per finalità di propaganda elettorale, in vista delle elezioni degli organi di vertice della federazione.

Al riguardo, premesso che l'attuale natura privatistica delle federazioni sportive (come stabilita dal d.lg. n. 242/1999) non consentiva di applicare alla vicenda le norme sul trattamento dei dati personali da parte degli enti pubblici, si è chiarito che occorreva individuare uno dei presupposti di liceità che la legge prevede per il trattamento dei dati da parte di soggetti privati: quindi, il consenso informato e specifico per tale operazione di trattamento (in relazione allo statuto o all'atto costitutivo), oppure uno degli altri presupposti di legge.

14.2. Movimenti politici e propaganda elettorale

Nel periodo considerato sono state analizzate problematiche assai rilevanti per il settore in esame, in connessione anche con alcuni appuntamenti elettorali.

In particolare, durante la campagna elettorale svoltasi per le elezioni amministrative tenute in alcune regioni italiane nell'estate del 2003, sono pervenute varie segnalazioni aventi ad oggetto l'invio di comunicazioni elettorali a clienti di società, da parte di dipendenti, collaboratori o agenti delle società stesse, candidati alle elezioni o comunque sostenitori di candidati.

In tali casi, in accordo con l'orientamento già espresso in precedenti occasioni dal Garante (cfr. *Provv.* 7 marzo 2001; *Provv.* 9 ottobre 2000), va rilevato che per l'uso a fini di propaganda elettorale dei dati anagrafici raccolti presso banche dati pubbliche, registri o elenchi conoscibili da chiunque, deve essere fornita una chiara informativa agli interessati.

Il provvedimento del Garante del 12 febbraio 2004

Di recente il tema è stato già affrontato in termini generali nel provvedimento del Garante del 12 febbraio 2004 (pubblicato in *Gazzetta Ufficiale* 24 febbraio 2004, n. 45, e riportato negli allegati alla presente *Relazione*), che ha individuato i presupposti, le garanzie e i limiti per l'utilizzo di liste e indirizzari formati anche nell'ambito della prestazione di attività e servizi, al fine di inviare note di propaganda a favore di candidati interni o sostenuti da società, enti o associazioni.

In particolare, in vista delle consultazioni elettorali europee ed amministrative indette per il 12 e 13 giugno prossimi, il Garante, nel provvedimento del 12 febbraio 2004, ha indicato i casi in cui partiti, movimenti politici, comitati promotori, sostenitori e candidati possono utilizzare dati personali a fini di propaganda elettorale a prescindere dal consenso degli interessati, fornendo loro un'adeguata informativa. Tale ipotesi può ricorrere quando si utilizzano dati estratti da registri, elenchi, atti o documenti detenuti da un soggetto pubblico e accessibili liberamente in base ad un'espressa disposizione di legge o di regolamento. Si tratta, ad esempio, delle liste elettorali comunali, degli elenchi di iscritti ad albi e collegi professionali, dell'elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo, delle cd. liste aggiunte dei cittadini elettori di uno Stato membro dell'Ue, dell'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle relative liste elettorali e di quello degli aventi diritto al voto per l'elezione dei Comites (su cui cfr. *infra*, parag. 21.).

I dati estratti dagli elenchi della telefonia fissa possono essere invece trattati a fini di propaganda elettorale sotto forma di invio di posta ordinaria o di chiamate telefoniche effettuate da un operatore, a meno che gli interessati non si siano opposti. Fuori da ipotesi di questo tipo, non è possibile svolgere attività di propaganda politica senza un consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiaramente gli scopi per i quali i dati sono utilizzati. Ciò, in particolare, quando si ricorra all'invio di fax, di messaggi *Sms* e *Mms*, o di *e-mail*, nonché a chiamate telefoniche senza l'intervento di un operatore oppure a chiamate a terminali di telefonia mobile.

Quando si utilizzano dati di iscritti ad associazioni politiche o a partiti, il consenso specifico deve essere manifestato per iscritto, versandosi in un caso di trattamento di dati di tipo sensibile (v., per altro, quanto previsto dagli artt. 26, comma 4, lett. *a)* e 181, comma 1, lett. *b)* del Codice). L'utilizzazione di dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politica è possibile invece solo quando sia disposta legittimamente in base all'ordinamento interno, le modalità di utilizzo dei dati a fini di propaganda siano compatibili con gli scopi principali perseguiti dall'associazione e ne venga fatta menzione nell'informativa resa agli iscritti al momento dell'adesione o del suo rinnovo.

Il Garante ha anche precisato che i titolari di alcune cariche elettive non sono legittimati ad ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per la propaganda anche dopo la scadenza dal mandato; gli stessi possono però utilizzare i dati personali raccolti direttamente, nel quadro delle relazioni interpersonali con cittadini ed elettori.

In ogni caso, l'informativa che chi svolge attività di propaganda elettorale è tenuto a rendere agli interessati deve essere inserita nel materiale di propaganda e può essere resa anche in forma sintetica. Limitatamente alle imminenti consultazioni elettorali, il Garante ha tuttavia esonerato a date condizioni dall'obbligo di fornire l'informativa i soggetti che utilizzano dati personali per esclusivi fini di propaganda, ritenendo tale adempimento sproporzionato nel caso in cui i dati siano estratti da elenchi pubblici e gli interessati non vengano poi contattati, nonché quando il materiale propagandistico sia di dimensioni talmente ridotte da non permettere di inserire agevolmente l'informativa (art. 13, comma 5, d.lg. n. 196/2003).

Uso dei dati a fini promozionali e commerciali

Particolare attenzione è stata prestata al requisito della specificità del consenso richiesto per l'uso dei dati a fini promozionali e commerciali e alla necessità che eventuali utilizzi ulteriori per fini di propaganda politica siano indicati in tali consensi in modo univoco. Il problema è stato affrontato anche successivamente su richiesta della Federazione delle concessionarie di pubblicità e di un operatore del settore ai quali, con note del 25 marzo e del 6 aprile 2004, sono state rappresentate le necessarie garanzie che consentono o precludono l'invio di *e-mail* di propaganda o l'inserzione di pubblicità elettorale all'interno di *newsletter* richieste dagli interessati per altri fini.

14.3. Confessioni religiose

Per quanto riguarda il trattamento di dati sensibili in ambito religioso, occorre sottolineare l'importante novità normativa introdotta sul punto dal Codice.

Nel sistema previgente, in parziale applicazione dei principi comunitari in materia di associazioni e di altri organismi senza scopo di lucro, era infatti prevista una disciplina particolare per la Chiesa cattolica e per le altre confessioni religiose che avessero stipulato accordi o intese con lo Stato italiano.

Questa disciplina si basava sulla possibilità di prescindere dal consenso degli interessati e dal rispetto dell'autorizzazione del Garante per trattare i dati sensibili degli aderenti e degli altri soggetti che avessero contatti regolari con le confessioni, purché fossero rispettate certe condizioni, tra le quali l'osservanza di idonee garanzie che le confessioni stesse avrebbero dovuto introdurre nei propri ordinamenti.

La modifica introdotta dal Codice

Il Codice estende ora questa specifica disciplina alle altre confessioni religiose, purché i dati non siano diffusi o comunicati al di fuori delle confessioni e vengano osservate idonee garanzie di cui le stesse devono dotarsi, nel rispetto dei principi contenuti in un'autorizzazione del Garante (art. 26, comma 3, lett. *a)*, d.lg. n. 196/2003).

L'art. 181, comma 6, del d.lg. n. 196/2003 consente poi alle confessioni religiose che, prima dell'entrata in vigore del Codice, abbiano già adottato le garanzie richieste nell'ambito dei propri ordinamenti, di proseguire il trattamento nel rispetto delle medesime.

Nella materia in esame, il Garante ha tra l'altro affrontato la questione del trattamento di dati idonei a rivelare convinzioni religiose, effettuato da un'associazione per avviare le pratiche di annullamento di matrimoni religiosi. In proposito, l'Autorità ha ribadito che i dati raccolti dovevano essere trattati soltanto per le procedure rivolte all'accertamento della nullità del matrimonio davanti al tribunale ecclesiastico e non anche per scopi ulteriori (*Nota* 10 aprile 2003).

I registri dei battezzati

Nel corso del 2003 sono anche pervenuti ricorsi e segnalazioni tesi ad ottenere l'aggiornamento e l'integrazione di dati personali contenuti nei registri dei battezzati presenti negli archivi parrocchiali, con specifico riferimento al dato sull'appartenenza religiosa degli interessati che non risulti più rispondente alla realtà.

Al riguardo, il Garante ha confermato la legittimità delle richieste intese a far annotare, a margine del dato da aggiornare, la volontà degli interessati di non appartenere più alla Chiesa cattolica, reputando l'annotazione compatibile con la necessaria documentazione del fatto storico dell'avvenuto battesimo.

L'Autorità ha poi chiarito che la conservazione dell'istanza presentata dall'interessato in allegato al registro dei battesimi non è sufficiente a far risultare in modo inequivoco e permanente la volontà del medesimo interessato di non appartenere più alla Chiesa cattolica. In presenza di una richiesta di integrazione e aggiornamento del dato relativo all'appartenenza religiosa, occorre quindi effettuare un'apposita annotazione a margine sul registro dei battesimi (*Provv.* 19 marzo 2003).

In una decisione su un ricorso, l'Autorità ha infine precisato che, per presentare la richiesta finalizzata ad aggiornare ed integrare i dati personali del richiedente con spe-

cifico riferimento al dato relativo all'appartenenza religiosa, non è necessario recarsi personalmente presso determinati uffici (ad esempio, quelli del Vicariato) al fine di dimostrare e controfirmare la dichiarazione di non voler essere più considerato appartenente alla Chiesa cattolica. La normativa sulla protezione dei dati personali non prevede, infatti, che il richiedente debba presentarsi di persona presso la sede del titolare per esercitare i propri diritti e, nel caso esaminato, confermare la menzionata volontà. È stata invece ritenuta legittima ogni eventuale attività della Curia volta a richiamare l'attenzione dell'interessato sugli effetti che l'istanza produce (*Newsletter* 10-16 novembre 2003).

In tema di questioni concernenti il trattamento dei dati religiosi, l'Autorità si sta occupando anche del regime di pubblicità delle anagrafi parrocchiali e della raccolta di dati idonei a rivelare convinzioni religiose in occasione di visite specialistiche o ricoveri ospedalieri.

La libertà di informazione

15 Attività giornalistiche e mezzi di informazione

Continuano a pervenire numerosi quesiti, segnalazioni e reclami in ordine alle problematiche relative al trattamento di dati personali effettuato nell'esercizio dell'attività giornalistica. Parallelamente è cresciuta, nei confronti di tali temi, l'attenzione degli operatori dell'informazione, che hanno interpellato il Garante chiedendo chiarimenti sul corretto utilizzo delle informazioni, nel quadro delle vigenti norme in materia di protezione dei dati personali e del codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*Provv.* 29 luglio 1998, in *Gazzetta Ufficiale* 3 agosto 1998, n. 179).

Nel corso dell'anno è stato avviato un nuovo confronto tra il Garante ed il Consiglio nazionale dell'ordine dei giornalisti. In tale contesto, si è costituito un gruppo di lavoro comune incaricato, tra l'altro, di elaborare documenti utili a fornire un concreto contributo al lavoro di chi opera nel mondo dell'informazione e ad esaminare alcuni aspetti applicativi del d.lg. n. 196/2003. Sulla base dei primi spunti di riflessione pervenuti dall'ordine, il Garante ha fornito da ultimo un quadro di approfondite indicazioni circa la liceità e la correttezza della raccolta e diffusione di specifiche fonti di informazione.

Allo scopo di dare un utile riscontro a tale accresciuta attenzione, il Garante ha poi pubblicato una raccolta dei più significativi provvedimenti adottati dall'Autorità in materia di giornalismo e tutela dei dati personali. Il volume, curato da Mauro Paissan, componente del collegio, è stato presentato a Roma il 6 novembre 2003 alla presenza del Presidente della Camera e di diversi esponenti del mondo politico e dell'informazione. La raccolta –organizzata per macroargomenti (tutela dei minori, rapporti tra cronaca e giustizia, uso dei dati relativi a personaggi pubblici, trasparenza delle fonti pubbliche, tutela dei dati relativi alla salute ed alla sfera sessuale, uso di fotografie)– è preceduta da un quadro di sintesi delle disposizioni del codice di deontologia dei giornalisti e da una generale riflessione del curatore dell'opera sulle principali problematiche che emergono nella delicata opera di bilanciamento tra tutela della persona e libertà di manifestazione del pensiero (cfr. pure *infra*).

15.1. Tutela dei minori

Il Garante è nuovamente intervenuto a tutela dei diritti dei minori coinvolti in fatti di cronaca, vietando, tra l'altro, con un provvedimento d'urgenza diretto a diversi editori e direttori di quotidiani, nazionali e locali, l'ulteriore diffusione di informazioni relative a due bambini vittime di atti di violenza. Nel caso di specie, pur non essendo stata resa apertamente nota l'identità dei minori e dei genitori, sono state diffuse varie informazioni (tra cui anche la foto segnaletica dell'adulto ritenuto responsabile di dette violenze) giudicate, oltre che eccedenti e non indispensabili a rappresentare la vicenda, tali da rendere comunque immediatamente riconoscibili i minori all'interno della cerchia familiare, degli amici e dei conoscenti. In questo modo risultavano violate le garanzie normative, nazionali e internazionali (art. 13

della Convenzione sui diritti del fanciullo; art. 734-*bis* c.p.; art. 13 d.P.R. 22 settembre 1988 n. 448; art. 7 codice deontologico; Carta di Treviso) poste a tutela della sfera privata dei minori, riaffermate ed ampliate anche dal Codice (artt. 50 e 52).

La vicenda presenta sviluppi ancora in fase di svolgimento, come dimostrano, ad esempio, le note con le quali il direttore di una delle testate oggetto di divieto, si è poi attivato per prevenire analoghe infrazioni, mentre un consiglio dell'ordine locale ha chiesto al Garante di fornire i nomi dei giornalisti autori degli articoli pubblicati ai fini della loro convocazione.

15.2. Foto segnaletiche e cronache giudiziarie

L'Autorità è intervenuta in maniera incisiva nei confronti della prassi diffusa presso organi di informazione di pubblicare fotografie di persone arrestate o indagate.

Il provvedimento del Garante del 19 marzo 2003

È stata più volte riscontrata la violazione degli specifici divieti, riaffermati anche dal codice deontologico per l'attività giornalistica, a tutela delle persone coinvolte nei fatti oggetto della notizia. Il Garante ha osservato che, fermo restando il divieto di pubblicare immagini di persone con ferri o manette ai polsi, ovvero sottoposte ad altri mezzi di coercizione fisica, senza il consenso dell'interessato, la diffusione di fotografie di individui in stato di detenzione è ammessa solo per comprovati fini di giustizia e di polizia e in ogni caso nel rispetto della dignità personale (*Provv.* 19 marzo 2003). Limitatamente ad una delle testate interessate dal divieto, il provvedimento è stato caducato con decreto del 26 giugno 2003 del Tribunale di Milano, dinanzi al quale era stata proposta la relativa impugnazione. Il tribunale, pur ritenendo in punto di fatto non interamente comprovata la constatazione dell'Autorità (provenienza delle immagini da foto "segnaletiche" oppure da documenti di identità) e quindi accogliendo il ricorso, ha comunque confermato il principio di diritto affermato dal Garante, in base al quale, come si è detto, la diffusione di fotografie riguardanti persone sottoposte a misure restrittive della libertà personale è ammessa, in mancanza del consenso delle persone ritratte, per il perseguimento di esclusive finalità di giustizia e di polizia e nel rispetto della disposizione del codice deontologico sull'attività giornalistica (art. 8) che vieta le riprese in stato di detenzione.

Tale principio è stato ribadito di recente con riguardo alla diffusione di foto "segnaletiche" di alcune persone coinvolte in un'indagine su stupefacenti e prostituzione avviata dalla magistratura romana (*Provv.* 26 novembre 2003). In questo caso l'Autorità, rilevando l'assenza dei presupposti di legge, ha vietato l'utilizzazione delle foto "segnaletiche" ed ha segnalato al Capo della polizia le illiceità rilevate. Ha inoltre provveduto a richiedere informazioni agli uffici di polizia interessati dalle operazioni di trattamento oggetto del divieto, anche con riferimento alla diffusione di altri dati (dettagli relativi al contenuto di conversazioni telefoniche, estremi identificativi di utenze telefoniche) inerenti all'indagine in corso.

In relazione alle problematiche generali riguardanti le cronache giudiziarie, l'Autorità ha più volte ricordato agli organi di informazione che l'esigenza di informare l'opinione pubblica su vicende giudiziarie non deve recare pregiudizio alla vita privata delle persone. Ha quindi ribadito che la diffusione di tale tipo di informazioni, anche in mancanza del consenso dell'interessato, non è preclusa; deve tuttavia essere assicurato il rispetto dei limiti previsti per l'esercizio del diritto di cronaca, in particolare quello dell'essenzialità dell'informazione riguardo a fatti di interesse

pubblico, oltre che l'osservanza degli specifici divieti posti dagli ordinamenti penale e processualpenale.

15.3. Privacy dei personaggi pubblici

Il Garante, con una decisione adottata su ricorso, ha rilevato i limiti entro cui può considerarsi legittima l'informazione su fatti di cronaca coinvolgenti persone che godono di una certa notorietà in ragione del ruolo o della funzione ricoperti. Un caso ha riguardato, ad esempio, il trattamento di dati relativi ad un ingegnere, noto in ambito locale per la sua attività di progettista e direttore dei lavori di un piano di riassetto territoriale. L'Autorità ha ritenuto lecita la pubblicazione dei dati relativi alla posizione del professionista, ai suoi impegni e agli onorari percepiti, in ragione della rilevanza pubblica della notizia (giustificata anche da esigenze di trasparenza sull'utilizzo del denaro pubblico), nonché della notorietà del ricorrente, impegnato a vario titolo e con ruoli di responsabilità in un'operazione urbanistica ed economica di primario rilievo locale. Si è ritenuto invece che fosse fonte di illiceità sia la diffusione, nell'ambito dello stesso servizio giornalistico, di dati attinenti alla sfera privata ed allo stato salute del ricorrente (disagi psicologici per i quali era ricorso ad una specifica terapia psicoanalitica), sia il collegamento effettuato con le vicende personali del fratello, in gravi condizioni di salute psicofisica. In tale caso il Garante ha pure prescritto all'editore di unire copia della propria decisione inibitoria agli esemplari del servizio giornalistico oggetto della decisione, conservati presso lo stesso editore, e di dare conferma all'Autorità dell'avvenuto adempimento (*Provv.* 29 dicembre 2003).

La Dichiarazione del Consiglio d'Europa del 12 febbraio 2004

I principi richiamati dal Garante trovano conferma nella Dichiarazione del Consiglio d'Europa del 12 febbraio 2004, nella quale viene precisato, fra l'altro, come l'esigenza di bilanciare libertà di espressione e diritto al rispetto per la vita privata imponga di non rivelare particolari della vita privata delle figure pubbliche, a meno che tali informazioni non siano di diretto interesse pubblico per le modalità con cui tali soggetti svolgono o hanno svolto le funzioni alle quali sono state chiamati, e venga tenuta in debita considerazione la necesssità di non danneggiare terze persone.

La Decisione della Corte europea dei diritti dell'uomo sul "caso Craxi"

Da ultimo merita di essere ricordato che, nella nota vicenda relativa all'On. Bettino Craxi, l'Italia è stata condannata dalla Corte europea dei diritti dell'uomo di Strasburgo per violazione del diritto al rispetto della vita privata sancita dall'art. 8 della Convenzione europea dei diritti dell'uomo (Decisione 17 luglio 2003). La vicenda concerneva la diffusione di contenuti di intercettazioni telefoniche a carattere personale relative a conversazioni intrattenute dal *leader* del Partito socialista italiano nell'ambito di un procedimento penale a suo carico presso il Tribunale di Milano. I contenuti delle intercettazioni e i nomi degli interlocutori, infatti, erano stati letti in udienza dal pubblico ministero e successivamente diffusi dai giornali.

La Corte europea ha osservato che, nel caso in esame, le autorità italiane non hanno tutelato la riservatezza delle intercettazioni, né hanno svolto indagini efficaci sulle modalità con cui le conversazioni telefoniche private sono divenute di pubblico dominio. Secondo la Corte, inoltre, nell'ambito del processo, si sarebbe dovuto provvedere, in sede di udienza preliminare, ad escludere i passaggi delle conversazioni non necessari ai fini del procedimento. La pubblicazione degli stralci di inter-

cettazioni a contenuto strettamente personale, infine, è apparsa non necessaria rispetto alla legittima finalità di informare il pubblico.

15.4. Essenzialità dell'informazione

Anche nel periodo considerato, il Garante ha riscontrato violazioni delle norme deontologiche in relazione alla diffusione, nel contesto di una notizia di possibile rilevanza generale, di dati personali non essenziali, eccedenti e non pertinenti rispetto alla finalità del trattamento. In particolare, nel caso di un giornale che, riferendo di un delitto commesso in un appartamento, aveva pubblicato le generalità di colui che risultava essere proprietario dell'immobile, il Garante ha ritenuto insussistenti i presupposti –originalità del fatto, descrizione dei modi particolari in cui è avvenuto e qualificazione dei protagonisti (art. 6, comma 1, codice deontologico)– che consentono la divulgazione di informazioni anche dettagliate (*Provv.* 23 gennaio 2003).

Pure nella vicenda di un'emittente radiofonica che, commentando l'operato di un'agente della polizia municipale, ha diffuso, oltre alle generalità dell'agente, altri dettagli (e cioè l'età, il comune di residenza, l'indirizzo, nonché i nomi dei suoi genitori) si è constatata l'inosservanza del principio di non eccedenza rispetto al legittimo esercizio del diritto di critica e di cronaca sulla vicenda (*Nota* 23 febbraio 2004).

15.5. Dati idonei a rivelare lo stato di salute ovvero le opinioni politiche o filosofiche

Ripetuti sono stati i richiami del Garante al rispetto delle specifiche garanzie a tutela della riservatezza e della dignità delle persone malate, dettate dal codice deontologico per l'attività giornalistica (artt. 5 e 10). Ne è esempio emblematico la vicenda, di ampio clamore nei *media*, che ha avuto come protagonista una donna rifiutatasi di sottoporsi ad un intervento chirurgico ad una gamba ritenuto dai medici necessario per salvarle la vita. In tale occasione il Garante ha richiamato gli organi di informazione alla salvaguardia della dignità della persona malata, nonché al rispetto delle esigenze di riservatezza espresse dalla sua famiglia. L'Autorità ha inoltre evidenziato come la diffusione di indirizzi e dati personali dell'interessata, e l'insistenza nella ricerca di particolari sulla vicenda, finisse per lederne non solo la riservatezza, ma la stessa libertà di autodeterminazione nel maturare in silenzio e tranquillità una difficile scelta personale (cfr. *Comunicato stampa* 3 febbraio 2004).

Il Garante è stato chiamato ad occuparsi anche della pubblicazione –su taluni quotidiani e riviste– di elenchi di iscritti ad associazioni massoniche, nonché di altre informazioni ad essi relative (luogo di residenza e professione). Al riguardo, sono state chieste informazioni ai responsabili dei giornali, al fine di valutare la liceità e correttezza del trattamento, in special maniera sotto il profilo dell'essenzialità dei dati personali diffusi rispetto alla finalità di informare su fatti di interesse pubblico (*Note* 13 agosto 2003).

15.6. Esercizio dei diritti e giornalismo on line

Come già accennato più sopra (cfr. parag. 7.11.), il Garante ha chiarito che i diritti spettanti agli interessati in base all'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice) possono essere esercitati anche laddove il trattamento consista nella diffusione di fotografie e di altri dati personali attraverso pubblicazioni consultabili tramite Internet.

In particolare, nell'esaminare due ricorsi concernenti la stessa pubblicazione disponibile anche via *web*, nei quali le ricorrenti contestavano l'autenticità delle dichiarazioni di consenso acquisite dalla società che aveva originariamente raccolto i dati, il Garante ha posto l'accento sulla necessità che l'editore si accerti della genuina identità degli inserzionisti e dell'affidabilità del materiale informativo che intende utilizzare. L'Autorità ha ritenuto pertanto necessario approfondire in altra sede i presupposti di liceità del trattamento effettuato dall'editore e dalle altre società coinvolte nella vicenda.

Pubblicazione occasionale di articoli o saggi

La diffusione di dati personali tramite siti Internet può essere effettuata anche nell'ambito di attività di manifestazione del pensiero diverse dal giornalismo, compiute da soggetti che non esercitano professionalmente l'attività giornalistica, ma finalizzate anch'esse alla pubblicazione o diffusione occasionale di articoli, saggi ed altre manifestazioni del pensiero. Ai trattamenti di dati svolti nell'ambito di queste attività, secondo la disciplina della legge n. 675/1996 confermata dal Codice, si applicano le disposizioni previste per l'attività giornalistica. Si tratta di regole semplificate in materia di informativa e consenso, nonché di altre prescrizioni, contenute anche nel codice deontologico, volte a contemperare i diritti della persona con il diritto all'informazione ed alla libertà di espressione. Il principio è stato ribadito dall'Autorità nell'esaminare un ricorso relativo ad una vicenda in cui la pubblicazione di dati personali via *web* era stata effettuata tramite la riproduzione di una pagina originariamente creata dal ricorrente (*Provv.* 16 gennaio 2004). Il Garante ha inoltre precisato che la medesima disciplina è applicabile anche alla diffusione di dati derivanti da attività che si caratterizzano come modalità di esercizio del diritto di critica, con riferimento a personaggi conosciuti nell'ambito della "rete" (*Provv.* 10 dicembre 2003).

La libertà di iniziativa economica

16 Settore del credito finanziario e assicurativo

16.1. Credito

Nel 2003 il settore del credito è stato oggetto di particolare attenzione da parte del Garante, in special modo a seguito dei numerosi ricorsi, segnalazioni e reclami da parte di clienti di istituti di credito e di associazioni di consumatori, concernenti specialmente l'impropria divulgazione di dati personali da parte di uffici o dipendenti di banche.

Diversi cittadini si sono ad esempio lamentati delle particolari modalità con cui sono stati contattati telefonicamente da impiegati di istituti bancari per esigenze connesse allo svolgimento del rapporto bancario. In varie occasioni, infatti, addetti di istituto di credito, per mezzo del telefono, hanno comunicato a persone diverse dal diretto interessato informazioni relative al rapporto in essere o hanno addirittura sollecitato la regolarizzazione di situazioni di sofferenza, anche di lieve entità.

In altri casi, alcuni clienti hanno lamentato l'invio di comunicazioni bancarie in busta aperta (che ne ha reso conoscibile il contenuto da parte di terzi), oppure l'erroneo invio ad estranei di comunicazioni bancarie relative invece ai segnalanti e ad altri clienti.

In merito alle predette vicende, l'Autorità ha sottolineato in varie occasioni la necessità, per gli istituti di credito, di impartire precise istruzioni ai propri dipendenti ed incaricati e di predisporre apposite procedure per limitare al minimo indispensabile la divulgazione anche accidentale a terzi di dati personali dei clienti, non necessari per espletare le comunicazioni bancarie.

Per ciò che concerne, invece, l'esercizio dei diritti previsti dall'art. 13 della legge n. 675/1996 (ora, art. 7 del Codice), le questioni più rilevanti affrontate dall'Autorità nel settore del credito, anche in relazione alle novità normative, hanno riguardato il diritto di accesso ai dati personali del defunto e la gratuità dell'accesso, come già illustrato nella parte di questa *Relazione* specificamente dedicata al diritto di accesso ai dati personali (v. *supra*, parag. 7.7.).

16.2. Intermediazione finanziaria

Anche il settore dell'intermediazione finanziaria ha visto presentare, nel 2003, vicende di rilevante interesse per l'Autorità.

Trattamento di dati da parte di promotore finanziario

In particolare, merita di essere ricordato un caso che ha riguardato il trattamento di alcuni dati personali (compresi quelli relativi a rapporti bancari e finanziari) da parte di un promotore finanziario, pure incaricato in termini generali del trattamento da parte della banca titolare. Il promotore ha trattato i dati in discorso prima

che gli fosse formalmente richiesto di curare clienti già seguiti da altri promotori. Questo trattamento era finalizzato alla presa di contatto con i clienti per conto della banca, così da consentire la continuità del rapporto contrattuale.

In tale occasione il Garante ha segnalato alla banca la necessità e l'urgenza di specificare meglio ai promotori finanziari della propria rete di distribuzione l'ambito e le modalità del trattamento nella fase antecedente alla formale assegnazione dei clienti già seguiti da altri promotori, assicurando la puntuale osservanza delle istruzioni e dei compiti impartiti in proposito e rispettando i principi di necessità e pertinenza. L'Autorità ha inoltre prescritto alla banca di fornire ai clienti maggiori chiarimenti in ordine all'ambito ed alle modalità del trattamento in questione, con particolare riferimento alla possibile comunicazione dei loro dati personali ad un promotore finanziario, anche prima della sua formale investitura, nonché al ruolo rivestito dal promotore medesimo in tale fase.

16.3. "Centrali rischi" e società finanziarie

Nel 2003 si è registrato un ulteriore e significativo incremento delle istanze riguardanti il trattamento di dati personali relativi a richieste o a rapporti di finanziamento da parte di banche, società finanziarie e "centrali rischi" private. I numerosi ricorsi, segnalazioni e reclami hanno messo in luce soprattutto il mancato rispetto dei principi e degli obblighi richiamati nel provvedimento generale adottato in materia dal Garante il 31 luglio 2002.

La delicata materia del trattamento dei dati relativi ai sistemi di informazione gestiti da soggetti privati, ed utilizzati per il rilascio di crediti al consumo e la valutazione dell'affidabilità e puntualità nei pagamenti, è destinata a trovare nel più breve periodo una compiuta regolamentazione con il codice deontologico di cui è imminente la sottoscrizione.

Il codice deontologico

I lavori di tale codice hanno richiesto un notevole impegno soprattutto per la definizione dello schema delle nuove regole di comportamento che, dopo un ampio confronto con gli operatori interessati, è stato sottoposto alle valutazioni di soggetti e organismi controinteressati, in particolare delle associazioni dei consumatori e degli altri soggetti partecipanti ai lavori del codice. Lo schema, dopo la temporanea diffusione del suo contenuto anche tramite il sito *web* del Garante, verrà presto formalmente sottoscritto.

Le linee essenziali del codice deontologico riguarderanno in particolare:

- l'ambito soggettivo, con la precisazione delle categorie degli enti partecipanti e delle modalità con le quali gli stessi potranno accedere caso per caso alle singole tipologie di informazioni;

- le modalità con cui viene resa l'informativa agli interessati e le procedure adottate per consentire loro l'esercizio dei diritti di accesso e degli altri diritti ora previsti dall'art. 7 del Codice (d.lg. n. 196/2003);

- le modalità di trattamento relative all'utilizzo di tecniche o sistemi cd. di *credit scoring*, nonché le misure di sicurezza adottate per la protezione dei dati e dei sistemi informativi;

I cd. dati negativi

- i tempi di conservazione dei dati nei sistemi di rilevazione del rischio creditizio, con particolare attenzione alla distinzione tra le informazioni di tipo positivo e i cd. dati negativi (relativi, ad esempio, a morosità o sofferenze), nel rispetto dei principi in tema di consenso degli interessati e relativi casi di esclusione (tra cui, il bilanciamento degli interessi: v. art. 24, lett. *g)*, d.lg. n. 196/2003).

Cancellazione delle "sofferenze"

Proprio con riferimento a quest'ultimo aspetto, l'Autorità, a seguito dei ricorsi presentati da alcuni consumatori, ha ribadito la necessità di cancellare entro un anno dall'avvenuta regolarizzazione le segnalazioni relative a "sofferenze" successivamente sanate senza alcuna perdita per l'ente finanziatore, confermando l'illiceità di ogni ulteriore conservazione dei dati relativi a finanziamenti così estinti da un termine più lungo.

Non è stata poi ritenuta conforme ai principi espressi nel citato provvedimento generale del luglio 2002 l'annotazione da parte di una società, in via temporanea, della dicitura "regolarizzato", accanto al nominativo della ricorrente, per documentare l'integrale estinzione del debito: anche in tal caso si deve comunque procedere alla cancellazione integrale dei dati relativi a ritardi di pagamento regolarizzati senza debiti residui, che non possono essere ulteriormente conservati rispetto ai tempi indicati dal Garante (*Provv.* 12 marzo 2003 e 5 novembre 2003).

Il "diritto all'oblio" per i dati positivi

È stata quindi affrontata la questione della conservazione ed ulteriore comunicazione dei dati cd. positivi, che evidenziano un andamento regolare dei pagamenti degli interessati. Anche per questo tipo di dati è stato rivendicato il "diritto all'oblio": nelle decisioni adottate a seguito dei numerosi ricorsi presentati in proposito, si è confermato che, a prescindere dalla mancanza di specifiche annotazioni "negative" per l'interessato, i dati riferiti a tali posizioni estinte da tempo non possono essere ulteriormente trattati in assenza di un idoneo presupposto del trattamento, e in particolare del consenso dell'interessato (*Provv.* 5 novembre 2003 e 22 dicembre 2003).

Nonostante quanto puntualmente indicato nel citato provvedimento del 2002, la condotta di alcune finanziarie o "centrali rischi" private non è risultata in vari casi conforme alle relative prescrizioni e ciò ha determinato l'accoglimento anche parziale di innumerevoli ricorsi che continuano a caratterizzare buona parte del contenzioso pendente presso il Garante. L'Autorità si è anche costituita in giudizio in tutti i procedimenti instaurati dai predetti operatori allorché questi hanno impugnato decisioni del Garante, e seguirà con estrema attenzione l'affermazione dei principi di diritto già evidenziati, confidando comunque che il nuovo codice deontologico possa porre rapidamente fine in modo condiviso ad un quadro che non è ancora tranquillizzante per i cittadini interessati.

Comunicazione dei dati alla centrale rischi gestita dalla Banca d'Italia

Numerose sono state le istanze relative alle segnalazioni obbligatorie effettuate da banche e società finanziarie, anche a quelle riguardanti il sistema di centralizzazione dei rischi gestito dalla Banca d'Italia. In particolare, è stata lamentata la comunicazione di dati effettuata da parte di alcuni istituti di credito a tale centrale, erroneamente inseriti nella categoria di censimento "sofferenze". L'Autorità ha osservato che la comunicazione, da parte delle banche, alla centrale rischi gestita dalla Banca d'Italia dei dati di clienti relativi all'indicazione di un particolare stato contabile del rapporto, come quello ascrivibile alla categoria di "sofferenza", deve essere effettuata attenendosi scrupolosamente a quanto prescritto dalla stessa Banca d'Italia nelle

proprie istruzioni rivolte agli intermediari creditizi. In particolare, le istruzioni prevedono che la segnalazione di una sofferenza sia preceduta da un'attenta valutazione, da parte dell'intermediario, della complessiva situazione finanziaria del cliente e non possa invece scaturire automaticamente da un mero ritardo nei pagamenti.

In base a tali considerazioni, l'Autorità ha pertanto sollecitato gli istituti di credito ad adottare misure ed accorgimenti, anche organizzativi, idonei ad assicurare il pieno rispetto dei principi di correttezza, pertinenza e non eccedenza dei dati, nonché delle istruzioni per gli intermediari creditizi impartite dalla Banca d'Italia, in relazione alla comunicazione dei dati alla centrale rischi gestita da quest'ultima.

16.4. Anagrafe degli assegni bancari e postali

Anche l'archivio informatizzato degli assegni bancari e postali e delle carte di pagamento istituito ai sensi della legge n. 205/1999 e del d.lg. n. 507/1999 presso la Banca d'Italia, e in funzione dal giugno 2002, è interessato dalle novità introdotte dal d.lg. n. 196/2003, in materia, ad esempio, di trattamento dei dati giudiziari, dei diritti degli interessati e di misure di sicurezza.

Centrale d'allarme interbancaria

L'archivio, denominato Centrale d'allarme interbancaria (Cai), è composto, in primo luogo, da una sezione centrale presso la Banca d'Italia, che, oltre ai dati anagrafici degli interessati, contiene ulteriori segmenti relativi agli strumenti di pagamento presi in considerazione, assegni o carte di pagamento, ad informazioni rilevate riguardanti, ad esempio, smarrimenti o revoche, nonché ad eventuali sanzioni amministrative e penali. La Cai è inoltre composta da sezioni remote che riproducono, in tutto o in parte, l'intero archivio presso le banche, gli uffici postali e gli intermediari finanziari vigilati emittenti carte di pagamento, abilitati alla loro consultazione ed interessati all'individuazione di situazioni anomale od irregolari, anche rispetto alla propria clientela.

La Banca d'Italia e tali soggetti dovranno adeguarsi alle nuove disposizioni del Codice, con particolare riferimento alle attività di trasmissione e ricezione dei dati, nel rispetto del livello minimo di sicurezza previsto per i trattamenti di dati effettuati con l'ausilio di strumenti elettronici e per la gestione dei dati giudiziari (ciò per la parte dell'archivio relativa a sanzioni anche di natura penale).

Come ricordato nelle precedenti relazioni annuali, l'archivio risponde alla finalità di interesse generale di assicurare il regolare funzionamento del sistema dei pagamenti e viene alimentato da soggetti pubblici (autorità giudiziaria e Ministero dell'interno) e privati (banche, uffici postali, società emittenti carte di credito), tenuti a trasmettere i provvedimenti o le segnalazioni riguardanti sia persone che hanno emesso assegni senza autorizzazione o provvista, sia titolari di carte di pagamento revocate (per mancato pagamento o costituzione di fondi), sia, ancora, carte di pagamento o assegni sottratti, smarriti, o bloccati.

Nei confronti delle persone i cui nominativi risultano iscritti nella Cai, vi è un obbligo, per la banca, di revoca dell'autorizzazione ad emettere assegni, con un divieto che si estende anche agli altri istituti di credito per non meno di sei mesi.

Nel 2003 sono pervenute all'Autorità diverse segnalazioni relative al trattamento dei dati personali effettuato da alcune banche, uffici postali e società di carte di

pagamento nell'ambito della Cai. È aumentato anche il numero delle istanze presentate dagli interessati al fine di ottenere l'accesso, la rettificazione o la cancellazione dei dati iscritti nell'archivio. In particolare, è stato lamentato che la segnalazione nell'archivio avviene spesso senza rispettare i termini previsti per il dovuto preavviso, oppure a fronte di meri errori o disguidi nei pagamenti.

Segnalazione di scoperti di lieve importo

In relazione all'utilizzo di carte di pagamento, si rileva che taluni automatismi segnalati, relativi all'iscrizione in Cai anche per scoperti di conto corrente di lieve importo, rischiano di penalizzare i clienti che non riuscirebbero a tutelare in maniera tempestiva i propri diritti anche a causa dell'assenza (diversamente da quanto accade per gli assegni) di precise indicazioni circa le modalità di preavviso dell'eventuale revoca della carta di pagamento. Tali profili saranno oggetto d'esame nei prossimi mesi, anche nell'ambito della collaborazione avviata con la Banca d'Italia in questa materia sin dalla fase di istituzione dell'archivio.

16.5. Assicurazioni

Il settore assicurativo continua ad essere interessato da novità normative che si riflettono sulla materia della protezione dei dati personali. A tal proposito si può fare accenno, in primo luogo, al d.m. n. 74/2004 sull'accesso agli atti delle imprese di assicurazione (v. *infra*, parag. 45.2.). Merita pure di essere ricordato l'art. 120 del Codice, il quale riproduce le disposizioni dell'art. 2, commi 5-*quater* e 5-*quinquies*, della legge n. 137/2000, recanti l'istituzione, presso l'Isvap, di una banca dati dei sinistri relativi all'assicurazione obbligatoria per i veicoli a motore immatricolati in Italia, al fine di rendere più efficace la prevenzione ed il contrasto di comportamenti fraudolenti in tale settore (per le procedure e le modalità di funzionamento della banca dati, nonché di accesso alle informazioni in essa contenute, cfr. il provvedimento Isvap n. 2179 del 10 marzo 2003, già menzionato nella *Relazione* 2002).

Anche l'annunciata emanazione di un "Codice delle assicurazioni private", allo studio del Ministero per le attività produttive, potrebbe offrire l'occasione per approfondire alcuni aspetti dell'attività assicurativa che hanno delle implicazioni sulla protezione dei dati personali.

L'Autorità ha avviato una nuova riflessione con l'associazione di categoria, per esaminare alcune problematiche del settore connesse all'entrata in vigore del Codice, nonché per risolvere questioni da tempo evidenziate dagli operatori.

Il problema della "catena assicurativa"

In particolare, questi ultimi hanno sostenuto che la formulazione dell'informativa agli interessati dovrebbe tenere in considerazione le peculiari caratteristiche dei trattamenti effettuati in questo settore e la complessa struttura della "catena assicurativa". In proposito si deve peraltro osservare che, anche nel 2003, l'Autorità ha avviato l'esame di numerosi reclami e segnalazioni riguardanti carenze nelle informative fornite dalle società di assicurazioni a clienti o a soggetti cui liquidare i sinistri, carenze che –si ricorda– si riflettono sulla validità del consenso manifestato dagli interessati. La necessità di rivedere i modelli di informativa si pone anche nei casi, frequenti, in cui l'impresa di assicurazioni intenda acquisire, con uno stesso modulo, il consenso ai diversi trattamenti effettuati da altri autonomi titolari dei trattamenti.

L'Autorità ha comunque confermato la propria disponibilità a fornire un ausilio per la predisposizione di un idoneo modulo *standard* di informativa delle imprese

alla clientela (in analogia con quanto avvenuto per le banche), nonché ad affrontare alcuni delicati problemi interpretativi concernenti i presupposti di liceità del trattamento di dati sensibili, in particolare quelli sanitari.

Sempre nel merito dell'attività svolta dall'Autorità nel settore, va inoltre ricordata la segnalazione di un assicurato che aveva chiesto il rimborso della penale prevista per l'annullamento di un viaggio prenotato anche per conto di altre persone e poi annullato per la malattia di un congiunto di un compagno di viaggio. L'impresa di assicurazioni ha negato il rimborso a causa della mancata acquisizione della cartella clinica del malato, il cui esame, sarebbe stato a suo avviso necessario per verificare se la patologia che aveva determinato l'annullamento del viaggio rientrava o meno tra i rischi assicurati.

Al riguardo l'Ufficio del Garante ha in primo luogo richiamato la disposizione (art. 3 legge n. 675/1996, ora, art. 5, comma 3, d.lg. n. 196/2003), in base alla quale il trattamento di dati effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione della normativa sulla protezione dei dati solo se i dati sono destinati alla comunicazione sistematica o alla diffusione. Nel caso esaminato, si è pertanto constatata l'inapplicabilità di tale normativa alla raccolta ed al trattamento di dati personali anche sensibili relativi a compagni di viaggio –e relativi familiari– del segnalante, effettuati da quest'ultimo, pure per conto di altri, per prenotare il viaggio. Ad identica conclusione si è giunti per quanto riguarda la comunicazione all'impresa di assicurazione della documentazione necessaria al rimborso della penale conseguente all'annullamento del viaggio, visto il carattere non sistematico della comunicazione.

Inoltre, l'Autorità ha ritenuto indebita la peculiare forma di acquisizione dei dati consistente nell'esercizio, da parte del segnalante o di altri soggetti, del diritto di accesso alla cartella clinica detenuta dalla struttura ospedaliera presso cui la persona interessata è stata ricoverata. Infatti, alla luce dell'art. 60 del Codice e dei principi richiamati dal Garante nel provvedimento del 9 luglio 2003 (su cui v. *infra* lo specifico paragrafo 19.2.), l'accesso alle cartelle cliniche detenute presso strutture sanitarie deve ritenersi consentito solo se la situazione giuridica che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale o inviolabile. Ciò non si era invece verificato nel caso segnalato, in cui il diritto fatto valere aveva ad oggetto unicamente la pretesa al rimborso della penale pagata al *tour operator* in seguito all'annullamento del viaggio. A breve, l'Autorità valuterà nuovamente la questione all'esito del riscontro chiesto all'impresa assicurativa.

Trattamento di dati idonei a rivelare lo stato di salute

Infine, l'Autorità è tornata ad esaminare il problema dei limiti di ammissibilità del trattamento di dati idonei a rivelare lo stato di salute da parte delle imprese di assicurazione, in relazione alla gestione del contratto assicurativo ed all'acquisizione dei dati di assicurati o di terzi.

Sul punto, si è ribadita la liceità della raccolta di dati sanitari contenuti in cartelle cliniche degli assicurati qualora tali dati siano strettamente necessari per fornire le specifiche prestazioni richieste dagli interessati. Si è tuttavia osservato che, in ossequio a quanto stabilito dalla legge (art. 26, comma 1, del Codice) e dalle autorizzazioni generali nn. 2/2002 e 5/2002 (efficaci sino al 30 giugno 2004), la previsione contrattuale dell'onere di fornire, ai fini del rimborso, copia della cartella clinica in

caso di ricovero, è comunque subordinata anche all'acquisizione del consenso scritto dell'interessato al quale si riferiscono i dati contenuti nella cartella. Il consenso deve essere preceduto da idonea informativa e deve avere specifico riguardo al trattamento dei dati sanitari. Rispetto alla vicenda analizzata, sono state pertanto ritenute inoperanti le ipotesi equipollenti al consenso individuate dalla normativa (v. l'art. 26, comma 4, del Codice).

In ogni caso, come si è detto, la raccolta ed il successivo trattamento dei dati sanitari devono essere effettuati in conformità ai principi di indispensabilità, pertinenza e non eccedenza dei dati rispetto alle finalità perseguite (art. 11 del Codice) e ciò proprio con riguardo alla stretta necessità per l'impresa di assicurazione di acquisire copia integrale di una cartella clinica ai fini della liquidazione di un sinistro. La stessa acquisizione dell'intera cartella clinica può non essere rispettosa di tali principi poiché tale documento, insieme ad elementi che potrebbero essere necessari ai fini delle verifiche effettuate dalla società di assicurazione per procedere al rimborso richiesto dall'assicurato (riguardo, ad esempio, ad informazioni che permettono di stabilire la natura della malattia, documentabile in modo idoneo con modalità alternative), contiene ulteriori dati di carattere sanitario che possono non avere alcun rilievo ai fini delle verifiche e che devono essere quindi stralciati.

Comunicazione dei dati contenuti nelle perizie medico-legali

Va ricordato anche in questo paragrafo che il Garante ha riaffermato più volte il principio (ora confermato anche nel citato d.m. del 2004) secondo cui le informazioni personali comprese nelle valutazioni e negli altri elementi di giudizio riportati nelle perizie medico-legali delle compagnie di assicurazione rientrano nella sfera dei dati personali e vanno pertanto comunicate all'interessato quando questi ne faccia richiesta. La questione è stata affrontata in dettaglio nella parte della *Relazione* specificamente dedicata al diritto di accesso ai dati personali, cui si fa rinvio (parag. 7.9.; cfr. pure parag. 50.1.)

17 *Marketing*

Numerosi reclami e quesiti hanno confermato la forte sensibilità di consumatori rispetto alle intrusioni nella propria vita privata derivanti dall'adozione di nuovi strumenti e strategie di commercializzazione di prodotti o servizi.

In particolare, nel corso dell'anno sono stati sottoposti al Garante diversi episodi di ricezione di lettere, telefonate ed altre comunicazioni indesiderate da parte di operatori di *direct marketing*, soprattutto nell'ambito di attività di promozione di carte di credito.

Utilizzo delle liste elettorali a fini di *marketing*

Per quanto riguarda, poi, la prassi, diffusa tra gli operatori commerciali, di attingere dati personali da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per intraprendere operazioni di *marketing*, il Garante ha evidenziato alcune importanti novità introdotte nel settore in esame dal Codice. L'art. 177, comma 5, del d.lg. n. 196/2003 ha, infatti, modificato le norme relative all'utilizzabilità delle liste elettorali, prevedendo che tali liste possano essere accessibili e rila-

sciate in copia solo "in applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca scientifica o storica, o a carattere socio-assistenziale" o, ancora, per la tutela di un interesse collettivo o diffuso. Perciò, le liste elettorali, sebbene di formazione "pubblica", non possono più essere sfruttate per scopi commerciali o pubblicitari, a differenza di quanto era consentito alla luce della disciplina in vigore fino al 31 dicembre scorso, che dava invece la possibilità a chiunque di copiarle, stamparle o metterle in vendita.

In ambito diverso, oggetto anch'esso di approfondita analisi, il Garante ha poi autorizzato una casa editrice, previa fissazione di limiti e garanzie, a trattare eventuali dati sensibili forniti spontaneamente all'atto della formulazione di quesiti rivolti ad esperti di vari settori, da parte delle persone che richiedono servizi di consulenza *on line* offerti a pagamento attraverso siti e pagine *web* di testate giornalistiche.

Consulenze *on line* e dati sensibili

L'Autorità, nel richiamare la casa editrice al rispetto dell'autorizzazione generale n. 2/2002 riguardante i dati idonei a rivelare lo stato di salute e la vita sessuale, ha autorizzato il trattamento di altri dati sensibili, eventualmente rilasciati, soltanto se realmente pertinenti all'argomento trattato o al quesito posto, oltre che indispensabili per fornire il servizio di consulenza *on line*. Alla società istante è stato, quindi, prescritto di inserire in modo visibile, nell'informativa fornita agli utenti, l'invito a non indicare nei quesiti dati di carattere sensibile non strettamente necessari per la risposta.

Nell'eventualità, poi, che la domanda e la risposta siano inserite, previo consenso dell'utente, negli spazi consultabili liberamente dal pubblico (ad esempio in una rubrica delle domande più frequenti, cd. *faq*), l'Autorità ha imposto alla società di verificare prima della loro pubblicazione che, oltre al nome ed all'indirizzo *e-mail* dell'interessato, non vi compaiano altri dati, anche diversi da quelli sensibili, che possano rendere identificabile l'utente. Gli esperti *on line* –designati responsabili del trattamento– devono perciò controllare che nelle risposte pubblicate non vi sia alcun elemento che permetta di risalire all'identità della persona che ha richiesto la consulenza. Essi devono ricevere poi adeguate istruzioni in merito alla necessità di verificare la pertinenza dei dati sensibili riportati nei quesiti, in vista della loro eliminazione ove non necessari per la prestazione del servizio.

Nel periodo di riferimento, sono stati anche completati gli accertamenti (v. *Relazione* 2002, p. 104) riguardanti la raccolta e il trattamento dei dati personali nell'ambito della distribuzione nei supermercati di carte di fidelizzazione della clientela per promuovere operazioni a premi o sconti. È quindi imminente l'adozione di un provvedimento di carattere generale su tale tematica, per richiamare l'attenzione di quanti ricorrono a tali iniziative sulla necessità di riformulare alcuni modelli di informativa agli interessati e di richiesta del consenso, e di adottare altre misure necessarie per conformare alle leggi i trattamenti di dati.

Profilazione della clientela

Dall'istruttoria svolta è già emersa la necessità di far assicurare il rispetto della normativa sulla *privacy* nei casi di trattamento dei dati con finalità di profilazione della clientela, quando, cioè, sulla base dei volumi di spesa e delle tipologie di prodotti acquistati dai singoli clienti, vengono predefinite determinate categorie o gruppi di consumatori abituali o meno, per procedere poi alla realizzazione di promozioni ed offerte ad essi mirate (volte a premiare la frequenza di visita, a promuovere l'acquisto di determinati prodotti, ecc.).

È stata peraltro già rilevata la tendenza di alcune società ad effettuare in tutto o in parte il trattamento dei dati dei clienti in forma prevalentemente anonima.

Particolare rilevanza riveste poi, per il settore in esame, la prossima definizione del codice di deontologia relativo al trattamento dei dati personali a scopo di *marketing* diretto e di invio di materiale pubblicitario, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale. Tale codice dovrà, infatti, prevedere a breve forme semplificate per la manifestazione del consenso da parte dell'interessato, ovvero per rendere meglio conoscibile la sua eventuale opposizione all'invio di determinate comunicazioni commerciali.

Codice di condotta proposto dalla Fedma

A livello europeo si segnala infine l'approvazione, a seguito della consultazione delle parti interessate, del codice di condotta proposto dalla Federazione europea del *marketing* diretto. Nel Parere 3/2003 del 13 giugno 2003, il Gruppo istituito dall'art. 29 della direttiva n. 95/46/CE ha ritenuto il codice di condotta conforme alla direttiva sulla protezione dei dati ed alle disposizioni nazionali di attuazione. Il codice in questione affronta i problemi specifici della protezione dei dati nel settore del *marketing* diretto e propone alcune soluzioni.

19 Trasparenza dell'attività amministrativa

La necessità di bilanciare il principio di trasparenza dell'attività amministrativa, sancito dalla legge n. 241/1990 e da altre disposizioni di settore (per gli enti locali, cfr. l'art. 10, comma 1, del d.lg. n. 267/2000) con quello di tutela della riservatezza continua a rappresentare una delle problematiche che più di frequente vengono sottoposte all'attenzione del Garante.

Di tale tematica si è già dato parzialmente conto più sopra (cfr. parag. 8.2.), in riferimento all'esercizio, ad opera degli interessati, del diritto alla cancellazione dei dati trattati in violazione di legge. In quella sede si è detto che un criterio guida del bilanciamento tra riservatezza e trasparenza dell'attività amministrativa è stato individuato dall'Autorità anche nel rispetto dei principi di pertinenza e non eccedenza.

Pubblicità delle deliberazioni comunali e divieto di diffusione dei dati sulla salute

Con particolare riferimento agli enti locali, l'Autorità ha ribadito poi in varie occasioni che, sebbene la normativa preveda la pubblicità per le deliberazioni comunali attraverso la loro affissione all'albo pretorio, nel caso in cui esse contengano dati sulla salute occorre tenere presente il divieto di diffusione di tali informazioni (art. 23, comma 4, legge n. 675/1996; ora, art. 22, comma 8, d.lg. n. 196/2003). L'ente può quindi utilizzare unicamente diciture generiche, codici numerici o lettere puntate che impediscano di giungere all'identificazione dell'interessato, attraverso una nuova tecnica di redazione dei provvedimenti soggetti ad obbligatoria pubblicazione, che lascia comunque impregiudicato il diritto dei controinteressati ad accedere in conformità ai presupposti di legge, presso gli uffici dell'ente, ai dati sensibili (da omettere, invece, nella delibera diffusa ad un pubblico indeterminato).

Anche in riferimento ad altri momenti della vita amministrativa, le amministrazioni sono tenute in termini più generali a selezionare con particolare attenzione i dati personali, specie se di tipo sensibile o attinenti a vicende giudiziarie, la cui menzione sia effettivamente necessaria per perseguire, nei singoli casi, le finalità di trasparenza delle attività dei propri organi, nel rispetto dei principi di pertinenza e non eccedenza (art. 9 legge n. 675/1996; ora, art. 11 d.lg. n. 196/2003).

La necessità del rispetto di tali principi, quale criterio che deve concorrere al bilanciamento tra le esigenze di riservatezza e quelle di trasparenza dell'attività amministrativa, è stata ribadita anche in altre circostanze.

Così, nel caso di un ente locale (che aveva riportato su un manifesto affisso per le vie del comune l'ordine del giorno di una seduta del consiglio comunale, contenente vari dati personali riferiti ad un dipendente e ad una vicenda giudiziaria che lo vedeva coinvolto), l'Autorità ha ritenuto contraria al principio di non eccedenza l'indicazione dettagliata di informazioni personali, sebbene in forma di pubblicazione effettuata legittimamente dall'amministrazione. L'avviso pubblico destinato all'affissione avrebbe dovuto infatti contenere soltanto la menzione dell'oggetto e degli estremi della pronuncia giudiziaria di interesse, e non anche il nominativo delle parti interessate. La documentazione integrale poteva, invece, essere comunicata ai consiglieri comunali, ai quali va garantita, ai sensi dell'art. 39, comma 4, del d.lg. n. 267/2000, un'informazione adeguata e preventiva sulle questioni sottoposte

al consiglio, per consentire loro l'espletamento dei propri compiti istituzionali (*Provv.* 9 dicembre 2003).

Analogamente, non è stata giudicata proporzionata l'introduzione, in una deliberazione comunale riguardante una controversia che opponeva l'amministrazione alla ricorrente, del testo integrale di una relazione dell'ufficio legale nella quale era riportata una serie di dati personali concernenti la ricorrente stessa. La relazione, che indicava tra l'altro nel dettaglio le richieste di risarcimento del danno formulate dall'interessata nei confronti del comune, avrebbe potuto essere infatti riportata in sintesi, oppure semplicemente riassunta nella deliberazione, senza con ciò pregiudicare l'obbligo di adeguata motivazione degli atti amministrativi (art. 3, comma 3, legge n. 241/1990) e rimanendo pur sempre accessibile ai controinteressati, nella sua versione integrale, in base alle norme vigenti in materia (*Provv.* 17 aprile 2003).

È stato per altro verso considerato non contrastante con la normativa sulla riservatezza il rilascio ad organi interni al consiglio comunale, come ad esempio una commissione trasparenza, di determinati verbali di accertamento e di alcuni altri atti stilati dalla locale polizia municipale. In particolare, è stata riconosciuta a tale organo la possibilità di accedere anche a taluni documenti contenenti dati di natura sensibile, tenuto pure conto del fatto che lo svolgimento delle funzioni di controllo, di indirizzo politico e di sindacato ispettivo (nonché di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per consentire l'espletamento di un mandato elettivo), rientra tra le attività di rilevante interesse pubblico per il cui perseguimento è permesso il trattamento di questa categoria di informazioni (*Nota* 13 maggio 2003).

Registrazione di sedute del consiglio comunale

In merito alla pubblicità degli atti e delle sedute del consiglio comunale, l'Autorità ha anche precisato che un consigliere comunale può registrare con l'ausilio di strumenti propri le sedute dell'assemblea consiliare a condizione che, quando la registrazione, in ipotesi particolari, è effettuata per fini esclusivamente personali, i dati non siano destinati alla comunicazione sistematica o alla diffusione, e quando invece è (più spesso) effettuata per scopi diversi, gli interessati siano posti previamente in condizione di essere informati (*Nota* 23 aprile 2003).

Gli obblighi previsti in materia di informativa comportano peraltro che le amministrazioni pubbliche rendano conoscibile agli interessati, con modalità adeguate, anche il trattamento dei dati che li riguardano effettuato a fini istituzionali. In questo senso, può non contrastare con la normativa sulla protezione dei dati la verifica, per motivi di sicurezza, dell'identità delle persone che accedono ad uffici pubblici, purché sia resa l'informativa agli interessati, anche tramite modalità semplificate (ad esempio, mediante l'affissione di avvisi chiari e sintetici), e siano osservati rigorosamente i principi di pertinenza e di non eccedenza dei dati raccolti con particolare riferimento alla mera verifica dell'identità, all'annotazione degli ingressi oppure alla (spesso contestata) prassi di fotocopiare documenti (*Nota* 23 aprile 2003).

Sulla questione della raccolta di dati identificativi degli interessati, è stata infatti completata l'istruttoria sulla prassi adottata da alcuni soggetti pubblici di raccogliere e registrare dati personali mediante l'acquisizione della copia fotostatica di un documento di identità personale, a scopi di sicurezza (come avviene per i dati personali dei visitatori raccolti all'ingresso degli edifici sede di uffici pubblici), o addirittura "statistici", sia nel caso in cui la copia del documento di riconoscimento venga

acquisita per adottare atti o provvedimenti richiesti dal cittadino. La problematica sarà definita entro breve termine con la formulazione di utili prescrizioni al riguardo.

19.1. Accesso ai documenti amministrativi

L'Autorità è stata interpellata innumerevoli volte in merito alle problematiche relative al diritto di accesso agli atti amministrativi che, come ribadito in più occasioni anche alla luce della consolidata giurisprudenza, costituisce ancora una delle più significative applicazioni del principio di trasparenza (cfr., da ultimo, C.d.S. Sez. VI, 9 gennaio 2004, n. 14).

Dati personali contenuti in esposti e denunce

A tal proposito, è stato rilevato (*Nota* 16 maggio 2003) che i principi di pertinenza e non eccedenza non permettono di riportare sugli atti di avvio degli accertamenti in materia di abusi edilizi alcuni dati personali contenuti negli esposti che hanno dato origine all'accertamento. Sebbene le persone interessate possano avere accesso agli atti che li riguardano, compresi, in determinate circostanze, anche eventuali esposti o denunce presentati contro di esse, una pubblicità indifferenziata del contenuto degli esposti non può ritenersi conforme ai principi in materia di protezione dei dati, come peraltro confermato anche dalla giurisprudenza amministrativa (C.d.S. Sez. V, 3 aprile 2000, n. 1916).

Elenchi di intestatari di contratti di fornitura di pubblici servizi

L'Autorità è stata anche chiamata a precisare ulteriormente il rapporto tra il diritto di accesso e quello alla protezione dei dati personali, con particolare riferimento alla possibilità per i comuni di accedere ad elenchi dettagliati detenuti dalle società concessionarie dell'erogazione di pubblici servizi, recanti gli intestatari di contratti di fornitura. Al riguardo è stato evidenziato che i soggetti privati possono comunicare i dati personali con il consenso degli interessati, ovvero in presenza di uno degli altri presupposti di liceità, come ad esempio l'adempimento di un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria. In particolare, si può prescindere dal consenso dell'interessato nel caso in cui sussistano esigenze di istituzione o completamento del catasto degli impianti termici, poiché l'art. 17 del d.P.R. n. 551/1999 ha espressamente previsto che le società distributrici di combustibile comunichino agli enti locali che ne facciano richiesta la titolarità degli impianti da esse riforniti nel corso degli ultimi dodici mesi (*Nota* 1° marzo 2004).

Occorre infine segnalare che è allo studio dell'Autorità la predisposizione di un nuovo provvedimento sulla delicata questione del diritto di accesso dei consiglieri comunali e provinciali, già oggetto di varie pronunce in casi specifici.

19.2. Il principio del cd. pari rango

L'esperienza applicativa ha individuato da tempo alcuni opportuni presupposti per bilanciare il diritto alla riservatezza e il diritto di accesso ai documenti amministrativi, specie quando i documenti contengono dati attinenti alla salute o alla vita sessuale.

La questione dei limiti alla comunicazione di dati sulla salute e sulla vita sessuale a persone diverse dall'interessato ha assunto, non di rado, rilevanza nel caso di richieste di accedere a cartelle cliniche detenute presso strutture sanitarie, a volte formulate da un difensore nell'ambito delle cd. indagini difensive (art. 391-*quater* c.p.p.).

Con riferimento al caso in cui una pubblica amministrazione riceva una richiesta di accesso a documenti amministrativi contenenti tale tipo di dati, il Codice (art. 60), risolvendo alcuni dubbi interpretativi sorti sulla base delle disposizioni previgenti (art. 16 d.lg. 11 maggio 1999, n. 135), dispone che il trattamento dei dati finalizzato a permettere l'accesso è consentito se la situazione giuridica che si intende tutelare con la richiesta di accesso ai documenti amministrativi è "di rango almeno pari ai diritti dell'interessato", ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile.

Ad identica valutazione sul "rango" della situazione soggettiva fatta valere sono tenuti i soggetti privati nel caso in cui sia loro richiesto di comunicare a terzi singole informazioni sulla salute e sulla vita sessuale dell'interessato, come evidenziato dal Garante in una vicenda riguardante una casa di cura privata (*Nota* 4 settembre 2003).

La valutazione del "rango" della situazione soggettiva

In tutte queste ipotesi il destinatario della richiesta, per decidere se accogliere anche in parte l'istanza di comunicazione di dati o di accesso ai documenti, deve previamente verificare in concreto se il diritto che si intende far valere o difendere sulla base delle informazioni o della documentazione richiesta sia almeno "di pari rango" rispetto al diritto alla riservatezza, alla dignità ed agli altri diritti e libertà fondamentali dell'interessato. La comunicazione di dati che rientrano nella sfera di riservatezza dell'interessato può, in definitiva, ritenersi giustificata e legittima solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti fondamentali ed inviolabili.

Questa significativa affermazione, ora espressamente confermata dal Codice (artt. 26, comma 4, lett. *c)*, 60, 71 e 92, comma 2, d.lg. n. 196/2003), è contenuta in un provvedimento del 9 luglio 2003 dell'Autorità, con il quale sono stati forniti alcuni criteri guida che devono caratterizzare il bilanciamento delle diverse situazioni coinvolte.

Provvedimento del 9 luglio 2003 (cd. pari rango)

In tale provvedimento si fa riferimento in particolare alla richiesta di accesso, da parte di persone diverse dall'interessato, alla cartella clinica di quest'ultimo (che può presentare delicate informazioni riferite talvolta anche ad individui diversi dall'interessato: si pensi alle anamnesi familiari), accanto ad altre considerazioni utili per altri tipi di documenti detenuti in ambito pubblico o privato.

Si è così precisato che:

- la comunicazione all'interessato di dati personali sulla salute va effettuata solo per il tramite di un medico (art. 23, comma 2, legge n. 675/1996; vedi però, ora, art. 84 d.lg. n. 196/2003, in riferimento agli esercenti le professioni sanitarie e agli organismi sanitari);

- occorre avere presente, quale elemento di raffronto per il bilanciamento degli interessi, non già, in sé considerato, il diritto alla tutela giurisdizionale, che pure è costituzionalmente garantito, bensì il diritto soggettivo sottostante, che si intende far valere sulla base del materiale documentale di cui si vorrebbe avere conoscenza;

- la valutazione sui diritti soggettivi va fatta in concreto, così da evitare "il rischio di soluzioni precostituite poggianti su una astratta scala gerarchica

dei diritti in contesa" (nello stesso senso, C.d.S. Sez. VI, 30 marzo 2001, n. 1882 e 9 maggio 2002, n. 2542; cfr. pure C.d.S. Sez. V, 31 dicembre 2003, n. 9276);

- oltre a verificare, anche nell'ottica di un eventuale accoglimento parziale della richiesta, l'effettiva necessità dei dati ai fini dell'azione o della difesa, occorre osservare comunque i principi di pertinenza e di non eccedenza nel trattamento, al cui rispetto sono tenuti pure i soggetti pubblici (artt. 3-4 d.lg. n. 135/1999; ora, art. 22 d.lg. n. 196/2003);

- se la richiesta è rivolta ad una amministrazione pubblica, nel procedimento instaurato dall'istanza di accesso dovrebbe essere poi informato l'interessato, stimolando un "contraddittorio anticipato" che ponga in condizione quest'ultimo di esercitare i propri diritti ed eventualmente opporsi per motivi legittimi al trattamento delle informazioni che lo riguardano;

- i medesimi criteri devono essere seguiti nel caso in cui la richiesta di accesso o di comunicazione di dati sia formulata da un difensore che abbia ricevuto specifico incarico, anche ai sensi della normativa sulle investigazioni difensive (così la *Nota* 10 dicembre 2003).

Il limite del "pari rango", ad ogni modo, non trova applicazione nel caso di accesso ai dati personali direttamente da parte dell'interessato e per il rilascio di copia della cartella clinica all'interessato medesimo o a persona da lui specificamente delegata (o ancora, in caso di decesso, a chi "ha un interesse proprio o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione": art. 9, comma 3, d.lg. n. 196/2003). Deve trattarsi comunque di un esercizio del diritto di accesso frutto di una libera determinazione da parte dell'interessato e non di una costrizione, come quella che potrebbe venire da una controparte più "forte", nel quadro ad esempio di un rapporto di lavoro o contrattuale.

20 Tessera elettorale

Le problematiche connesse ai dati personali da riportare nella tessera elettorale continuano ad essere seguite con attenzione dall'Autorità. Tale documento, che ha sostituito in via permanente il certificato elettorale, è stato sinora realizzato solo in forma cartacea (d.P.R. 8 settembre 2000, n. 120), sebbene l'art. 13 della l. 30 aprile 1999, n. 120 avesse previsto l'adozione, in via sperimentale, della carta d'identità elettronica con funzioni anche elettorali.

Profili critici

Il Garante ha già espresso in passato il proprio giudizio critico sull'utilizzo del formato cartaceo anziché del supporto informatico, anche alla luce delle caratteristiche del modello cartaceo approvato, nonché della circostanza che la tessera è in ipotesi utilizzabile per diciotto consultazioni elettorali e/o referendarie e presenta vari spazi per apporre timbri che certificano la partecipazione al voto. Tutto ciò

rende conoscibili diversi dati relativi ai comportamenti dell'interessato in occasione delle consultazioni e, in date condizioni, gli stessi suoi orientamenti.

Nel corso del 2003 sono state affrontate anche questioni più di dettaglio, come la richiesta di cancellazione dai documenti elettorali del nome del coniuge separato. In argomento, l'Autorità ha ritenuto conforme alla normativa sulla protezione dei dati personali il diniego opposto dalle autorità locali a tali richieste di cancellazione, poiché la disciplina di settore prevede espressamente che sulla tessera elettorale il cognome delle donne coniugate possa essere seguito da quello del marito (art. 2 d.P.R. n. 299/2000). Inoltre, secondo gli artt. 156-*bis* c.c. e 5, secondo comma, della legge n. 898/1970, la donna, che durante la separazione personale dei coniugi conserva (salvo diverso provvedimento del giudice) il cognome del marito aggiunto al proprio per effetto del matrimonio, lo perde solamente a seguito della sentenza di scioglimento o cessazione degli effetti civili del matrimonio.

21 Documentazione anagrafica e materia elettorale

Anche nel periodo di riferimento sono pervenuti numerosi quesiti sulle modalità di trattamento dei dati contenuti nei registri anagrafici, negli atti dello stato civile e nelle liste elettorali.

Significativa è stata ad esempio l'indicazione fornita dall'Autorità circa la possibilità di affidare la funzione di lettura ottica tramite *scanner* degli atti contenuti nei registri dello stato civile ad un soggetto esterno all'amministrazione comunale, designato quale responsabile del trattamento e sulla base di attente istruzioni, concernenti anche la sicurezza dei dati. Il comune deve poi vigilare sull'osservanza di tali istruzioni e sul più generale rispetto delle norme in materia di protezione dei dati personali, anche tramite verifiche periodiche, e può pure prevedere che sia il responsabile a designare, all'interno della propria struttura, i soggetti aventi legittimo accesso ai dati personali in qualità di incaricati del trattamento (*Nota* 23 aprile 2003).

Conoscibilità dei dati anagrafici

L'Autorità è stata nuovamente interpellata anche sulla possibilità per i comuni di comunicare a privati le informazioni contenute negli archivi anagrafici, e così, ad esempio, di dare una notizia sul comune di emigrazione di una persona già iscritta all'anagrafe. In proposito, si è ribadito ancora una volta che la normativa sulla protezione dei dati non ha modificato espressamente la disciplina vigente in materia di stato civile e anagrafi, secondo cui –a parte la comunicazione dei dati anagrafici, resi anonimi ed aggregati, agli interessati che ne facciano richiesta, per fini statistici e di ricerca– possono essere rilasciati, a chi lo richieda, solo i certificati concernenti la residenza o lo stato di famiglia. Ai sensi dell'art. 33, comma 2, del d.P.R. n. 223/1989, ogni altra posizione desumibile dagli atti anagrafici (quindi, pure l'informazione sul comune di emigrazione) resta attestabile o certificabile, qualora non vi ostino gravi o particolari esigenze di pubblico interesse, dall'ufficiale di anagrafe, d'ordine del sindaco (*Nota* 4 giugno 2003).

Uso degli elenchi anagrafici per finalità di comunicazione istituzionale

In merito al trattamento dei dati contenuti negli elenchi anagrafici, il Codice ha peraltro, integrato la disciplina di settore, che consente l'utilizzo di questi elenchi da parte delle pubbliche amministrazioni esclusivamente per scopi di pubblica utilità (art. 34, comma 1, d.P.R. n. 223/1989). L'art. 177, comma 1, del d.lg. n. 196/2003, sulla scia di due noti casi che avevano interessato in passato i comuni di Roma e Milano, ha ora chiarito, da un lato, che rientrano tra tali scopi di pubblica utilità quelli di applicazione della disciplina in materia di comunicazione istituzionale e, dall'altro, che tra i soggetti pubblici che possono avvalersi di tale opportunità è compreso lo stesso comune presso il quale è istituita l'anagrafe. Ciò comporta, quindi, l'utilizzabilità, da parte del comune, dei dati personali contenuti nei registri anagrafici per le finalità di comunicazione istituzionale ora indicate.

Il Garante è stato di seguito richiesto di verificare l'applicabilità di questo principio con una decisione su un ricorso relativo ad una vicenda in cui un comune aveva inviato a cittadini minorenni un invito a prendere parte alla sagra patronale ed alla festa di *Halloween* organizzate dall'ente. Il Garante non ha riscontrato specifiche violazioni ed ha pronunciato non luogo a provvedere sul ricorso. I dati trattati, ottenuti tramite il locale ufficio anagrafe, non erano conservati presso il comune, la gestione delle comunicazioni effettuate era stata organizzata direttamente dal comune stesso e le finalità e la logica del trattamento consistevano unicamente nell'intenzione di fare conoscere ai bambini il contenuto delle iniziative ricreative organizzate dall'amministrazione (*Provv.* 30 gennaio 2004).

Nel corso dell'anno, il Garante è stato altresì sollecitato in più occasioni a pronunciarsi in materia elettorale.

Liste elettorali ed elenco degli italiani residenti all'estero

Si è in primo luogo nuovamente ribadito a chi ne ha fatto richiesta (*Nota* 7 marzo 2003) che la normativa sulla protezione dei dati personali non aveva a suo tempo modificato la disciplina in materia di ostensibilità delle liste elettorali detenute dai comuni, la quale consentiva a chiunque di copiare, stampare o mettere in vendita le liste elettorali del comune (art. 51 d.P.R. 20 marzo 1967, n. 223).

L'Autorità si è poi pronunciata sulla conoscibilità dell'elenco provvisorio degli aventi diritto al voto detenuto dalle rappresentanze diplomatico-consolari, previsto dal regolamento di attuazione della legge sull'esercizio del diritto di voto dei cittadini italiani residenti all'estero (d.P.R. n. 104/2003, attuativo della legge n. 459/2001).

In alcune note indirizzate al Ministero degli affari esteri, il Garante ha ritenuto applicabili il regime di pubblicità e le modalità ostensive delle liste elettorali detenute dai comuni, anche alla luce della ricordata legge n. 459/2001, che considera equivalenti le funzioni svolte dalle liste elettorali e dall'elenco provvisorio distribuito dagli uffici consolari. Per l'utilizzo dell'elenco dei residenti all'estero l'art. 5 del d.P.R. n. 104/2003 prevede poi una specifica limitazione, vietando la comunicazione e la diffusione dei dati degli elettori per finalità diverse da quelle politico-elettorali stabilite dalla citata legge n. 459 (*Nota* 13 giugno 2003).

Le novità introdotte dal Codice

Rispetto al regime di piena conoscibilità e pubblicità delle liste elettorali degli enti locali, il Codice ha peraltro introdotto una modifica rilevante, prevedendo, in applicazione del principio di finalità (e tenendo conto di quanto prospettato dal Ministero dell'interno in occasione di un quesito sulla *ratio* di questa ipotesi di pub-

blicità), che le liste elettorali possano essere rilasciate in copia solo in favore di chi intende perseguire una finalità di attuazione della disciplina in materia di elettorato attivo o passivo, di studio, ricerca scientifica o storica o socio-assistenziale, oppure per perseguire un interesse collettivo o diffuso (art. 177 d.lg. n. 196/2003).

Tale modifica, benché posteriore alla normativa sul voto dei cittadini italiani residenti all'estero, non sembra incidere particolarmente sul regime di conoscibilità dell'elenco provvisorio detenuto dagli uffici consolari, in ragione dell'espresso divieto di utilizzare i dati in esso contenuti per finalità diverse da quelle politico-elettorali, come sopra rammentato (*Nota* 4 settembre 2003).

I Comites

Il d.P.R. 29 dicembre 2003, n. 395, recante il regolamento di attuazione della legge n. 286/2003 sull'istituzione dei comitati degli italiani all'estero (Comites), ha peraltro precisato che l'elenco aggiornato degli italiani residenti all'estero può essere utilizzato per finalità riguardanti la determinazione della consistenza delle comunità italiane, in relazione all'istituzione di tali comitati, nonché la predisposizione delle liste e lo svolgimento della campagna elettorale per l'elezione dai componenti dei comitati stessi. Sempre per le finalità politico-elettorali connesse all'elezione dei Comites, l'autorità consolare può consentire a chi ne faccia richiesta di copiare l'elenco degli aventi diritto al voto, ovvero può fornirne copia.

22 Istruzione

Nell'ultimo anno di attività l'Autorità è stata nuovamente sollecitata a chiarire alcuni aspetti relativi alla protezione dei dati nel settore dell'istruzione.

Pubblicità degli esiti scolastici

In questo quadro, è tra l'altro in fase di definizione il procedimento relativo ad un istituto scolastico il quale aveva acquisito dati personali di studenti dagli elenchi affissi all'albo di altri istituti, al termine dell'anno scolastico, ed aveva inviato loro comunicazioni di carattere commerciale. In passato, con riferimento a casi analoghi, il Garante aveva già rilevato che la pubblicità degli esiti scolastici risponde ad essenziali esigenze relative alla vita scolastica dei singoli, nonché al controllo pubblico e dei cointeressati sullo svolgimento delle predette attività. Tale conoscibilità delle valutazioni finali non autorizza, però, i terzi che vi accedano ad utilizzare i dati acquisiti per inviare materiale pubblicitario, dovendosi tener conto delle sole specifiche finalità cui è preordinata la pubblicità del dato.

L'Autorità si è inoltre pronunciata in merito alla liceità dell'affissione, da parte di un'università, dell'elenco nominativo di tutti i soggetti che partecipano agli esami di Stato per l'abilitazione all'esercizio di una professione. Nella specifica vicenda si è ritenuta lecita la pubblicazione dei soli nominativi di coloro che avevano superato le prove d'esame, dal momento che la disciplina di settore (d.m. 9 settembre 1957) prevede un espresso regime di pubblicità solo per questa categoria di soggetti (*Nota* 22 aprile 2003).

La frammentarietà di queste fattispecie ha indotto l'Autorità ad aprire l'istrutto-

ria in vista dell'adozione di un provvedimento di carattere generale volto a riassumere vari aspetti relativi alla diffusione, in singoli casi, degli esiti concorsuali o delle graduatorie da parte di soggetti pubblici, in particolare se effettuata tramite Internet. Proprio in riferimento a quest'ultimo mezzo di diffusione, occorrono infatti soluzioni nuove e specifiche per contemperare l'esigenza di pubblicità di elenchi, liste e graduatorie con il diritto degli interessati a non subire un'ingiustificata divulgazione dei propri dati personali, in particolare quando vi sono dati di carattere sensibile.

È stata pure avviata, come già detto nel parag. 2, lett. *g)*, una collaborazione con il Ministero dell'università, dell'istruzione e della ricerca sul progetto relativo all'istituzione di un'anagrafe degli studenti universitari, con particolare riferimento alle modalità di trattamento di dati di carattere sensibile.

Sono in corso anche alcuni approfondimenti sull'attività di monitoraggio della presenza di allievi stranieri nel territorio provinciale, promossa da un istituto scolastico. Tale attività, che prevede la raccolta di dati sugli alunni tramite questionari distribuiti agli istituti d'istruzione, può comportare il trattamento di dati sensibili degli alunni stessi (in particolare, di informazioni relative all'origine razziale o etnica), nonché di altre delicate informazioni di carattere personale, come quelle concernenti adozioni o affidamenti.

23 Enti locali

Al fine di accelerare l'adeguamento da parte dei soggetti pubblici alle disposizioni in materia di trattamento di dati sensibili e giudiziari, proseguono le attività di collaborazione avviate dall'Autorità con organismi rappresentativi delle autonomie locali (Anci, Upi e Uncem).

Ciò anche alla luce delle modifiche introdotte dal Codice, che, come si è già sottolineato, impegna regioni ed enti locali, al pari di altre amministrazioni pubbliche, ad identificare e rendere pubblici non oltre il 30 settembre 2004 (pena l'illiceità del trattamento) i tipi di dati utilizzati e le operazioni effettuate, mediante un atto di natura regolamentare adottato in conformità al parere espresso dal Garante anche attraverso schemi tipo.

Il regolamento sui trattamenti di dati sensibili e giudiziari

Nell'ambito della collaborazione instauratasi, è stata già redatta una prima bozza di regolamento per comuni e comunità montane, da utilizzare per indicare poi la denominazione dei trattamenti effettuati, la fonte normativa, le rilevanti finalità di interesse pubblico perseguite, i tipi di dati trattati e di operazioni eseguibili, nonché anche la sintetica, ma esauriente, descrizione dei trattamenti e dei flussi informativi.

È ormai imminente la pubblicazione del modello predisposto sul sito *web* dell'Anci e dell'Ancitel, al fine di poter raccogliere eventuali suggerimenti, integrazioni ed osservazioni prima che il Garante esprima il parere in proposito e lo ponga formalmente a disposizione dei comuni.

Sono inoltre in corso analoghe forme di collaborazione con l'Upi e con le regioni, per la stesura di analoghi schemi di regolamento utili per amministrazioni provinciali e regionali.

Per quanto riguarda, poi, la collaborazione con le regioni, si è anche tenuto conto dell'esigenza di coinvolgere il Ministero della salute, gli assessorati alla sanità (qualora non già presenti) e le aziende sanitarie locali, considerata la necessità di includere, nello schema di regolamento, anche i trattamenti di dati relativi alla salute. Ciò alla luce della nuova disciplina dettata in argomento dal Codice, che non prevede più una specifica competenza del Ministero della salute a regolamentare tali trattamenti (a differenza dell'art. 23, comma 1-*bis* della legge n. 675/1996) e demanda tale incombenza all'iniziativa delle diverse amministrazioni.

In proposito è opportuno aggiungere che il Garante è intervenuto sulla questione dell'individuazione del titolare dei trattamenti effettuati dalle amministrazioni regionali: con la decisione del 30 dicembre 2003 si è infatti chiarito che il titolare deve essere identificato nell'ente regione complessivamente considerato e non anche in suoi specifici uffici od organi, presso i quali possono operare, se designati, responsabili del trattamento.

Il sistema integrato Ina-Saia

Anche nel 2003 l'Autorità si è occupata dei flussi di dati anagrafici previsti dal sistema integrato Ina-Saia (Indice nazionale delle anagrafi-Sistema di accesso e interscambio anagrafico).

Il Garante, nel parere reso al Ministero dell'interno sullo schema di regolamento relativo alla gestione dell'Ina, ha sottolineato la necessità di individuare la fonte normativa legittimata a disciplinare l'utilizzo dei servizi Ina, non essendo adeguato il riferimento alle competenze attribuite dalla legge agli enti interessati. Apposite convenzioni dovrebbero inoltre individuare le specifiche finalità per le quali possono essere utilizzati i dati resi accessibili mediante il sistema. La possibilità di accedere ai servizi per i soggetti diversi dagli enti pubblici dovrebbe poi essere stabilita da una norma di legge o di regolamento e non da mere determinazioni amministrative (*Nota* 13 febbraio 2004).

Flussi documentali tra p.a.

Con riguardo alla gestione dei flussi documentali tra amministrazioni pubbliche, l'Autorità ha ricevuto un quesito dal Ministero dell'interno. La questione concerneva la possibilità di attivare un canale informativo tra l'Ufficio territoriale del Governo di Palermo e la Regione Sicilia, per verificare periodicamente le autocertificazioni presentate dai soggetti che ricoprono incarichi pubblici su nomina regionale, in particolare circa l'inesistenza delle condizioni di cui alla legge n. 55/1990 sulla prevenzione della delinquenza di tipo mafioso (art. 4, comma 1, lett. *h)*, l.r. n. 19/1997). Al riguardo, si è osservato che tale comunicazione dovrebbe essere prevista quantomeno da una norma di rango regolamentare, ancorché sia volta al perseguimento di finalità lecite, per le quali è consentito il trattamento di dati di carattere sensibile (autorizzazione del Garante n. 7/2002; cfr. pure l'art. 11 del d.lg. n. 135/1999).

È stato poi condiviso l'orientamento del Ministero in merito alla necessità che i controlli sulle autocertificazioni siano effettuati dall'amministrazione interessata tramite la consultazione del sistema informativo del casellario giudiziale, ovvero, per quelle informazioni non contenute nei relativi certificati, tramite la competente autorità giudiziaria (*Nota* 8 settembre 2003).

Tra le questioni allo studio dell'Autorità concernenti l'attività degli enti locali, è in corso di definizione quella relativa alle modalità della raccolta differenziata dei rifiuti solidi urbani, per i profili di eventuali violazioni della riservatezza degli interessati che ne possono discendere.

24 Notificazione di atti e comunicazioni

Conformemente alle indicazioni già fornite in passato (cfr. *Provv.* 22 ottobre 1998 e 26 ottobre 1999), il Garante ha ribadito l'esigenza di tutelare la riservatezza delle persone cui sono notificati atti e documenti attraverso l'adozione di prassi più rispettose della loro dignità, in attesa della modifica delle relative norme processuali.

Le novità apportate dall'art. 174 del Codice

La disciplina delle notificazioni degli atti giudiziari e degli altri atti è mutata con l'entrata in vigore del Codice, che ha accolto molte delle indicazioni a suo tempo già fornite dall'Autorità, intervenendo sulle relative disposizioni processuali (art. 174 d.lg. n. 196/2003).

Il principio alla base delle modifiche apportate dal Codice è quello secondo il quale, qualora la notificazione non possa essere eseguita nelle mani del destinatario, la copia dell'atto deve essere consegnata in busta sigillata e su questa non devono essere apposte indicazioni da cui possa desumersi il contenuto dell'atto stesso. Tale principio si applica nell'ambito del processo sia civile, sia penale, nonché per le notificazioni di sanzioni amministrative e di atti e documenti provenienti da organi delle pubbliche amministrazioni, se effettuate a soggetti diversi dagli interessati.

È stata poi modificata anche la disciplina sulla pubblicazione degli avvisi concernenti le vendite giudiziarie. Il Codice ha, infatti, stabilito che negli avvisi relativi all'esecuzione immobiliare deve essere omessa l'indicazione del debitore e che nella vendita senza incanto i dati relativi al debitore possono essere forniti dalla cancelleria del tribunale a chiunque vi abbia interesse.

Visibilità di dati personali sulle buste

Nel merito delle questioni affrontate dall'Autorità nel settore in esame, va ricordato il caso di un istituto previdenziale che aveva inviato tramite posta una comunicazione ad un proprio assistito, utilizzando una busta con finestra trasparente. Ciò consentiva di leggere non solo i dati personali indispensabili all'invio della comunicazione alla persona cui era diretta, ma anche altre informazioni, quali la sua data di nascita e notizie sui rapporti di parentela.

A seguito dell'intervento dell'Autorità, l'istituto previdenziale ha quindi provveduto ad indicare le misure da adottare al riguardo, a cominciare dalla necessità di una modifica dell'applicazione informatica di acquisizione dei dati al fine di rilevare più chiaramente la differenza tra informazioni anagrafiche ed altri tipi di dati. L'istituto ha anche richiamato le sedi periferiche all'osservanza di talune istruzioni volte a tutelare la riservatezza degli interessati, come l'indicazione sulle buste del solo cognome, nome e indirizzo degli aventi diritto alle prestazioni e la menzione del codice fiscale soltanto in casi particolari.

Per quanto concerne, invece, la notifica da parte del comune, attraverso il messo comunale, di un invito a regolarizzare una violazione finanziaria, è stato ricordato che la possibilità per il messo (come pure per gli addetti al protocollo) di accedere al contenuto del documento non integra una violazione delle regole sulla comunicazione dei dati personali, trattandosi di soggetti incaricati del trattamento e per di più tenuti al segreto di ufficio in virtù del loro *status* di dipendenti pubblici (*Nota* 5 agosto 2003).

25 Pubblici registri, elenchi, atti e documenti conoscibili da chiunque

La materia del trattamento dei dati raccolti da pubblici registri, elenchi, atti e documenti conoscibili da chiunque continua a dar luogo a situazioni di insufficiente rispetto della *privacy*, come dimostrano i numerosi ricorsi e segnalazioni tuttora portati all'esame del Garante. Il problema è reso più complicato dalla presenza di normative di settore che solo in minima parte tengono conto dei diritti degli interessati alla protezione dei dati personali. Emblematiche in proposito sono le questioni relative all'accesso ai dati riguardanti procedure concorsuali, dove il rischio è l'azzeramento di fatto dell'efficacia del provvedimento di riabilitazione dal fallimento.

Ancor più significativo è poi il perdurare, pur dopo la legge n. 235/2000, di problemi nel settore dei protesti, dovuti in particolare al differente regime di cancellazione dei protesti cambiari rispetto a quelli levati per il mancato tempestivo pagamento di assegni bancari (sul punto, cfr. Corte cost., 14 marzo 2003, n. 70).

Delle problematiche derivanti dal trattamento dei dati raccolti da pubblici registri, elenchi, atti e documenti conoscibili da chiunque si è già parlato nel paragrafo 8.2., dedicato alle tutele esperibili nei confronti del trattamento dei dati personali concernenti il comportamento debitorio. Si è visto, in quella sede, che su tali aspetti sono stati proposti numerosi ricorsi, volti in particolare ad ottenere la cancellazione dei dati stessi.

Trattamento di dati provenienti da pubblici registri da parte di soggetti privati

Questioni analoghe sono state sottoposte all'attenzione del Garante anche al di fuori dei casi di proposizione di ricorso. Ha così formato oggetto di segnalazione all'Autorità il rifiuto della richiesta di cancellazione di dati personali concernenti la trascrizione di un pignoramento immobiliare da una banca dati gestita da una società e contenente informazioni tratte da pubblici registri. La società, nel rifiutare la cancellazione, ha osservato che i dati corrispondevano a quelli riportati dai pubblici registri (nel caso di specie, la conservatoria dei registri immobiliari) e potevano essere quindi modificati soltanto dopo l'annotazione in tali registri delle relative variazioni.

Nell'attuale assetto normativo, l'attività di consultazione, ad opera di privati, dei dati provenienti dalle conservatorie avviene anche attraverso apposito collegamento telematico; l'abilitazione a tale servizio è rilasciata con convenzione, in base al d.m. 10 ottobre 1992 ed alla circolare del Dipartimento del territorio n. 144T del 17 luglio 2000. Per quanto riguarda invece l'aggiornamento della banca dati catastale

ed ipotecaria, il decreto direttoriale del 28 febbraio 2002 stabilisce i termini di un giorno (per l'esecuzione delle formalità di iscrizione nonché di trascrizione di atti) e di novanta giorni (per le annotazioni a margine delle stesse formalità).

Prendendo spunto dalle questioni sottoposte alla sua attenzione, il Garante ha avviato pertanto un approfondimento sulla liceità e correttezza del trattamento di dati provenienti da pubblici registri effettuato in specie da parte di privati, in modo da fornire indicazioni sulla corretta applicazione della normativa in materia di protezione dei dati personali. Ciò specialmente in relazione alla prevista elaborazione sia del codice di deontologia in tema di dati provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici (deliberazione del Garante n. 2 del 10 aprile 2002, e art. 61 del Codice), sia di quello in tema di trattamento di dati effettuato a fini di informazione commerciale (cfr. art. 119 del Codice).

In particolare, è stato rilevato che si deve valutare la conformità del termine di novanta giorni previsto per l'annotazione a margine delle formalità al principio della conservazione dei dati per il tempo necessario al perseguimento delle finalità per le quali gli stessi sono raccolti e successivamente trattati, anche con riguardo al più breve termine previsto per l'esecuzione delle formalità di iscrizione e trascrizione di atti.

Per quanto concerne, poi, la banca dati gestita dalla società, è emersa la questione della necessità di assicurare che i privati che gestiscono banche dati di questa categoria aggiornino i dati stessi e forniscano tempestivo riscontro alle richieste di rettificazione o cancellazione avanzate dagli interessati, anche quando negli elenchi pubblici da cui i dati sono tratti non si sia ancora provveduto al relativo aggiornamento.

In relazione a tale profilo, la società ha ipotizzato una soluzione provvisoria in base alla quale il gestore della banca dati cancellerebbe i dati personali relativi ad atti ancora riportati nei registri immobiliari, qualora gli interessati esibiscano copia autentica del titolo su cui si fonda la richiesta di cancellazione dell'atto e la ricevuta della conservatoria, attestante il deposito della domanda di annotazione della cancellazione presso la conservatoria medesima.

La direttiva comunitaria sul riutilizzo dei documenti del settore pubblico

Per quanto concerne gli aspetti di novità della disciplina comunitaria, si segnala anche l'adozione della direttiva n. 2003/98/CE sul riutilizzo dei documenti del settore pubblico, ai cui lavori preparatori ha partecipato attivamente, nell'ambito della delegazione italiana, l'Ufficio del Garante.

L'obiettivo della direttiva è quello di agevolare il riutilizzo delle informazioni del settore pubblico al fine di favorire la creazione di prodotti e servizi a contenuto informativo su scala comunitaria, anche nella prospettiva della diffusione di nuove piattaforme di comunicazione. L'esistenza di norme e prassi diverse negli Stati membri in materia di tariffe, tempi di risposta, accordi di esclusiva e disponibilità generale dei dati ai fini del riutilizzo, rendeva infatti necessaria un'armonizzazione al livello comunitario. Allo scopo di favorire lo sviluppo di prodotti e servizi informativi a valore aggiunto da parte delle imprese, nonché di limitare le distorsioni della concorrenza sul mercato europeo, la direttiva definisce un quadro di garanzie in materia di condizioni di mercato, tariffazione, tempi e modalità di risposta.

I principi dettati non incidono comunque sui regimi nazionali esistenti in materia di accesso ai documenti e sulle garanzie poste a tutela dei dati personali, che sono fatte espressamente salve dalla direttiva.

26 Attività fiscale e tributaria

Nel settore in esame l'Autorità è intervenuta per valutare alcuni aspetti relativi ad attività realizzate dal Ministero dell'economia e delle finanze e da altri soggetti operanti in ambito fiscale (agenzie fiscali e concessionari della riscossione).

In primo luogo il Garante ha approfondito talune problematiche in tema di protezione dei dati personali connesse all'adozione, da parte dell'Agenzia delle entrate, di un *call-center* e di un servizio via *web* volti a snellire il rapporto con i contribuenti, con particolare riguardo alla fase di identificazione di questi ultimi ed a quella di accesso alle informazioni contenute nell'anagrafe tributaria tramite l'uso di un *pin* e di una *password*.

Si è poi verificata la sussistenza dei presupposti di liceità per la comunicazione del codice fiscale, da parte dell'Agenzia delle entrate, ad amministrazioni pubbliche e gestori di pubblici servizi che ne abbiano fatto richiesta, nonché per la comunicazione degli elenchi dei contribuenti da parte dell'amministrazione finanziaria ai comuni e per la pubblicazione delle controversie dei contribuenti stessi da parte delle commissioni tributarie.

Richieste di dichiarazione stragiudiziale sui crediti del contribuente moroso

L'Autorità, a seguito di numerosi quesiti, segnalazioni e ricorsi, ha esaminato anche la prassi delle società concessionarie del servizio per la riscossione dei tributi di chiedere, senza il consenso del contribuente moroso, informazioni personali a terzi per ottenerne una dichiarazione stragiudiziale che attesti la presenza di crediti su cui rivalersi (cfr. *supra*, parag. 9.1.).

Tale attività, che comporta la comunicazione a terzi di informazioni concernenti la situazione debitoria del soggetto ritenuto moroso, è stata giudicata illecita in quanto nessuna previsione legislativa o regolamentare attribuisce alla società concessionaria il potere di effettuare questo tipo di trattamento senza il consenso del contribuente interessato: la procedura è risultata disciplinata, infatti, solo da risoluzioni dell'Agenzia delle entrate e da mere circolari ministeriali.

La procedura è stata inoltre ritenuta in contrasto con il principio di non eccedenza (art. 11 d.lg. n. 196/2003), in quanto sproporzionata rispetto alla finalità di recupero del credito che può essere comunque perseguita con altri strumenti.

In alcuni casi esaminati a seguito di ricorso il Garante ha quindi disposto il blocco del trattamento illecito dei dati di un contribuente da parte delle società concessionarie, che hanno dovuto sospendere l'utilizzo delle informazioni detenute, limitandosi solo a conservarle (*Newsletter* 22 febbraio 2004).

L'Agenzia ha poi emanato un'apposita risoluzione, volta a sollecitare i concessionari della riscossione ad astenersi da questa prassi (Risoluzione 35/E del 12 marzo 2004); a sua volta, l'Inps, con nota del 30 marzo 2004, prendendo atto di quanto stabilito dal Garante, ha deciso di sospendere l'attività di rilascio delle dichiarazioni stragiudiziali ai concessionari, in attesa di ulteriori delucidazioni.

Tra le attività svolte dall'Autorità va sottolineata la collaborazione con l'Ufficio centrale antifrode dei mezzi di pagamento (Ucamp) del Ministero dell'economia e delle finanze, in merito alla realizzazione ed alla gestione di una banca dati informatica relativa alle frodi effettuate attraverso mezzi di pagamento.

L'Autorità ha infine fornito indicazioni all'Ufficio federalismo fiscale del Ministero dell'economia e delle finanze, allo scopo di contribuire alla stesura di uno schema di decreto sullo scambio di informazioni tra l'amministrazione finanziaria e le regioni concernenti l'imposta regionale sulle attività produttive (Irap), rispettoso dei principi di liceità e correttezza del trattamento dei dati personali.

27 Attività giudiziaria ed informatica giuridica

Per quanto riguarda le informazioni contenute nei provvedimenti dell'autorità giudiziaria che dispongono il giudizio penale, il Garante ha ribadito che, fermo restando il rispetto dei principi di pertinenza e di non eccedenza, la normativa in materia di protezione dei dati non pregiudica l'esercizio dell'attività giudiziaria, in particolar modo quando il codice di rito preveda specificamente l'inserimento in tali provvedimenti di precise informazioni per determinate finalità processuali. Specifici suggerimenti sono stati peraltro formulati a proposito dell'eventuale notificazione degli atti per pubblici proclami.

Altra problematica, portata all'attenzione dell'Autorità da alcune segnalazioni, è quella della pubblicazione sui siti Internet dell'autorità giudiziaria di decisioni contenenti informazioni delicate relative alle parti in giudizio.

Pubblicazione *on line* di provvedimenti giurisdizionali

La questione è stata ora risolta dal Codice, il quale agevola sia l'accessibilità *on line* dei dati identificativi delle questioni pendenti presso le autorità giudiziarie di ogni ordine e grado (quindi anche i giudici amministrativi e contabili) da parte di chi vi ha legittimo interesse, sia l'accessibilità al pubblico delle sentenze e delle altre decisioni delle medesime autorità una volta depositate in cancelleria o in segreteria.

Le sentenze devono essere redatte secondo le ordinarie regole che individuano nominativamente tutte le parti interessate. Tuttavia, in caso di riproduzione in qualunque forma di sentenze o altri provvedimenti giurisdizionali effettuata nel quadro delle legittime e doverose attività di informazione a fini giuridici, prima che sia definito il giudizio si può chiedere per motivi legittimi all'autorità giudiziaria (che può disporla anche d'ufficio) l'apposizione sul provvedimento di un'annotazione volta a precludere l'indicazione, nella versione pubblicata, delle generalità e di altri dati identificativi degli interessati.

Una tutela rafforzata è poi garantita dagli artt. 51 e 52 del d.lg. n. 196/2003 per i minori e per i soggetti coinvolti in procedimenti in materia di rapporti di famiglia e di stato delle persone, indipendentemente dall'annotazione apposta sul provvedimento.

Formano oggetto di particolare approfondimento anche alcune iniziative istituzionali intraprese da tribunali e camere di commercio, che si propongono di rendere disponibili sui propri siti istituzionali banche dati contenenti informazioni e documenti relativi a procedure concorsuali.

Per quanto riguarda poi lo sviluppo di metodi alternativi di risoluzione delle controversie, è stato sottoposto all'attenzione dell'Autorità un protocollo di intesa tra una camera di commercio, un tribunale ed un consiglio dell'ordine degli avvocati, che prevede l'avvio di una fase sperimentale di conciliazione delegata fondata sull'individuazione, da parte delle istituzioni coinvolte, di un numero di controversie idonee ad un efficace esperimento del tentativo di composizione stragiudiziale.

Consultazione del casellario giudiziale da parte delle p.a.

In merito alle problematiche connesse all'adozione del decreto dirigenziale del Ministero della giustizia regolante la consultazione del casellario giudiziale da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi, si rimanda alla specifica trattazione che ne verrà fornita nel paragrafo sull'attività consultiva del Garante rispetto agli atti del Governo (cfr. diffusamente, parag. 45.2.)

28 Attività di polizia e Guardia di finanza

Nel settore in esame, l'Autorità si è occupata tra l'altro di verificare talune modalità con le quali la Guardia di finanza accerta le posizioni reddituali e patrimoniali dei nuclei familiari dei soggetti beneficiari di prestazioni sociali agevolate. In particolare, il Garante è intervenuto in una vicenda in cui una struttura periferica del Corpo aveva richiesto ad un comune alcuni elenchi nominativi di beneficiari corredati di tutta la relativa documentazione, a partire dalla tipologia della prestazione sociale e dall'importo del contributo erogato.

A seguito dell'intervento dell'Autorità, il Comando generale ha impartito specifiche direttive alla struttura periferica chiarendo che, in una prima fase del controllo, devono essere acquisiti solo i nominativi dei beneficiari. Ulteriori elementi possono essere eventualmente acquisiti solo in una fase successiva, qualora emerga la reale necessità di svolgere approfondimenti sulla situazione economica dei soggetti sottoposti a controllo.

È in procinto di essere completata la verifica su un protocollo di intesa sottoscritto tra una regione e la Guardia di finanza ai fini del coordinamento dei controlli e dello scambio di informazioni in materia di spesa sanitaria, che presenta profili critici sul piano della proporzionalità e liceità delle modalità di trattamento previste.

Sono stati pure avviati specifici accertamenti sull'attivazione di un sistema infor-

matico realizzato da un comune al fine di garantire alle forze di polizia un accesso preferenziale alle banche dati dell'ente. In particolare, il comune ha consegnato alla Guardia di finanza, all'Arma dei carabinieri ed alla Polizia di Stato una *smart card* con i connessi codici di sicurezza, che consente l'accesso ad una serie di dati personali dei cittadini di carattere anagrafico, patrimoniale, fiscale e giudiziario.

Acquisizione di dati per via telematica da parte delle autorità di p.s.

In argomento va anche ricordato che, dopo le modifiche introdotte dal Codice, l'acquisizione presso terzi di informazioni e documenti da parte delle autorità di pubblica sicurezza e delle forze di polizia, in conformità alla legge ed ai regolamenti, può essere realizzata anche per via telematica attraverso convenzioni, a condizione che le modalità di collegamento previste assicurino un accesso selettivo ai soli dati necessari al perseguimento delle finalità di sicurezza ed ordine pubblico, nonché di prevenzione, accertamento e repressione dei reati (artt. 3, 11 e 54 d.lg. n. 196/2003), anche sulla base di convenzioni-tipo adottate dal Ministero dell'interno su conforme parere del Garante.

29 Rapporto di lavoro

L'Autorità si è pronunciata più volte sul tema della protezione dei dati personali nel settore del lavoro e della previdenza sociale, oggetto ora della specifica disciplina dettata dal Titolo VIII del Codice.

Comunicazione o diffusione di dati sulla salute dei dipendenti

Nel settore del pubblico impiego sono stati anzitutto esaminati alcuni casi in cui, nelle comunicazioni concernenti l'adozione di provvedimenti di gestione interna del personale (trasferimenti o avvicendamenti) sono riportati dati di carattere sensibile riguardanti, in particolare, la salute di dipendenti. Il trattamento di queste informazioni per perseguire una rilevante finalità d'interesse pubblico di gestione di rapporti di lavoro può in generale ritenersi lecito. Occorre, tuttavia, che sia rispettato anche il principio di necessità, in virtù del quale possono essere oggetto di trattamento soltanto i dati indispensabili al raggiungimento di tale finalità. Non è stata ad esempio ritenuta rispondente al principio di necessità l'indicazione, in questo tipo di comunicazione, del luogo del ricovero di un dipendente e della gravità dei motivi di salute su cui era fondata la sua sostituzione, tenuto oltretutto conto dell'invio della comunicazione anche alle rappresentanze sindacali (*Nota* 4 settembre 2003).

Trattamento di dati del personale delle forze armate e di polizia

È in procinto di essere ultimata l'attività del tavolo di lavoro sul trattamento dei dati del personale delle forze armate e di polizia promosso dall'Autorità in collaborazione con le amministrazioni interessate. L'iniziativa mira ad approfondire congiuntamente alcune questioni riguardanti, in particolare, la gestione dei fascicoli personali dei dipendenti, per consentire l'elaborazione di indicazioni e soluzioni a tutela della riservatezza e degli altri diritti degli interessati.

Nell'ambito di tale tavolo di lavoro sono state esaminate varie questioni, tra cui:

- la richiesta di documentare la diagnosi, oltre alla prognosi, indirizzata ai dipendenti che si assentano dal servizio per motivi di salute, e la successiva

conservazione della relativa documentazione nel fascicolo personale;

- il trattamento dei dati sulla salute connesso agli accertamenti dell'idoneità psico-fisica al servizio svolti nei confronti del personale, sia al momento dell'assunzione, sia in costanza del rapporto di lavoro;

- il trattamento dei dati sensibili contenuti in documenti quali il fascicolo personale, il foglio matricolare ed altri atti, con particolare riferimento al principio di necessità dei dati stessi e al periodo della loro conservazione.

L'iniziativa ha consentito anche di sollecitare la cessazione di talune prassi adottate da strutture periferiche delle amministrazioni, già portate all'attenzione dell'Autorità.

Si è posto così rimedio anche al caso verificatosi in un istituto penitenziario, dove era stata affissa in bacheca una lista del personale assente per malattia comprensiva di nominativi, periodi di prognosi e diagnosi. Nel novembre del 2003 l'amministrazione penitenziaria ha emanato una circolare con la quale ha richiamato gli uffici periferici al rispetto delle rigorose cautele apprestate dalla normativa sulla protezione dei dati a tutela delle informazioni di carattere sensibile, con particolare riguardo al divieto di diffondere le notizie sulla salute.

Sempre in materia di trattamento di dati del personale delle forze armate e di polizia, un dipendente di una questura ha presentato un ricorso lamentando che le informazioni relative alle sue condizioni di salute, accertate nel corso di una visita medica cui era stato sottoposto per verificare la sua idoneità al servizio, erano state comunicate ad altri soggetti al fine del ritiro cautelativo dell'arma in dotazione e del tesserino di servizio.

In proposito, l'Autorità ha però constatato che tali comunicazioni erano avvenute lecitamente, in quanto effettuate in conformità alle disposizioni sulle autorizzazioni di polizia per la detenzione ed il porto d'armi e finalizzate all'adozione dei relativi provvedimenti (*Provv.* 15 gennaio 2004).

Questionari di valutazione

In un altro ricorso, il Garante si è invece pronunciato sulla liceità della gestione di questionari di valutazione dell'attività svolta da dipendenti dell'amministrazione.

In particolare, sono stati reputati conformi alla normativa sulla protezione dei dati la raccolta e l'esame di schede anonime di valutazione, quando il trattamento coinvolga soltanto uffici interni all'amministrazione interessata. Si devono peraltro adottare tutte le necessarie misure di sicurezza, anche diverse da quelle minime, al fine di assicurare che i dati contenuti nei questionari siano trattati dal personale specificatamente individuato, per le sole finalità conformi a quelle che rendono lecito il trattamento e con modalità operative rispettose dei principi di pertinenza e di non eccedenza (*Provv.* 22 settembre 2003).

In relazione alla gestione della documentazione matricolare del personale militare, l'Autorità ha inoltre esaminato il ricorso di un dipendente che lamentava l'illiceità della conservazione nel suo stato matricolare di informazioni che lo riguardavano, concernenti l'applicazione di una pena concordata, in quanto erano trascorsi cinque anni dalla data di irrevocabilità della sentenza ed era avvenuta l'estinzione del reato (art. 445, comma 2, c.p.p.).

Il Garante ha giudicato infondato il ricorso poiché nel caso di specie non risultavano violate né la normativa di settore (r.d. n. 1236 del 1941), né le disposizioni sulla correttezza e l'aggiornamento dei dati personali; ha poi constatato la liceità del trattamento di informazioni di carattere giudiziario da parte dell'amministrazione per finalità di gestione del rapporto di lavoro (*Provv.* 17 aprile 2003).

Per quanto riguarda la normativa sul diritto al lavoro dei disabili, è pervenuta una segnalazione con la quale si lamentava che la graduatoria del collocamento obbligatorio, contenente i nominativi di circa tredicimila disabili, era stata pubblicata sul sito *web* del servizio per le politiche del lavoro di una provincia. L'accertamento preliminare ha rilevato che l'elenco era effettivamente accessibile da chiunque attraverso la pagina di apertura di tale sito.

La questione risultava rilevante, visto l'ingente numero di soggetti interessati dalla diffusione indiscriminata di dati idonei a rivelare il loro stato di salute. Il Garante ha pertanto curato ulteriori approfondimenti ai fini del blocco del trattamento, considerando che le disposizioni di settore (art. 8 legge n. 68/1999) non definiscono le modalità per garantire la pubblicità degli elenchi e delle graduatorie degli aventi diritto al collocamento obbligatorio.

Anche a tale proposito occorre comunque sottolineare che il divieto di diffusione dei dati idonei a rivelare lo stato di salute è espressamente ribadito dal Codice in relazione allo svolgimento delle attività di concessione di benefici ed agevolazioni previste dalla legge, dai regolamenti o dalla normativa comunitaria (art. 68, comma 3, d.lg. n. 196/2003).

Comunicazione all'Inail di dati sulla salute dei pazienti

L'Autorità ha altresì verificato la liceità delle segnalazioni trasmesse da medici all'Inail circa le malattie riscontrate nei pazienti, collegabili allo svolgimento di attività lavorative.

Sul punto si è precisato che, secondo il quadro normativo vigente (d.P.R. n. 1124/1965; d.m. 18 aprile 1973 e d.lg. n. 38/2000), il medico può trasmettere all'istituto assicuratore e ad altri organismi preposti le segnalazioni di malattie professionali che potrebbero essere state causate da un'attività lavorativa potenzialmente nociva, indicandone l'anamnesi lavorativa, i rischi e le sostanze cui il lavoratore sia (o sia stato) esposto.

Questa comunicazione deve essere però effettuata nel rispetto delle specifiche disposizioni in tema di assicurazioni contro gli infortuni sul lavoro e le malattie professionali, nonché del principio di pertinenza dei dati rispetto alle finalità per cui sono raccolti e successivamente trattati. (*Nota* alla procura della Repubblica di Torino del 27 ottobre 2003).

È infine nuovamente all'esame dell'Autorità la questione dell'indicazione di dati personali dei lavoratori nei buoni pasto (in particolare, i nominativi dei singoli beneficiari e la loro sede di servizio), accanto alle informazioni sul datore di lavoro, nonché dei presupposti di liceità per comunicare i dati dei dipendenti al soggetto tenuto all'erogazione del servizio.

30 Ricerca statistica

Codice deontologico

Il 1° ottobre 2002 è entrato in vigore il codice di deontologia e di buona condotta per i trattamenti dei dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (Sistan), ora allegato al Codice in materia di protezione dei dati personali.

Il codice deontologico regolamenta l'attività di ricerca statistica effettuata da enti ed uffici statistici che fanno parte, o partecipano, al Sistan per la realizzazione del programma statistico nazionale o per la produzione di informazione statistica in conformità ai rispettivi ambiti istituzionali.

Ai sensi dell'art. 106 del d.lg. n. 196/2003, il Garante deve promuovere la sottoscrizione di uno o più codici di deontologia e buona condotta per soggetti pubblici e privati, comprese le società scientifiche e le associazioni professionali, che trattano dati personali per scopi scientifici e statistici. Dopo l'adozione, a suo tempo, dell'atto di iniziativa, è stato ora portato a compimento il complesso *iter* che dovrebbe consentire di definire, entro un breve termine, un secondo codice deontologico di disciplina della ricerca statistica e scientifica effettuata da società scientifiche, nonché da istituti universitari, enti di ricerca e organismi non appartenenti al Sistan.

Con riferimento al Programma statistico nazionale per gli anni 2004-2006, e tenuto conto dei poteri di indirizzo e di coordinamento spettanti all'Istat nei confronti delle attività statistiche del Sistan, l'Autorità ha sollecitato il pieno rispetto del codice deontologico e della normativa di settore (d.lg. n. 322/1989), chiedendo all'Istituto di verificare l'effettivo adempimento alle relative prescrizioni prima dell'avvio dell'attività prevista dal Programma (*Nota* 1° settembre 2003).

Dati censuari

L'Autorità ha poi ultimato gli accertamenti istruttori già avviati in ordine allo svolgimento del quattordicesimo censimento generale della popolazione, per verificare la conformità delle operazioni censuarie alla normativa sulla protezione dei dati personali, anche in riferimento a trasferimenti di dati in Romania ed in Croazia.

Nel corso del censimento era altresì pervenuta la segnalazione della conservazione di dati censuari in un ufficio comunale anche successivamente al termine delle operazioni di raccolta. A seguito degli accertamenti effettuati dall'Autorità, è emerso che tali dati venivano trattati per svolgere operazioni di confronto con l'anagrafe e di revisione qualitativa dei questionari e sarebbero stati distrutti dopo la conclusione di queste operazioni. Il Garante ha, quindi, provveduto ad accertare l'avvenuta distruzione del materiale (Nota Istat 11 luglio 2003).

È ancora all'attento esame del Garante la questione del censimento linguistico nella Provincia di Bolzano, in merito alla quale già in passato è stata più volte evidenziata alle autorità di governo, a quelle comunitarie e ad organi locali la necessità di un intervento legislativo per conformare le disposizioni attuative dello Statuto provinciale alla normativa sulla protezione dei dati. Tale questione è oggetto, peraltro, di una denuncia di infrazione al diritto comunitario presentata alla Commissione europea. Sul punto l'Autorità tornerà entro breve ad evidenziare punti critici rimasti irrisolti e che anzi, per certi aspetti, sono stati resi più problematici.

31 Ordini e collegi professionali

Nel corso del 2003 sono pervenuti ancora quesiti sul trattamento dei dati personali relativi a soggetti iscritti ad albi e collegi professionali.

In questa materia l'Autorità ha ribadito quanto già affermato in passato e cioè che la legge n. 675/1996 non aveva modificato la disciplina previgente sul regime di pubblicità degli albi e sulla conoscibilità degli atti connessi allo *status* di iscritto.

Rispondendo nuovamente a quesiti e segnalazioni, il Garante ha poi sottolineato le significative innovazioni introdotte in argomento dal Codice, chiarendo anche la portata della nuova disciplina.

Le novità introdotte dal Codice (art. 61)

In primo luogo, è stato ricordato che, ai sensi dell'art. 61 del d.lg. n. 196/2003, in armonia con le disposizioni sulla comunicazione e diffusione di dati personali da parte dei soggetti pubblici, gli ordini e i collegi professionali possono ora più agevolmente comunicare anche a privati e diffondere pure per via telematica i dati (diversi da quelli sensibili e giudiziari) che, secondo le disposizioni legislative o regolamentari di settore, devono essere necessariamente inseriti nei rispettivi albi per legge o regolamento.

L'Ufficio ha poi precisato, in risposta alla segnalazione di un iscritto all'Ordine dei medici chirurghi e degli odontoiatri, che gli ordini ed i collegi professionali possono integrare i dati contenuti negli albi con ulteriori informazioni che l'iscritto richieda di aggiungere, purché pertinenti e non eccedenti in relazione alla sua attività professionale (art. 61, comma 3, cit.). Si é inoltre chiarito che, sempre a richiesta dell'interessato, possono essere fornite a terzi informazioni supplementari, ad es. quelle relative a speciali qualificazioni professionali non menzionate nell'albo o all'eventuale disponibilità a ricevere materiale informativo a carattere scientifico (art. 61, comma 4, d.lg. n. 196/2003).

In merito alle modalità di diffusione dei dati degli iscritti, si è peraltro rilevato che compete a ciascun ordine o collegio professionale valutare quali siano le più appropriate, sottolineando che il Codice autorizza comunque espressamente la pubblicazione dei dati divulgabili su siti Internet istituzionali o mediante altre reti di comunicazioni elettronica (art. 61, cit., comma 2).

Il Garante è anche tornato ad occuparsi della disciplina sulla divulgazione delle informazioni relative a provvedimenti disciplinari. Al riguardo è stato specificato che può essere divulgata pure l'esistenza di provvedimenti atti ad incidere sull'attività dell'iscritto all'albo (come ad es. la sospensione), fermo restando il dovere di porre in circolazione informazioni corrette, complete ed aggiornate, specie con riguardo ad eventuali sviluppi favorevoli per gli interessati (*Nota* 30 dicembre 2003).

Comunicazione di informazioni aggiuntive

Su richiesta dell'Ordine professionale degli assistenti sociali della Regione Sicilia, l'Autorità ha infine precisato che, al di là delle informazioni contenute negli albi professionali in base alla disciplina di settore o alle istanze formulate sul punto dagli stessi interessati nei termini appena precisati, non si possono comunicare a soggetti privati informazioni aggiuntive relative agli iscritti in mancanza di specifiche dispo-

sizioni normative che consentano tale comunicazione (quali ad es. quelle sull'accesso ai documenti amministrativi).

Al contrario, le informazioni aggiuntive possono essere comunicate ad altri soggetti pubblici anche in assenza di un'apposita disposizione che lo consenta, qualora ciò risulti necessario per lo svolgimento delle funzioni istituzionali e ne venga data previa notizia al Garante (art. 19, comma 2, d.lg. n.196/2003).

V - La privacy e le sfide del futuro
Reti di comunicazioni

32 Telefonia e reti di comunicazioni

32.1. Profili generali

Lo sviluppo di moderne tecnologie e di nuovi servizi di comunicazione elettronica ha reso necessario un ulteriore adeguamento della normativa sulla protezione dei dati personali in ambito italiano ed internazionale. Sul punto il Codice ha compiuto una ricognizione innovativa delle preesistenti norme sul trattamento dei dati nel settore delle telecomunicazioni (d.lg. n. 171/1998, come modificato dal d.lg. n. 467/2001), completando nello stesso tempo il recepimento della direttiva n. 2002/58/CE, relativa alla tutela della vita privata nel settore delle comunicazioni elettroniche.

La disciplina introdotta in materia dal Codice, riproponendo un criterio già presente nella normativa comunitaria, adotta un approccio "tecnologicamente neutro", ossia valido ed applicabile a tutte le forme di comunicazione elettronica a prescindere dal mezzo tecnico utilizzato.

32.2. Dati relativi al traffico telefonico

Si è già sintetizzata in altra parte della presente Relazione (cfr. parag. 1.11.) la recente vicenda che ha portato a modificare l'art. 132 del Codice e ad individuare garanzie rafforzate in riferimento al più lungo periodo di conservazione dei dati del traffico telefonico. In questa sede giova solo ricordare che il Garante, in conformità a quanto previsto dall'art. 132, comma 5, come modificato dalla legge n. 45/2004, definirà al più presto le misure e gli accorgimenti al cui rispetto è subordinato il trattamento dei dati relativi al traffico telefonico per le finalità di accertamento e repressione dei reati.

32.3. Fatturazione dettagliata ed altre questioni

Anche nel corso del 2003 l'Autorità si è occupata delle questioni connesse al mascheramento delle ultime tre cifre dei numeri telefonici nelle fatture inviate agli abbonati, che rappresenta una delle misure indicate dal Codice per tutelare la riservatezza degli abbonati chiamati, nonché degli utenti diversi dall'abbonato i quali effettuino chiamate dai terminali cui corrisponde l'abbonamento.

Nonostante i numerosi provvedimenti adottati in passato dal Garante, persistono alcuni nodi problematici testimoniati anche dai perduranti reclami e segnalazioni che pervengono all'Autorità.

Delle problematiche legate all'accesso alle informazioni incluse nella fatturazione,

ai limiti all'esercizio del diritto di accesso alle chiamate "in entrata" e alle cd. chiamate di disturbo, si è già parlato (cfr. *supra*, parag. 7.5.). In questa sede occorre, invece, sottolineare che durante il 2003 il Garante ha svolto approfondimenti in materia, destinati a confluire in un imminente provvedimento sulla fatturazione dettagliata, che riguarderà, fra l'altro, gli addebiti sulla linea telefonica dovuti a chiamate verso numeri a tariffazione speciale e a chiamate in entrata che comportano un costo per il ricevente.

Modalità di pagamento alternative alla fatturazione

In tale occasione saranno nuovamente esaminate le problematiche relative alla possibilità che le chiamate effettuate da qualsiasi terminale vengano pagate con modalità alternative alla fatturazione, e alla necessità di garantire in taluni casi la persona fisica del chiamante, ad esempio attraverso l'uso di carte prepagate (cfr. art. 5, comma 1, d.lg. n. 171/1998; ora, art. 124, comma 2, del Codice).

In proposito, secondo quanto confermato dal Codice, va ribadita l'importanza –per la tutela della sfera privata dei chiamanti, diversi dall'abbonato– dell'effettiva e diffusa disponibilità sul mercato di tali modalità alternative, il cui preventivo accertamento da parte del Garante, oltre che per eventuali provvedimenti sfavorevoli nei confronti dei titolari del trattamento inadempienti, costituirà presupposto indispensabile per autorizzare i fornitori ad indicare nella fatturazione i numeri completi relativi alle comunicazioni (art. 124, comma 5, del Codice).

In via preliminare, l'Autorità ha comunque già predisposto una prima nota di carattere generale volta a definire le modalità alternative alla fatturazione, anche anonime, che i fornitori di servizi di telefonia devono rendere disponibili da ogni terminale.

32.4. Banca dati unica dei numeri di telefonia fissa e mobile e nuovi elenchi telefonici

Con la deliberazione dell'Autorità per le garanzie nelle comunicazioni n. 36/02/Cons del 6 febbraio 2002 è stata prevista la costituzione della banca dati dove confluiranno alcuni dati personali di tutti gli abbonati e titolari di carte prepagate e in base alla quale potranno essere realizzati nuovi elenchi telefonici in formato cartaceo ed elettronico. In proposito va segnalato che è in fase avanzata l'analisi di quei profili che, nell'ambito della realizzazione di tale banca dati, riguardano più propriamente l'osservanza della normativa sulla protezione dei dati personali.

In particolare, i principali fornitori di servizi di telefonia fissa e mobile stanno predisponendo, in collaborazione con il Garante, versioni perfezionate dei modelli di informativa e consenso ispirate al rispetto della normativa sulla tutela dei dati personali, da sottoporre (tramite diverse modalità, a seconda che si tratti o meno di clienti con i quali già sussiste un rapporto) all'attenzione degli interessati, al fine dell'inserimento dei loro dati nella banca dati in discorso e, quindi, nei nuovi elenchi telefonici.

La problematica ha richiesto particolari approfondimenti, venendo in considerazione un "serbatoio" di informazioni dal quale innumerevoli soggetti potranno attingere per utilizzare dati relativi ai recapiti ed al numero di utenza degli interessati. La chiarezza, sinteticità e univocità dell'informativa è quindi essenziale per far comprendere a tutti gli abbonati le conseguenze che si determinano nel breve e medio periodo allorché si acconsenta all'utilizzo da parte di terzi dell'indirizzo o del numero di telefono anche mobile per inviare messaggi, missive, *fax*, *Sms* o *Mms*, altre chiamate vocali, ecc.

Con specifico riguardo agli elenchi, il Garante ha infatti segnalato come la relativa disciplina normativa sia stata recentemente oggetto di significative modifiche che ne hanno mutato in radice la natura e le finalità. Non a caso, quindi, il Codice ha attribuito a questa Autorità il compito di individuare, con proprio provvedimento, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati (ed ai titolari di carte prepagate) negli elenchi cartacei o elettronici disponibili al pubblico (art. 129).

Il Garante è pertanto in procinto di adottare tale provvedimento al fine di individuare, in particolare, idonee modalità di manifestazione del consenso degli interessati con riguardo sia alla semplice inclusione dei loro dati negli elenchi, sia all'utilizzo ulteriore dei medesimi dati per finalità riconducibili ad operazioni commerciali, di *marketing*, sondaggi, o simili.

32.5. Altre attività di cooperazione con l'Autorità per le garanzie nelle comunicazioni

In linea con gli obiettivi individuati nel corso della riunione congiunta fra il Garante e l'Autorità per le garanzie nelle comunicazioni del 20 febbraio 2003, si è intensificata l'attività di cooperazione fra le stesse.

Oltre ad incontri su temi di interesse comune, come il nuovo elenco telefonico unico per tutti gli operatori di telefonia fissa e mobile, nonché i servizi non richiesti, il Garante ha partecipato alla consultazione pubblica relativa all'introduzione in Italia del protocollo Enum (*e-number*), ponendo l'attenzione sulle problematiche concernenti la tutela della riservatezza degli interessati.

Protocollo Enum

Il protocollo Enum consente infatti di associare indirizzi Internet e numeri telefonici, al fine di realizzare un numero identificativo universale in grado di instradare il traffico verso i diversi recapiti dell'interessato, rendendo quest'ultimo facilmente rintracciabile.

L'Autorità, nel formulare le considerazioni preliminari sui possibili aspetti critici della materia, ha in particolare evidenziato agli operatori aderenti all'iniziativa alcuni profili relativi alla sicurezza e protezione dei dati personali. I primi risultati della consultazione, discussi anche all'interno di un *workshop* al quale hanno partecipato pure alcuni rappresentanti di questa Autorità, sono stati pubblicati nella *Gazzetta Ufficiale* del 24 aprile 2003, n. 95, e sono disponibili sul sito Internet dell'Autorità per le garanzie nelle comunicazioni *(www.agcom.it)*.

Carrier preselection

Sempre nel corso del 2003 si sono svolti incontri fra alcuni rappresentanti delle due Autorità di garanzia, al fine di verificare diversi punti problematici relativi alla tematica della *carrier preselection (Cps)*, ossia del sistema mediante il quale l'abbonato può instradare il proprio traffico telefonico verso un operatore preselezionato. Ciò, con particolare riferimento agli eventuali limiti ed alle modalità dei trattamenti dei dati connessi alle procedure per la disattivazione della *Cps*. Sull'argomento, l'Autorità ha già predisposto uno schema di provvedimento volto a chiarirne gli aspetti più controversi, ad esempio la necessità o meno per l'operatore di accesso di richiedere il consenso degli interessati.

32.6. Servizi non richiesti e consenso dell'interessato

Anche durante il periodo considerato il Garante ha prestato attenzione alle delicate questioni concernenti l'attivazione di contratti e servizi di telefonia mobile e fissa senza il preventivo consenso degli interessati, in riferimento a casi nei quali si verificano seri danni per gli interessati stessi. Sono stati effettuati anche taluni impegnativi interventi di carattere ispettivo. Uno degli interventi più significativi forma oggetto di trattazione dettagliata nel paragrafo di questa *Relazione* concernente le attività ispettive del capitolo relativo all'attività del Garante (cfr. *infra*, parag. 51.3.).

Sulla base delle informazioni acquisite, è già allo studio l'emanazione di un provvedimento di carattere generale volto ad offrire ulteriori indicazioni e chiarimenti in materia.

32.7. Comunicazioni indesiderate ed utenze telefoniche mobili

Il fenomeno delle comunicazioni di carattere pubblicitario o informativo realizzate su utenze telefoniche mobili ha subito di recente un'enorme espansione, vista la particolare efficacia con cui l'invio di *Sms (Short message service)* permette di comunicare in tempo reale con un numero elevato di interessati, ovunque essi si trovino, con modalità che possono, tra l'altro, risultare particolarmente invasive (si pensi alle ipotesi di ricezione del messaggio in orari notturni).

L'uso pur legittimo degli *Sms* presuppone dunque apposite cautele, specificamente evidenziate da questa Autorità in alcuni provvedimenti.

Sms *istituzionali*

Sms istituzionali

Il Garante ha individuato i principi che i fornitori di servizi di telecomunicazioni e le amministrazioni pubbliche sono tenuti a rispettare per l'invio degli *Sms* cd. istituzionali e cioè di quei messaggi utilizzati da amministrazioni centrali o locali per campagne informative e di sensibilizzazione (ad esempio, in relazione a giornate dedicate a particolari tematiche) o per diffondere notizie ritenute di pubblica utilità (ad esempio, in tema di viabilità, avvenimenti culturali, termini di pagamento di tasse o imposte o validità di documenti).

In un provvedimento del 12 marzo 2003, l'Autorità ha innanzitutto distinto l'ipotesi dell'invio effettuato da gestori di servizi telefonici su incarico delle pubbliche amministrazioni (con utilizzazione dei dati dei propri abbonati senza trasmetterli all'amministrazione che dispone l'invio) da quella dell'inoltro effettuato direttamente dal soggetto pubblico (che ha raccolto in proprio i dati degli abbonati).

Con riguardo al primo caso, è stato osservato che l'utilizzazione dei numeri di telefonia mobile da parte dei gestori per conto della pubblica amministrazione non può prescindere dal consenso espresso degli abbonati, prestato in forma specifica e documentato per iscritto, sia per semplici comunicazioni informative (blocco del traffico, pagamento tributi, ecc.), sia per ulteriori fini di pubblica utilità legati ad eventi culturali, ricorrenze o altro.

Si è inoltre specificato che gli operatori telefonici possono inviare *Sms* istituzionali, prescindendo dal consenso, solo in caso di disastri e calamità naturali o altre reali emergenze di ordine pubblico, e che l'invio dei messaggi in deroga alla disciplina sulla protezione dei dati può essere legalmente disposto solo da un soggetto

pubblico che adotti, se consentito dalla legge, un provvedimento d'urgenza per ragioni di ordine pubblico, igiene e sanità pubblica.

L'amministrazione pubblica deve a tal fine valutare preventivamente se la norma di legge che prevede l'adozione di provvedimenti urgenti conferisca effettivamente anche il potere di derogare alla disciplina in materia di trattamento dei dati personali e che, in presenza di accertati presupposti di necessità ed urgenza, la situazione di pericolo per la popolazione non possa essere affrontata con strumenti ordinari.

Gli operatori telefonici devono, in ogni caso, informare preventivamente ed adeguatamente gli utenti della possibilità di ricevere eventuali *Sms* istituzionali, nonché della possibilità di manifestare il consenso a ricevere solo alcune categorie di informazioni e non altre. L'interessato deve avere inoltre la possibilità di esercitare i propri diritti agevolmente e gratuitamente, anche in caso di precedente manifestazione del consenso. Gli operatori devono rispettare in ogni caso l'art. 9 della legge n. 675/1996 (ora, art. 11 del Codice). Di regola devono perciò essere seguite forme di comunicazione che non implichino l'identificazione nominativa degli abbonati. Inoltre l'operatore deve utilizzare i dati nei limiti e per il tempo necessario a trasmettere il messaggio.

Con riguardo, invece, all'invio di *Sms* istituzionali direttamente da parte dei soggetti pubblici ad utenti che abbiano liberamente lasciato i propri recapiti soltanto per essere informati sull'esito di una pratica o per ricevere sistematicamente alcuni tipi di messaggi (anche tramite reti civiche), il Garante ha chiarito che l'acquisizione del consenso è esclusa per l'invio di tali comunicazioni strettamente istituzionali.

È stato comunque richiamato l'obbligo dei soggetti pubblici di informare l'utente sulle modalità e sugli scopi dell'utilizzo dei dati che lo riguardano, nonché il principio secondo cui l'uso dei dati per l'invio degli *Sms* deve essere limitato alle finalità per le quali i dati sono stati rilasciati dagli utenti all'amministrazione.

Sms *pubblicitari*

Sms pubblicitari

Con un provvedimento del 10 giugno 2003 il Garante ha sottolineato l'illiceità dell'invio di *Sms* pubblicitari senza il preventivo consenso libero ed informato degli abbonati, nonché dell'espediente adottato da alcuni fornitori di servizi telefonici, di subordinare la stipula del contratto o l'attivazione della carta prepagata alla prestazione del consenso a ricevere messaggi pubblicitari. Si è pure evidenziato come sia illecito inserire tra gli obblighi contrattuali una dichiarazione *standard* di "impegno" all'invio degli *Sms* commerciali.

Anche i ben distinti messaggi con i quali le società telefoniche pubblicizzano servizi o opportunità che presuppongono un onere aggiuntivo per la clientela –come ha avuto modo di indicare l'Autorità con decisione del 9 aprile 2003– danno luogo ad un trattamento di dati a scopo promozionale ammesso solo con il consenso informato dell'interessato.

L'Autorità ha, inoltre, precisato che il principio del consenso libero ed informato trova applicazione anche nei confronti dei soggetti che trasmettono *Sms* pubblicitari senza estrarre i numeri delle utenze telefoniche da un'apposita banca dati, bensì sulla base di una composizione casuale o automatizzata di numeri, che prescinda da una verifica della loro esistenza o attivazione.

È stato chiarito, ancora, che la necessità di raccogliere una chiara e specifica manifestazione di volontà dei destinatari sussiste anche nel caso in cui gli *Sms* pubblicitari siano inviati da soggetti diversi dai fornitori di servizi di telefonia mobile, quali i fornitori di servizi telematici (ad esempio, gestori di siti *web* che offrano la possibilità di disporre gratuitamente di una casella di posta elettronica).

L'inosservanza dei principi fin qui sintetizzati è stata accertata in diversi ricorsi esaminati dal Garante nel corso dell'anno e concernenti l'invio anche notturno di *Sms* promozionali indesiderati. In questi casi l'Autorità ha avviato procedimenti autonomi rispetto a quelli instaurati con i ricorsi, al fine di verificare i presupposti per applicare sanzioni amministrative, per adottare altri provvedimenti e per l'eventuale denuncia all'autorità giudiziaria penale, in relazione ai reati che si possono configurare anche a seguito della mancata acquisizione del consenso informato degli interessati (*Provv.* 13 e 19 novembre 2003).

Il Codice, nel dettare una disciplina specifica in materia di comunicazioni commerciali non sollecitate, ha peraltro equiparato, quanto alla normativa applicabile, strumenti quali posta elettronica, *Sms*, *Mms* e *fax* (art. 130). Ne discende l'inapplicabilità, ai trattamenti effettuati con tali mezzi, delle fattispecie equipollenti al consenso dell'interessato di cui all'art. 24 del Codice e, quindi, anche l'inoperatività della disposizione riguardante, all'interno di tale articolo, i trattamenti di dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

32.8. Messaggi multimediali (cd. Mms*) e videochiamate*

Completata, con l'adozione del provvedimento del 12 marzo 2003 (in *Relazione* 2002, p. 115) l'analisi delle problematiche legate ai messaggi multimediali (*Mms*), il Garante ha esaminato la questione dei trattamenti di dati personali effettuati in occasione delle cd. videochiamate, ossia delle chiamate (realizzate attualmente tramite la rete *Umts*) nel corso delle quali possono essere trasmesse, oltre a suoni, immagini dei soggetti coinvolti nella conversazione.

La caratteristica peculiare di tali trattamenti consiste nel fatto che, a differenza di quanto accade per l'invio dei *Multimedia messaging service (Mms)*, vengono raccolte immagini contestualmente all'effettuazione della chiamata, le quali riguardano peraltro contemporaneamente il chiamante, il chiamato e persone eventualmente a loro vicine.

In proposito sono in corso di predisposizione chiarimenti ed indicazioni volte ad evitare che in occasione di questo tipo di chiamate si possano violare i diritti dei soggetti a vario titolo coinvolti.

32.9. Localizzazione

Con l'adozione del d.lg. n. 196/2003 è stata introdotta nel nostro ordinamento una disciplina specifica sul tema della localizzazione, che prevede apposite cautele per il trattamento dei dati relativi all'ubicazione diversi dai dati di traffico (art. 126). Ciò, sia per la specifica informativa che il titolare deve rendere preventivamente all'attivazione del servizio, sia in termini di revocabilità del consenso o momentaneo "congelamento" del servizio. La norma dispone infatti che l'interessato possa interrompere gratuitamente e mediante una funzione semplice, anche temporaneamente, il servizio a valore aggiunto.

Proprio in ragione della particolare delicatezza che caratterizza questo tipo di dati, l'Autorità adotterà entro breve termine, sulla base dei risultati di uno studio già ultimato in proposito, un provvedimento per chiarire alcuni termini della questione. Appare comunque utile ricordare che la Commissione europea ha affrontato alcuni aspetti della materia nella Raccomandazione del 25 luglio 2003 (2003/558/CE) sul trattamento delle informazioni relative alla localizzazione del chiamante sulle reti di comunicazione elettronica a fini della fornitura di servizi di chiamata di emergenza con capacità di localizzazione.

33 Trattamento di dati personali in Internet

33.1. Profili generali

Il progressivo sviluppo delle comunicazioni elettroniche ha determinato la crescita esponenziale di nuovi servizi e tecnologie. Se ciò ha comportato, da un lato, indiscutibili vantaggi in termini di semplificazione e rapidità nel reperimento e nello scambio di informazioni fra utenti della rete Internet, dall'altro, ha provocato un enorme incremento del numero e delle tipologie di dati personali trasmessi e scambiati, nonché dei pericoli connessi al loro illecito utilizzo da parte di terzi non autorizzati.

Si è così maggiormente diffusa l'esigenza di assicurare una forte tutela dei diritti e delle libertà delle persone, con particolare riferimento all'identità personale e alla vita privata degli individui che utilizzano le reti telematiche.

Nel corso del 2003 il Garante ha proseguito l'opera di costante monitoraggio dell'evoluzione tecnica del settore, promuovendo incontri e consultazioni con i diversi operatori, nonché con gli altri organi istituzionali interessati dalle tematiche trattate.

Si deve tenere presente, inoltre, che in ragione delle peculiarità del settore e dell'estrema rapidità con cui la tecnologia va evolvendosi, sono opportunamente destinati a svolgere un ruolo determinante, sul piano della disciplina dei trattamenti e delle garanzie per gli interessati, i codici deontologici e di buona condotta previsti da ultimo dal d.lg. 30 giugno 2003, n. 196.

Le diverse questioni emerse nella materia in esame confermano peraltro la necessità di una cooperazione internazionale, anche in ragione del recepimento in Italia del principio di stabilimento, che può limitare il potere di intervento dell'Autorità rispetto ai trattamenti di dati personali effettuati da soggetti situati all'estero (sul punto, cfr. il *Provv.* sullo *spamming* adottato dal Garante in data 29 maggio 2003, v. subito *infra*).

L'Autorità ha partecipato attivamente ai lavori svoltisi al riguardo nelle apposite sedi quali Ocse, Commissione europea e Gruppo dei garanti europei istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

In particolare, quest'ultimo ha esaminato le problematiche connesse a Internet ed alle reti di comunicazione nel parere n. 2/2003 del 13 giugno 2003. Sono stati

affrontati i problemi posti, in termini di protezione dei dati, dai cosiddetti *"database Whois"*, consultabili in rete, che contengono informazioni utili per contattare i responsabili dei domini o di siti Internet. In tale occasione, i Garanti hanno segnalato che non dovrebbero essere resi indiscriminatamente pubblici ed accessibili a chiunque i dati contenuti in tali elenchi, come pure l'esigenza di distinguere fra dati assolutamente necessari e dati "opzionali". Inoltre, l'utilizzazione di tali registri o elenchi per finalità di *marketing*, realmente massiccia, non è ammissibile alla luce della direttiva europea sulla protezione dei dati personali in quanto non è conforme agli scopi per i quali i registri stessi sono stati istituiti.

Database Whois

Degli orientamenti emersi a livello europeo il Garante italiano terrà conto anche nell'esame delle diverse segnalazioni e richieste di chiarimenti pervenute in ordine all'attuale regime di conoscibilità dei dati relativi ai soggetti che registrano siti *web* (cd. *registrant*). L'Autorità ha infatti in programma l'emanazione di un provvedimento generale che fornisca alcuni chiarimenti ed indicazioni agli operatori del settore. Specifici approfondimenti sono stati svolti in tal senso in occasione del *summit* mondiale organizzato da Icann a Roma nello scorso mese di marzo, durante il quale il segretario generale dell'Autorità è stato invitato ad illustrare le prospettive esistenti in materia in Italia alla luce del Codice.

33.2. Messaggi di posta elettronica non desiderati e nomi a dominio

L'Autorità ha adottato, in data 29 maggio 2003, un provvedimento generale relativo alla pratica dell'inoltro di messaggi di posta elettronica non sollecitati aventi carattere pubblicitario o commerciale (fenomeno comunemente noto come *spamming*), al fine di precisare il quadro normativo di riferimento ed offrire indicazioni utili agli operatori del settore.

Il Garante ha in primo luogo precisato che il consenso deve essere manifestato liberamente, in modo esplicito e, soprattutto, in forma chiara e differenziata rispetto alle diverse finalità ed alle categorie di servizi e prodotti offerti, prima dell'inoltro del messaggio commerciale. Tale disciplina non può essere peraltro elusa inviando una prima *e-mail* che, pur chiedendo il consenso, presenti un contenuto comunque promozionale o pubblicitario, oppure riconoscendo in concreto al destinatario un mero diritto di opposizione a ricevere in futuro altri messaggi pubblicitari (sistema cd. *opt-out*). Simili precisazioni sono coerenti con la disciplina generale in materia di comunicazioni commerciali non sollecitate dettata dal Codice, che, all'art. 130, ha recepito e rafforzato il principio della necessità del consenso preventivo ed informato (sistema cd. *opt-in*).

Il consenso del destinatario

Tuttavia, come anticipato nel provvedimento ora citato e, poi, confermato dallo stesso Codice (art. 130, comma 4), è stato introdotto nell'ordinamento un parziale temperamento al principio del consenso preventivo. In particolare, le aziende potranno, previa idonea informativa, inviare comunicazioni pubblicitarie o commerciali ai propri clienti con i quali già sussistono rapporti contrattuali, qualora questi ultimi abbiano in precedenza fornito, pur sempre previa idonea informativa, le proprie coordinate di posta elettronica nel contesto della vendita di un prodotto o di un servizio. Ciò, purché si tratti di prodotti o servizi analoghi a quelli per i quali era già stato instaurato un rapporto e purché sia offerta esplicitamente e senza ambiguità, all'inizio del rapporto e in occasione di ogni singolo invio, la possibilità di rifiutare tale pratica commerciale (prime indicazioni utili al

riguardo sono rinvenibili nel recente parere del Gruppo art. 29 di cui si tratta in questo stesso paragrafo).

Inoltre è stato chiarito che, nel caso in cui una società acquisisca da altre aziende banche dati contenenti indirizzi di posta elettronica, deve accertarsi che ciascun interessato abbia effettivamente acconsentito validamente alla comunicazione dell'indirizzo anche per fini di promozione pubblicitaria. In ogni caso, la società deve inviare agli interessati un messaggio di informativa, al fine di facilitare a questi ultimi l'esercizio dei diritti di cui all'art. 7 del Codice.

È stato pure ribadito il principio, più volte affermato dall'Autorità, secondo il quale la semplice conoscibilità di fatto di un indirizzo di posta elettronica (ad esempio, in quanto rinvenibile tramite *newsgroup*, *forum* o *chat*) non legittima l'invio di messaggi in assenza del preventivo consenso informato dell'interessato.

Nell'esaminare un ricorso, il Garante ha anche avuto occasione di chiarire che non richiede il preventivo consenso informato dell'interessato l'utilizzo di un indirizzo di posta elettronica rinvenibile in un *newsgroup*, qualora questo sia stato indicato dal medesimo interessato nell'ambito del gruppo di discussione per una specifica finalità e il dato venga utilizzato conformemente alla finalità indicata. In questa ipotesi, è stato ritenuto lecito l'inoltro di una *e-mail* inviata in risposta alla richiesta di informazioni formulata dal ricorrente in un *newsgroup*, poiché l'*e-mail* si riferiva appunto a questioni del tutto pertinenti e correlate con il tema oggetto di discussione (*Provv.* 21 marzo 2003).

Deve però rilevarsi che, in ragione del principio di stabilimento recepito dal Codice, qualora i messaggi provengano da Paesi terzi, il Codice stesso potrebbe risultare inapplicabile. Tuttavia, a parte la possibilità che si applichi comunque la legge penale italiana in virtù di altre circostanze relative ad esempio a reati connessi (es. truffa), vi è non di rado l'ulteriore eventualità di potersi rivolgere alle competenti autorità del Paese nel quale lo *spamming* è considerato illecito in base alla relativa disciplina nazionale.

L'attività di *spamming*, specie se sistematica ed effettuata a fini di profitto o per arrecare ad altri un danno, quando provoca un nocumento costituisce reato e può essere denunciata all'autorità giudiziaria penale (cfr. art. 167 del Codice). È sanzionato penalmente anche l'invio di messaggi indesiderati a scopo promozionale o pubblicitario omettendo l'indicazione del mittente del messaggio e dell'indirizzo fisico presso il quale i destinatari possono rivolgersi per chiedere che i dati personali non vengano più usati.

Il Garante ha intensificato le attività di controllo e verifica presso fornitori di servizi di comunicazione elettronica, individuati grazie anche alle numerosissime segnalazioni pervenute pure nel 2003. In alcuni casi ciò ha portato a sospendere le attività illecite per effetto di provvedimenti di blocco delle banche dati o di divieto di ulteriori trattamenti. Altre volte ne è poi conseguita l'adozione di sanzioni, anche a seguito delle risultanze emerse dalla trattazione dei numerosi ricorsi decisi in materia.

Lo *spamming* nel contesto internazionale

Il tema dello *spamming* è stato oggetto di particolare attenzione altresì a livello internazionale.

A tale questione l'Ocse ha dedicato numerosi documenti e gruppi di lavoro, trattandosi di un argomento rispetto al quale c'è una particolare sensibilità nei Paesi membri. Dopo la creazione di un apposito gruppo di discussione, cui hanno partecipato ventitre delegazioni, si è organizzato un seminario internazionale ospitato dalla Commissione europea, per tracciare un bilancio delle iniziative intraprese ed elaborare una strategia di contrasto comune. Al Garante, rappresentato dal segretario generale, è stato chiesto di svolgere una relazione sui meccanismi di *enforcement* volti ad assicurare l'effettivo rispetto della legge.

È stata ribadita da molti, in questa circostanza, l'esigenza di affrontare il tema a livello sovranazionale e con un approccio che tenga conto della tutela dei consumatori, della sicurezza informatica e della protezione dei dati personali. Anche l'elenco delle soluzioni proposte mette in luce la necessità di combinare insieme misure tecniche, legislative, disposizioni di autoregolamentazione e campagne di sensibilizzazione rivolte ad utenti ed imprese. Un forte impegno su scala internazionale in questo settore è fondamentale per preservare la fiducia dei consumatori e delle imprese nello sviluppo di Internet. Lo *spamming* può essere collegato ad altre attività illegali, ciò che comporta il rischio di un arresto nello sviluppo sia dell'*e-commerce* sia dell'*e-government*. Per tali ragioni l'Ocse ha proposto una riflessione comune tra i rappresentanti dei governi, delle imprese e del mondo accademico. In proposito è stata effettuata una raccolta di materiali e documenti frutto dei lavori.

A livello comunitario, il Gruppo dei garanti europei ha di recente ritenuto doveroso adottare un parere (Parere n. 5/2004 WP 90 del 27 febbraio 2004), al fine di fornire un'interpretazione uniforme dell'art. 13 della direttiva n. 2002/58/CE in tema di comunicazioni commerciali non richieste, evitando divergenze nel suo recepimento e nella sua concreta applicazione da parte dei diversi Stati membri. Secondo il Gruppo, il concetto di *e-mail* deve essere interpretato nel senso di ritenere che si configura una comunicazione elettronica ogni qualvolta non sia richiesta la simultanea partecipazione del mittente e del destinatario. Il requisito del previo consenso *("opt-in")*, poi, può essere derogato solo nel caso in cui i dati siano stati già forniti nell'ambito di un rapporto commerciale preesistente ed il *marketing* si riferisca a prodotti o servizi che, eventualmente riguardati anche dal punto di vista obiettivo del destinatario della comunicazione, siano "simili" a quelli oggetto del rapporto, nei termini suggeriti dal parere.

33.3. Il codice deontologico

Sulla base dell'art. 133 del d.lg. n. 196/2003, il Garante, nell'ambito di una più generale collaborazione con i diversi operatori del settore, intende portare a conclusione in tempi rapidi (nonostante la complessità dell'argomento) le attività necessarie per la sottoscrizione del codice di deontologia e buona condotta sui trattamenti dei dati personali effettuati da fornitori di servizi di comunicazione e informazione offerti per via telematica. Ciò consentirà di fornire ulteriori criteri per assicurare una più adeguata informazione e consapevolezza agli utenti delle reti di comunicazione elettronica, nonché di favorire una maggiore trasparenza e correttezza nei confronti dei medesimi utenti ed il pieno rispetto dei principi di cui all'art. 11 del Codice.

Nel codice deontologico saranno disciplinati, tra l'altro, i presupposti ed i limiti entro i quali è lecito l'utilizzo della rete di comunicazione elettronica per accedere

ad informazioni archiviate nell'apparecchio dell'utente. In tale sede potranno pertanto essere individuate le regole per l'utilizzo lecito dei cd. *cookies*, ai quali fa riferimento anche la Raccomandazione n. 2/2001 del Gruppo dei garanti europei, relativa ai requisiti minimi per la raccolta di dati *on line* nell'Unione europea.

La rilevanza del codice deontologico è accresciuta dal fatto che il rispetto delle disposizioni in esso contenute costituirà condizione di liceità e correttezza del trattamento dei dati personali (art. 12, comma 3, d.lg. n. 196/2003).

Il trasferimento di dati personali all'estero

34 I trasferimenti all'estero di dati

Con il Codice è stata aggiornata la disciplina del trasferimento dei dati personali all'estero (Parte I, Capo VII), completando il recepimento della direttiva comunitaria n. 95/46/CE. È stato ribadito il principio generale in base al quale i flussi di dati verso un Paese situato al di fuori dell'Unione europea sono consentiti solo se tale Paese assicura un adeguato livello di tutela delle persone (v., al riguardo, le autorizzazioni rilasciate negli anni scorsi dal Garante in relazione al livello di adeguatezza del sistema di tutela dei dati personali previsto in Svizzera ed Ungheria, nonché ai principi del Safe Harbor circa il trasferimento dei dati verso gli Stati Uniti), ovvero se sussiste uno dei presupposti di liceità indicati dalla normativa nazionale (consenso dell'interessato, adempimento di obblighi contrattuali, ecc.).

Anche nel corso del 2003 e nei primi mesi del 2004, significativa è stata l'attività svolta dal Garante per dare attuazione ad alcune decisioni comunitarie relative al settore in esame.

Si segnalano, al riguardo:

- la deliberazione n. 6 del 30 aprile 2003, con cui l'Autorità italiana ha dato attuazione alla decisione della Commissione europea del 20 dicembre 2001, con la quale si è ritenuto adeguato il livello di protezione dei dati personali in Canada (v. *Relazione* 2002, p. 128);

- la deliberazione n. 2 del 15 aprile 2004, con cui il Garante ha attuato la decisione comunitaria del 21 novembre 2003 n. 2003/821/CE, recante il riconoscimento del Bailato di Guernsey tra i Paesi che garantiscono nel proprio ordinamento un adeguato livello di protezione dei dati personali.

A tale ultimo riguardo va specificato che il Gruppo dei garanti europei istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE, nel proseguire la propria attività di valutazione dell'adeguatezza del livello di protezione garantito da Stati non appartenenti all'Ue, si era pronunciato favorevolmente sul Bailato di Guernsey con il parere n. 5/2003 del 13 giugno 2003. Di conseguenza, la Commissione europea ha adottato la citata decisione n. 2003/821/CE con la quale ha stabilito che il livello di protezione dei dati nel territorio di Guernsey è "adeguato" ai fini del trasferimento di dati personali dall'Ue verso soggetti ivi residenti.

Sempre nella materia in esame, è in procinto di essere resa operativa in Italia anche la decisione della Commissione europea n. 2003/490/CE del 30 giugno 2003, riguardante l'adeguatezza del livello di tutela dei dati personali esistente in Argentina, su cui si era già espresso in senso favorevole, con il parere n. 4 del 3 ottobre 2002, il Gruppo dei garanti europei.

Infine, una decisione di contenuto analogo è in procinto di essere adottata dalla Commissione europea anche per l'Isola di Man, alla luce del parere favorevole del Gruppo (Parere n. 6/2003 del 21 novembre 2003).

Come anticipato nella *Relazione* per il 2002 (v. ivi, p. 127), il 2003 è stato inoltre caratterizzato da un intenso monitoraggio da parte dell'Autorità sulle attività di trasferimento di dati all'estero effettuate da alcuni operatori italiani, con particolare riguardo al tipo di garanzie adottate per tutelare i diritti degli interessati. Ciò allo scopo di verificare lo stato di attuazione delle disposizioni comunitarie e nazionali sui flussi di dati all'estero, prima di avviare specifici accertamenti relativi a singole società.

Indagine del Garante sulle attività di trasferimento dei dati

Dall'indagine svolta è emerso che:

- circa l'84% delle società interpellate effettua trasferimenti di dati all'estero; le aree geografiche di maggiore interesse sono rappresentate dagli Usa, dall'Europa dell'Est, dall'America centro-meridionale, dall'Africa, dalla Svizzera e dall'Asia;

- nel 40% circa dei casi analizzati, i dati personali oggetto di trasferimento all'estero riguardano principalmente dipendenti e, in misura minore, ma comunque non trascurabile, anche altre società o imprese (in qualità di clienti, concorrenti, fornitori, ecc.);

- i flussi di dati sono stati o sono effettuati, di regola, previa acquisizione del consenso specifico degli interessati o sulla base degli altri presupposti di legge (ad es., per l'esecuzione di obblighi contrattuali);

- soltanto in un numero ristretto dei casi esaminati (il 5% circa), relativi a flussi stabili e più complessi di dati, le società interpellate hanno utilizzato le clausole contrattuali *standard* indicate dalla Commissione europea;

- in alcune limitate ipotesi, caratterizzate dal fatto che la gestione delle risorse umane viene effettuata negli Usa, gli importatori dei dati (società capogruppo o comunque collegate o controllate) hanno aderito all'accordo sui principi del *Safe Harbor*, dichiarandosi in genere disponibili a cooperare con le autorità per la protezione dei dati dei Paesi europei.

L'indagine dimostra che nuovi strumenti, come le clausole contrattuali, cominciano ad essere utilizzati nell'ambito delle prassi economiche e commerciali con aziende di altri Paesi e che tali strumenti possono essere ancora migliorati, in particolare con riguardo alla disciplina di fenomeni più complessi e frequenti a livello internazionale, quali quelli relativi a gruppi societari, a rapporti multilaterali tra imprese, o al conferimento a terzi, all'estero, di attività o servizi precedentemente svolti in proprio (cd. *outsourcing*).

In argomento, il Gruppo di lavoro istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE ha evidenziato l'opportunità di introdurre eventuali correttivi, prevedendo ulteriori garanzie e regole di comportamento in aggiunta alle clausole contrattuali tipo già predisposte (v. il paragrafo seguente).

35 Le clausole contrattuali tipo

Diverse imprese e gruppi societari, operanti a livello internazionale, si sono rivolti al Garante per ottenere informazioni e chiarimenti sulla corretta applicazione della normativa in materia di trasferimento all'estero dei dati personali.

In particolare, l'Autorità ha esaminato un caso relativo alla realizzazione a livello internazionale di un sistema informativo centralizzato di gestione delle risorse umane di diverse società situate in vari Stati dell'Ue, tra cui l'Italia, affidato in *outsourcing* ad una società con sede negli Usa (ipotesi frequente in questi ambiti).

Contratto globale

Al fine di rendere lecito il trasferimento all'estero dei dati dei dipendenti nell'ambito di questa operazione, è stato sottoscritto, anche per conto delle società appartenenti ai gruppi societari coinvolti nella gestione di tali dati, un contratto cd. globale basato sulle clausole contrattuali-tipo relative ai flussi transfrontalieri di dati tra autonomi titolari del trattamento (cfr. decisione della Commissione europea del 15 giugno 2001, n. 2001/497/CE, attuata in Italia attraverso l'autorizzazione generale del Garante n. 35 del 10 ottobre 2001).

Le clausole contrattuali-tipo consentono alle imprese di trasferire dati personali nel rispetto dei principi della direttiva anche quando il Paese di destinazione non abbia una legislazione adeguata, prevedendo idonee garanzie attraverso strumenti negoziali.

Sulla base delle osservazioni formulate dal Garante e dalle altre Autorità di controllo europee interpellate, è stato predisposto poi uno schema di contratto integrativo del precedente, basato sulle clausole contrattuali-tipo indicate nell'autorizzazione generale n. 3 del 10 aprile 2002 e relative al trasferimento dei dati a responsabili del trattamento residenti in Paesi terzi.

L'Autorità si è, inoltre, espressa favorevolmente circa il mantenimento, nel contratto integrativo, della previsione di una responsabilità disgiunta e solidale dell'esportatore e dell'importatore dei dati per i danni subiti dagli interessati a causa della violazione delle regole contrattuali. Le imprese od enti che si avvalgono dei contratti *standard* possono infatti inserire ulteriori clausole pertinenti, purché non risultino limitative o incompatibili con le clausole-tipo approvate dalla Commissione europea. Si è ritenuto pertanto opportuno conservare nello schema di contratto la clausola sulla responsabilità appena descritta, in quanto espressiva di una maggiore garanzia per il risarcimento dei danni eventualmente causati agli interessati: questi ultimi potrebbero così attivare direttamente un'azione legale nei confronti di entrambe le parti contrattuali.

L'Autorità ha sottolineato, infine, la necessità che lo schema di contratto stipulato tra le società interessate anche in nome e per conto delle rispettive società controllate e collegate venga sottoscritto da ciascuna di queste società o, comunque, dalla maggior parte di quelle per le quali la capogruppo non abbia uno specifico mandato o procura a rappresentarle.

L'Autorità è anche giunta alla conclusione di considerare applicabile allo schema di contratto in esame l'autorizzazione generale n. 3 del 10 aprile 2002: non è,

quindi, necessario il rilascio di una specifica autorizzazione del Garante per trasferire all'estero i dati in questione.

Sempre in tema di trasferimento dei dati verso Paesi non appartenenti all'Ue (cd. Paesi terzi), il Gruppo dei garanti europei ha approfondito e sviluppato il lavoro sulle clausole contrattuali-tipo.

Binding corporate rules

Il Gruppo ha avviato una riflessione su quest'ultimo punto con riferimento al livello di tutela che può essere garantito dall'adozione di norme che possono apportare un vincolo nell'impresa (cd. *binding corporate rules*), una sorta di codici di condotta elaborati nell'ambito di un gruppo di imprese e impegnativi per tutti i soggetti che ne fanno parte. Con un documento di lavoro (WP del 3 giugno 2003) sono state formulate alcune indicazioni preliminari sulle condizioni in base alle quali questi speciali codici di condotta possono offrire garanzie sufficienti ai fini del trasferimento di dati verso Paesi terzi che non dispongano di un livello adeguato di protezione dei dati, con particolare riferimento ai trasferimenti fra società appartenenti ad uno stesso gruppo multinazionale.

Un modello alternativo di clausole contrattuali-tipo rispetto a quelle approvate con la decisione della Commissione n. 497/2001/CE ha formato oggetto di un successivo parere (Parere 8/2003 del 17 dicembre 2003). Il Gruppo ha espresso una valutazione positiva su un progetto di clausole contrattuali presentato dalla Camera di commercio internazionale e da altre organizzazioni commerciali, suggerendo alcune modifiche al fine rendere il livello di tutela equiparabile a quello delle clausole approvate dalla Commissione.

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.

In relazione ai campioni di materiali genetici, viene ribadita la necessità di garantire pienamente i diritti degli interessati durante il trattamento, così come l'opportunità di distruggere o rendere anonimi i campioni non appena ottenute le informazioni necessarie, anche in considerazione del loro eventuale impiego per fini di clonazione. Tutti i dati genetici devono inoltre essere trattati solo da professionisti qualificati, sulla base di specifiche autorizzazioni e regole.

Il documento si chiude invitando le autorità nazionali a svolgere un ruolo attivo nei rispettivi Paesi, con la previsione di forme di *prior checking* (in particolare per le cd. bio-banche) e ponendo l'accento sulla necessità di applicare i principi di proporzionalità e finalità.

La Conferenza di Sydney

44 La Conferenza e le Risoluzioni

Il Garante ha partecipato a numerose conferenze internazionali (su cui *infra*, parag. 52.3.): in questa sede va ricordata in particolare la partecipazione alla 25ª Conferenza internazionale delle autorità per la protezione dei dati personali, svoltasi a Sydney dal 10 al 12 settembre 2003.

La conferenza australiana ha rappresentato, infatti, un momento significativo nella discussione su una serie di temi emersi recentemente con piena evidenza: i prossimi passi nella regolamentazione della protezione dei dati personali, gli effetti che le normative sulla *privacy* producono a livello globale su imprese e consumatori, gli organismi, le tecnologie e gli incentivi per sostenere e sviluppare la difesa del diritto alla riservatezza, le implicazioni della protezione dei dati personali in campo giuridico, i rapporti tra tutela dell'ordine pubblico e rispetto delle persone, il ruolo svolto dalla *privacy* nella società contemporanea.

Alla Conferenza, che ha visto riuniti rappresentanti delle autorità per la protezione dei dati personali, esperti, imprese e rappresentanti governativi di oltre quaranta Paesi, l'autorità italiana ha partecipato con una delegazione guidata dal presidente prof. Stefano Rodotà, dal componente del collegio, on. Mauro Paissan e dal segretario generale, Giovanni Buttarelli. Il prof. Rodotà ha presieduto la sessione inaugurale dedicata alle nuove prospettive di regolamentazione della *privacy*. La Conferenza è stata preceduta da seminari di formazione e conferenze su diversi argomenti: tra queste va segnalata quella svoltasi l'8 settembre 2003 a Melbourne, dedicata a corpo fisico, corpo elettronico e dati personali, aperta dallo stesso prof. Rodotà.

La Conferenza si è conclusa con l'approvazione di cinque risoluzioni che richiamano l'attenzione su aspetti attuali e significativi della vita privata dei cittadini.

44.1. Trasferimento dei dati dei passeggeri

Una risoluzione riguarda il trasferimento di dati personali riguardanti i passeggeri da parte delle compagnie aeree alle autorità statunitensi. In essa viene affermato che nella lotta contro il terrorismo e la criminalità organizzata gli Stati devono osservare i principi fondamentali in materia di protezione dei dati, e che le informazioni sui viaggiatori diretti negli Usa possono essere acquisite e trasferite solo all'interno di un contesto che tenga conto delle esigenze di protezione dei dati ed in base ad un accordo internazionale. Questo accordo dovrebbe contenere norme adeguate in relazione ad alcuni profili: limitazione delle finalità, non eccedenza dei dati raccolti, tempi di conservazione, informativa, diritto di accesso, previsione di un'autorità di controllo indipendente.

44.2. Informativa

Al tema dell'informativa e, in particolare, all'esigenza di migliorarne insieme la chiarezza e l'efficacia dei contenuti è stata dedicata un'altra risoluzione, in cui è stato affermato che l'informativa deve essere il più possibile chiara e concisa. Le autorità garanti si sono impegnate ad elaborare un modello *standard* che soggetti pubblici e privati potranno utilizzare per fornire informazioni essenziali sul trattamento con un linguaggio semplice, inequivocabile e diretto. Nel modello deve essere specificato il soggetto che tratta i dati e le finalità per le quali li tratta. Inoltre, deve essere spiegato come contattare tale soggetto e quali sono i diritti riconosciuti agli interessati e deve indicarsi l'autorità di controllo alla quale rivolgersi. Nell'informativa sintetica saranno poi forniti gli elementi per reperire ulteriori informazioni, secondo le esigenze del singolo interessato. Questa informativa deve essere fornita prima di richiedere qualsiasi dato personale e, per quanto riguarda il settore telematico, possibilmente in maniera automatizzata (su questo punto la Conferenza si è richiamata espressamente al lavoro svolto in materia dal Gruppo di cui all'art. 29 della direttiva europea n. 95/46/CE).

Le autorità hanno anche ribadito la propria disponibilità a collaborare con tutti i soggetti impegnati a migliorare la comunicazione fra imprese, pubblica amministrazione e cittadini, in un'ottica di trasparenza e di rispetto per la vita privata.

44.3. Organizzazioni internazionali

Una terza risoluzione si è occupata degli organismi internazionali e sovranazionali. Le autorità hanno invitato questi ultimi ad impegnarsi nell'osservare le regole compatibili con i principi fissati a livello internazionale nella materia della tutela della *privacy* (direttive Ue, raccomandazioni del Consiglio d'Europa, linee-guida Ocse), tra le quali la creazione di autorità di controllo interne, effettivamente indipendenti sul piano operativo. È poi necessaria, a giudizio delle autorità garanti, una valutazione preliminare dell'impatto in materia di riservatezza di qualsiasi norma o regolamento elaborato da un organismo internazionale e che abbia riflessi sulla legislazione dei singoli stati.

44.4. Aggiornamenti automatici di software

Gli aggiornamenti automatici di *software* hanno formato oggetto di un'altra risoluzione adottata a Sydney. In particolare è stato rilevato che le case produttrici di *software* ricorrono sempre più a meccanismi non trasparenti per trasferire aggiornamenti di *software* nei computer dei singoli utenti. Per evitare i rischi derivanti dalla possibilità di leggere e raccogliere dati personali memorizzati nel *computer* dei singoli utenti senza che questi ne abbiano consapevolezza, e per non esporre gli utenti stessi al rischio di commettere involontariamente un illecito, la Conferenza ha invitato le società:

- ad aggiornare il *software on line* solo su richiesta dell'utente, secondo procedure trasparenti;

- a non richiedere dati personali se non assolutamente necessari per effettuare l'aggiornamento, anche in tal caso solo con il consenso informato dell'utente.

La risoluzione ha inoltre sottolineato l'opportunità di offrire forme alternative di distribuzione del *software* (ad esempio, attraverso specifici *Cd-Rom*).

44.5. **Radio frequency identification**

L'ultima risoluzione, adottata non contestualmente allo svolgimento della Conferenza, si è occupata del tema dell'identificazione attraverso radiofrequenze *(Rfid)*.

I dispositivi basati su tale sistema, che vengono utilizzati sempre più spesso, comportano significative implicazioni anche in materia di tutela della *privacy*. La tecnologia impiegata, infatti, potrebbe ricostruire le attività di singoli individui e istituire collegamenti fra le informazioni raccolte e banche dati preesistenti.

Per tali motivi le autorità garanti hanno invitato i titolari di trattamenti ad utilizzare, laddove possibile, approcci alternativi rispetto alla raccolta di dati personali o alla profilazione della clientela. Quando tale tecnologia risulta indispensabile, per scopi legittimi, la raccolta deve essere comunque chiara e trasparente, i dati devono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati raccolti e conservati solo fino al raggiungimento di tale scopo, e gli interessati dovrebbero avere la possibilità di cancellare i dati e di disattivare o distruggere le etichette *Rfid*. Viene inoltre sottolineata l'importanza di tener conto dei principi enunciati in materia di dati personali anche nella fase di progettazione e nell'utilizzazione di prodotti cui siano applicabili tecnologie basate su *Rfid*.

IL GARANTE

VI - L'attività del Garante

45 La collaborazione fornita dal Garante alle attività del Parlamento e del Governo

45.1. L'Autorità e le attività di sindacato ispettivo e di indirizzo del Parlamento

Anche nel corso del 2003 l'Autorità ha seguito con attenzione l'attività di sindacato ispettivo e di indirizzo esercitata dal Parlamento, in relazione agli aspetti di specifico interesse in materia di protezione dei dati personali, fornendo al Governo, laddove richiesto, i chiarimenti e le indicazioni necessarie.

Sono stati pure inviati al Governo gli elementi richiesti in relazione ad alcuni atti di sindacato fra i quali, in particolare, un'interrogazione a risposta immediata presentata dall'on. Folena (3-02832), relativa all'acquisizione da parte degli Usa dei dati dei passeggeri conservati nella banca dati dell'Alitalia (*Nota* 4 novembre 2003). In tale occasione il Garante ha ricordato, fra l'altro, che la richiesta formulata dalle autorità americane alle compagnie aeree di accedere a tutti i dati contenuti nel *Pnr* (*Passenger name record*, su cui cfr. *supra*, parag. 36.) relativi ad individui diretti, provenienti o in transito verso gli Stati Uniti, va valutata alla stregua delle disposizioni comunitarie in materia (in particolare, l'art. 25 della direttiva n. 95/46/CE).

Va infine ricordato che due mozioni analoghe della maggioranza (1-00304 Leone ed altri) e dell'opposizione (1-00215 Folena ed altri), poi approvate all'unanimità dal Parlamento il 14 gennaio 2004, con riferimento alle problematiche inerenti alla conversione del d.l. n. 354/2003 hanno impegnato il Governo a rimuovere tutte le norme potenzialmente lesive dei diritti di riservatezza e a regolamentare in modo più efficace il trattamento dei dati di traffico della telefonia mobile, al fine di tutelare il diritto degli individui (sul punto, cfr. più diffusamente parag. 1.11.).

45.2. L'attività consultiva del Garante sugli atti del Governo

L'articolo 154, comma 4, del d.lg. n. 196/2003 (che riproduce l'art. 31, comma 2, della legge n. 675/1996) stabilisce che il Presidente del Consiglio dei ministri e ciascun ministro debbano consultare il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere in materia di protezione di dati personali.

In relazione a tale competenza, nel corso dell'anno il Garante ha espresso vari pareri anche in importanti materie, fra cui, in particolare, quelli riguardanti:

- due schemi di regolamento in attuazione della legge n. 189/2002 concernenti, l'uno, il riordino del regolamento di attuazione del testo unico in materia di immigrazione e condizione dello straniero (d.P.R. n. 394/1999) e, l'altro, lo sviluppo e la razionalizzazione dei sistemi informativi delle pubbliche amministrazioni coinvolte nell'applicazione della legge, in particolare ai fini del funzionamento dello sportello unico per il rilascio del permesso di soggiorno (*Parere* 4 marzo 2004);

Il permesso di soggiorno elettronico

- lo schema di decreto interministeriale (Ministri per l'innovazione e le tecnologie e dell'interno) che disciplina il permesso di soggiorno elettronico. Dopo un primo parere del 15 ottobre 2003, a seguito di incontri tecnici tra rappresentanti dell'Autorità e del Ministero dell'interno, in cui sono stati forniti chiarimenti sul piano applicativo, il Garante ha formulato un secondo parere il 4 marzo 2004 con il quale ha, fra l'altro, indicato gli interventi necessari per garantire gli interessati in occasione della raccolta delle impronte digitali e, in particolare, nel caso di inserimento di dati biometrici nel documento elettronico. Al riguardo, l'Autorità ha anche confermato la propria disponibilità a proseguire la cooperazione con il Ministero al fine di approfondire i problemi ed i rischi derivanti dalle differenti tecniche di identificazione e di autenticazione, descritte dai Garanti europei a proposito dei dati biometrici nel parere del 1° agosto 2003 (su cui, *supra*, parag. 38.). Ciò anche allo scopo di individuare le cautele necessarie nella fase di attivazione del documento elettronico e di consegna dei documenti o di accesso selezionato ai dati, nonché le migliori garanzie di sicurezza disponibili. L'esito di tali approfondimenti potrebbe essere trasfuso nelle misure e negli accorgimenti che, in materia di dati biometrici, devono essere individuati dal Garante ai sensi dell'art. 55 del Codice;

- lo schema di decreto del Presidente della Repubblica recante il regolamento di disciplina dell'accesso al servizio di informatica giuridica del Centro elettronico di documentazione (C.e.d.) della Corte di cassazione (*Parere* 27 febbraio 2004).

- lo schema di regolamento (Ministri per la funzione pubblica e dell'interno) di gestione dell'Indice nazionale delle anagrafi (I.n.a.), in attuazione dell'art. 2-*quater* del decreto legge 27 dicembre 2000, n. 392, convertito dalla legge n. 26/2001 (*Parere* 13 febbraio 2004);

- uno schema di decreto dirigenziale del Ministero della giustizia, di attuazione in via parziale e transitoria dell'art. 39 del d.P.R. 14 novembre 2002, n. 313 (testo unico delle disposizioni legislative e regolamentari in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti), concernente la consultazione del casellario giudiziale da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi (*Parere* 28 gennaio 2004).

In occasione degli incontri di lavoro che hanno preceduto la redazione dello schema di decreto, l'Autorità aveva constatato il carattere transitorio della soluzione elaborata, in attesa di una regolamentazione definitiva della procedura di accesso diretto ai sensi dell'art. 39 del d.P.R. n. 313/2002. Nel parere del 28 gennaio 2004 è stata sottolineata la necessità che l'accesso ai dati giudiziari registrati nel casellario giudiziale, nonché il successivo utilizzo da parte delle pubbliche amministrazioni e dei gestori di pubblici servizi, siano consentiti nel rispetto dei limiti previsti dallo stesso d.P.R. n. 313/2002 e in misura proporzionata alle finalità da perseguire.

Consultazione ed utilizzo dei dati del casellario giudiziale da parte delle p.a.

Le osservazioni del Garante hanno tenuto conto anche del ricorso presentato da un privato interessato all'aggiudicazione di un appalto, che lamentava l'utilizzo da parte della pubblica amministrazione, ai fini dell'esclusione dalla gara, di dati contenuti in un certificato generale del casellario, contestando che quest'ultimo potesse essere rila-

sciato ad un soggetto pubblico, considerata l'equiparazione dei certificati rilasciabili ai privati interessati e alle pubbliche amministrazioni. L'Autorità ha ritenuto infondate le tesi del ricorrente, alla luce della normativa vigente, che consente alla pubblica amministrazione di acquisire dal casellario i dati necessari per accertamenti d'ufficio o per il controllo delle autodichiarazioni presentate dai privati (il ricorrente ha impugnato la decisione davanti all'autorità giudiziaria: v. pure *supra*, parag. 27.). Tuttavia, sia nella decisione del ricorso, sia nel parere del 28 gennaio scorso, il Garante ha richiamato l'attenzione del Ministero della giustizia sulla necessità di completare al più presto ed in via definitiva la messa a punto del sistema di consultazione in via telematica del casellario da parte delle pubbliche amministrazioni e dei gestori di pubblico servizio, superando l'attuale fase transitoria così da consentire un utilizzo selettivo delle informazioni necessarie nell'ambito dello specifico procedimento avviato;

- lo schema di d.P.C.M. recante regole tecniche per la generazione, apposizione e verifica delle firme digitali, adottato ai sensi del testo unico in materia di documentazione amministrativa (d.P.R. n. 445/2000), in sostituzione del d.P.C.M. 8 febbraio 1999 (Parere 19 novembre 2003);

- lo schema di regolamento recante disposizioni per il diritto di accesso agli atti delle imprese di assicurazione, in attuazione dell'art. 3 della l. 5 marzo 2001, n. 57 (*Parere* 13 agosto 2003). A tal proposito, si sottolinea che le indicazioni fornite dal Garante in merito alla necessità di mantenere chiara la distinzione tra il diritto di accesso agli atti delle imprese di assicurazione ed il diritto di accesso ai dati di cui al d. lg. n. 196/2003, sono state recepite nel d.m. 20 febbraio 2004, n. 74 (v. in particolare l'art. 1, comma 2);

- lo schema del regolamento di attuazione ed organizzazione della banca dati relativa ai minori dichiarati adottabili istituita dall'articolo 40 della legge 28 marzo 2001, n. 149 (*Parere* 11 luglio 2003); il regolamento è stato poi adottato con d.m. 24 febbraio 2004, n. 91 in *Gazzetta Ufficiale* 9 aprile 2004, n. 84;

Carta nazionale dei servizi

- lo schema di d.P.R. recante il regolamento sulle caratteristiche e le modalità per il rilascio della Carta nazionale dei servizi (*Parere* 9 luglio 2003). In tale parere il Garante ha richiesto un'attenta valutazione, da parte dell'amministrazione procedente, circa la pertinenza dei dati da inserire nella carta, che in ogni caso non potrebbero essere dati sensibili; si è inoltre espresso in favore della loro utilizzazione da parte delle amministrazioni esclusivamente a fini di identificazione dell'interessato e di legittimazione al servizio offerto. L'Autorità ha poi richiesto che le disposizioni dello schema relative all'utilizzo dell'Indice nazionale delle anagrafi (Ina) fossero rese coerenti con la funzione propria di tale indice, che è quella di mero strumento per l'individuazione agevole del comune di residenza degli interessati e non di sostanziale anagrafe nazionale;

- lo schema di regolamento per la tenuta dei fascicoli personali della carriera diplomatica ai sensi dell'art. 113 del d.P.R. n. 18/1967 (*Parere* 19 giugno 2003). Il regolamento è stato poi adottato con il decreto del Ministro degli affari esteri 13 ottobre 2003, n. 311;

- lo schema di regolamento concernente le modalità di istituzione e tenuta presso la Presidenza del Consiglio dei ministri della banca dati informatica dei componenti degli organi di amministrazione attiva, consultiva e di controllo dello Stato e degli enti pubblici a carattere nazionale e delle relative modalità di nomina (*Parere* 9 aprile 2003);

- lo schema di regolamento in materia di estensione delle disposizioni antiriciclaggio ad attività non finanziarie particolarmente suscettibili di utilizzazione a fini di riciclaggio, in attuazione dell'art. 4, comma 8, del d.lg. 25 settembre 1999, n. 374 (*Parere* 12 marzo 2003).

46 La cooperazione a livello europeo

46.1. L'attività del Gruppo istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE

Nel 2003 è proseguita la tendenza ad un ampliamento del ruolo e delle competenze del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito ai sensi dell'art. 29 della direttiva n. 95/46/CE.

Intenso è stato il lavoro svolto da tale Gruppo per interpretare, segnalare ed indirizzare l'attività della Commissione europea in relazione all'applicazione dei principi della direttiva generale in materia. Il rischio che potrebbe presentarsi al riguardo è che il Gruppo sia però considerato, anche presso uffici comunitari, alla stregua di un gruppo di lavoro specializzato, anziché un organismo consultivo indipendente.

A causa dell'attuale esiguità della struttura di segretariato, che svolge una funzione di supporto al Gruppo, la predisposizione degli elementi per la discussione e la successiva valutazione delle proposte della Commissione è stata a volte compiuta direttamente dagli uffici della stessa Commissione che avevano chiesto l'avviso del Gruppo. I pareri sono stati, inoltre, talora sollecitati non già in fase di predisposizione di misure comunitarie, bensì a volte dopo la presentazione delle relative proposte al Consiglio.

In proposito, un'iniziativa della Commissione tuttora in corso di elaborazione, sulla quale il Gruppo dei garanti europei ha fornito un parere preliminare, ha riguardato la proposta di una direttiva in materia di protezione dei dati dei lavoratori. Nel settore della protezione dei dati sono inoltre da segnalare le proposte della Commissione relative all'introduzione di modelli per il rilascio di visti e permessi di soggiorno, nonché di passaporti che prevedono l'inserimento obbligatorio di dati biometrici.

In ogni caso, come detto, il ruolo dei garanti europei in ambito comunitario ha acquisito un rilievo più forte.

Il Gruppo, che fino al 16 marzo scorso è stato presieduto dal prof. Rodotà, è stato più volte coinvolto ufficialmente nell'ambito di vari incontri, seminari, audizioni e lavori parlamentari, coordinati dal Parlamento europeo per discutere ed approfondire temi di particolare rilevanza: è quanto avvenuto, ad esempio, in relazione a

numerose proposte volte ad intensificare la creazione di basi di dati a livello europeo e a rendere accessibili, al di là delle previsioni delle singole convenzioni istitutive, i trattamenti di dati effettuati nell'ambito della cooperazione di polizia e giudiziaria.

Alla luce di ciò, potrebbe diventare necessario ridefinire la collocazione istituzionale del Gruppo nel quadro della complessa compagine comunitaria, come pure del suo segretariato. Questo anche in considerazione delle numerose proposte in corso di elaborazione su materie di confine tra il primo ed il terzo pilastro, la cui predisposizione compete ad uffici della Commissione diversi da quelli ai quali è affidata l'attuazione della direttiva n. 95/46/CE (D.g. mercato interno).

Nel corso del 2003, l'attività del Gruppo ha riguardato un'ampia gamma di tematiche, attinenti sia ai diversi ambiti di applicazione delle direttive n. 95/46/CE e n. 2002/58/CE, sia al trasferimento dei dati personali verso Paesi terzi.

Il Gruppo ha dedicato particolare attenzione alle richieste di alcuni Stati (Australia, Canada, Stati Uniti) di ottenere da parte delle compagnie aeree i dati personali dei passeggeri in viaggio da e verso il loro territorio. Tali richieste sono state motivate con la necessità di prevenire il terrorismo e di facilitare i compiti delle autorità doganali. Il Gruppo, nel ribadire l'esigenza di un approccio equilibrato alla lotta contro il terrorismo (v. Pareri n. 10/2001 e n. 6/2002), ha sottolineato la necessità di rispettare e di applicare correttamente anche in tale settore i principi sulla protezione dei dati personali (per maggiori dettagli sul punto, v. *supra*, parag. 36.).

Si ricorda, infine, un primo documento di lavoro (WP 86 del 23 gennaio 2004) sui dispositivi proposti dal consorzio *Trusted Computing Group* per incentivare la sicurezza delle transazioni elettroniche mediante strumenti non solo *software*, ma anche *hardware*.

46.2. La partecipazione ad altri comitati e gruppi di lavoro

Il Gruppo di Berlino

Sempre nell'ambito della definizione delle forme di collaborazione e scambio tra le autorità di protezione dei dati, va ricordata l'attività dell'*International Working Group on data protection in telecommunications* (cd. Gruppo di Berlino), in quanto sede di discussione ed approfondimento, non solo a livello europeo, su temi quali Internet, cifratura e comunicazioni elettroniche, tra esperti in materia di tecnologie ed informazione.

Nella riunione di Berlino del 2-3 settembre 2003 sono stati discussi numerosi temi, fra cui meritano di essere menzionati in particolare il *media privilege*, la *Radio frequency identification* (identificazione attraverso radio frequenze), il tempo di conservazione dei dati di traffico e lo *spamming*.

Con riferimento ai *media*, sono stati analizzati gli esiti dei questionari compilati a livello nazionale e sono state presentate le innovazioni introdotte in materia nella normativa nazionale dal d.lg. n. 196/2003.

È stato inoltre illustrato il contenuto del provvedimento del Garante relativo ai *Multimedia message systems (Mms)*, il quale potrà contribuire all'elaborazione di una dichiarazione che il Gruppo adotterà durante la prossima riunione.

Con riguardo alla *Radio frequency identification*, il Gruppo ha elaborato un documento che è successivamente servito come base per la risoluzione adottata dalle autorità di garanzia riunite a Sydney nel settembre del 2003 (v. *supra*, parag. 44.5.).

I Complaints Handling Workshop

Sono proseguiti gli incontri (cd. seminari in materia di *Complaints Handling*) organizzati ai fini dello scambio di informazioni e della definizione di linee operative comuni per la trattazione delle segnalazioni e dei ricorsi presentati alle autorità nazionali per la protezione dei dati, con particolare riguardo ai casi che, per la loro rilevanza o per la natura delle parti interessate, travalicano l'ambito nazionale.

Ai due incontri, tenutisi rispettivamente a Roma (VIII *Complaints Handling Workshop*, 23-24 ottobre 2003) ed a Stoccolma (IX *Complaints Handling Workshop*, 11-12 marzo 2004), hanno partecipato oltre quarantacinque delegati dei Paesi Ue e di quasi tutti i Paesi in via di adesione all'Unione.

Nel seminario di Roma è stata dedicata specifica attenzione al tema della biometria, con la discussione dei risultati di un questionario presentato dalla delegazione portoghese. Il tema della ricerca farmacologica e delle modalità di prestazione del consenso da parte dei pazienti e/o candidati è stato esaminato in relazione a un questionario predisposto dalla delegazione belga. La delegazione italiana ha impostato la discussione di due casi concreti di bilanciamento di interessi, evidenziando numerose difformità negli approcci seguiti dai singoli Paesi in rapporto, soprattutto, all'esistenza o meno di norme settoriali che indichino già criteri operativi. Sono stati pure presentati gli aggiornamenti relativi all'indagine conoscitiva condotta dal Garante nel 2002 sui meccanismi utilizzati dalle maggiori imprese italiane per trasferire dati personali (di clienti e/o dipendenti) verso Paesi terzi. La discussione ha poi preso in considerazione possibili linee-guida per assicurare che i seminari in materia di *"Complaints Handling"* continuino ad essere focalizzati su casi concreti e su positive modalità operative già in sperimentazione.

Alcuni dei temi affrontati durante l'incontro di Roma sono stati approfonditi in occasione del seminario di Stoccolma, con particolare riguardo alla biometria. Ciascuna delegazione ha, infatti, presentato un caso nazionale emblematico, prospettando le soluzioni volta per volta individuate. La delegazione portoghese ha segnalato l'esistenza di un "decalogo" emanato dall'autorità nazionale di protezione dati per regolamentare l'impiego di dispositivi biometrici ai fini del controllo dell'accesso a locali pubblici e/o privati. Sono state analizzate, inoltre, le strategie seguite dalle varie autorità nazionali per sollecitare l'attenzione dell'opinione pubblica. In particolare, l'autorità svedese e quella del Land di Brandeburgo hanno illustrato l'attività di sensibilizzazione ed educazione svolta rispetto ai cd. incaricati della protezione dei dati, cioè i soggetti che i titolari possono designare ai sensi dell'art. 18(2) della direttiva n. 95/46/CE con il compito, fra l'altro, di tenere un registro dei trattamenti, evitando così l'invio della notificazione all'autorità di controllo. I partecipanti hanno anche esaminato le priorità eventualmente individuate dalle rispettive autorità in relazione alle attività ispettive. Infine, è proseguita la discussione sulla configurazione futura dei seminari e, in particolare, sullo spostamento del nucleo centrale di attività dalla trattazione di casi che coinvolgono più Paesi al confronto su casi concreti affrontati dalle singole autorità. Un documento in merito è stato presentato per la discussione all'*European Spring Conference of Data Protection Commissioners* (Rotterdam, 21-23 aprile 2004).

46.3. EUROPOL: l'attività dell'Autorità comune di controllo e i primi casi di contenzioso

L'Autorità comune di controllo prevista dall'art. 24 della Convenzione Europol ha continuato la sua attività di verifica e controllo sulla gestione degli archivi Europol, che dal luglio 1999 comprendono gli archivi di analisi.

Tale Autorità ha seguito con attenzione i progetti di negoziato sottoposti dal Direttore dell'Europol per ottenere il consenso ad iniziare le trattative volte allo scambio di dati con alcuni Paesi terzi. Sono stati inoltre espressi pareri in merito all'apertura di *file* di analisi e alla nozione di dato personale nel contesto Europol, compresa la possibilità di includervi anche le persone decedute.

L'Autorità comune si è inoltre occupata degli sviluppi applicativi dell'accordo Europol-Stati Uniti per la trasmissione di dati personali a seguito della ristrutturazione del *Department of Homeland Security* ed ha espresso le sue preoccupazioni riguardo ai lavori per la revisione dei sistemi di informazione esistenti nel cd. terzo pilastro, che si svolgono presso il Consiglio dell'Unione europea ed ai quali partecipa il segretariato comune delle autorità comuni di controllo in tale ambito.

Nell'ottobre del 2003 sono stati rinnovati diversi componenti dell'Autorità comune di controllo e del Comitato ricorsi, per scadenza del rispettivo mandato, ed è iniziata un'attività di definizione delle regole per l'accesso agli atti e ai documenti detenuti dall'Autorità comune. Ciò anche in relazione all'apertura di uno specifico sito *web (http://europoljsb.ue.eu.int/home/default.asp?lang=it)* ed alla scelta dei documenti da mettere a disposizione del pubblico (oltre al rapporto di attività e al testo dei pareri adottati, anche informazioni sulla composizione dell'Autorità, sui compiti attribuiti, nonché sul funzionamento del comitato ricorsi).

Una discussione approfondita è stata dedicata alla bozza di accordo predisposta per lo scambio di dati ed informazioni tra Europol ed Eurojust.

Alle riunioni erano presenti, in veste di osservatori, i rappresentanti degli organismi incaricati della protezione dei dati dei Paesi in via di adesione all'Unione europea.

È stata anche svolta l'annuale ispezione alla sede dell'Europol incentrata sugli archivi di analisi e sugli sviluppi tecnologici del sistema, ed è stata effettuata una visita di controllo per verificare il grado di adempimento di Europol alle raccomandazioni impartite a seguito dell'ispezione.

La prima relazione di attività dell'Autorità comune

La prima relazione di attività, riguardante il periodo ottobre 1998-ottobre 2002, è stata ufficialmente presentata dal Presidente agli organi competenti ed è stata resa disponibile nelle diverse versioni linguistiche, sia in formato cartaceo (cfr. l'allegato alla presente Relazione), sia in formato elettronico sul sito *web* dell'Autorità comune.

Va, infine, ricordata la modifica della Convenzione Europol adottata dal Consiglio dei ministri giustizia e affari interni, che amplia il ruolo di Europol rispetto agli specifici scopi conferitigli inizialmente dalla Convenzione.

46.4. Il sistema informativo doganale

Il Sistema informativo automatizzato comune (Sistema informativo doganale-S.i.d.) è stato istituito dalla Convenzione sull'uso dell'informatica nel settore doganale del 26 luglio 1995, elaborata in base all'articolo K3 del Trattato Ue e ratificata dall'Italia con la legge 30 luglio 1998, n. 291.

La Convenzione mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'Ue, specie attraverso lo scambio di dati personali. A tal fine è appunto prevista la creazione del Sistema informativo doganale, che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La Convenzione istituisce, inoltre, un'autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati, che ha iniziato i suoi lavori nel corso della primavera del 2002. Nel periodo in esame l'Autorità ha definito il proprio regolamento interno e i metodi di lavoro. Ha espresso, inoltre, il parere sull'istituzione di un archivio di identificazione dei fascicoli a fini doganali (cd. Fide). Nelle ultime riunioni, l'Autorità comune di controllo si è occupata in particolare di definire gli aspetti relativi all'effettuazione di ispezioni *in loco*.

46.5. Eurodac

A seguito della nomina e costituzione dell'Autorità di controllo indipendente, avvenuta con la decisione del Parlamento e del Consiglio del 22 dicembre 2003, l'Autorità comune di controllo Eurodac per il confronto delle impronte digitali di coloro che richiedono l'asilo ha esaurito le sue funzioni.

La nuova Autorità di controllo su Eurodac

Il controllo su tale sistema informativo, costituito e gestito dalla Commissione, spetterà infatti in via definitiva alla predetta autorità di controllo indipendente prevista dall'art. 286, par. 2, del Trattato di Amsterdam, che ha il compito di controllare la correttezza dei trattamenti di dati effettuati dalle istituzioni e dagli organismi dell'Ue.

La nuova cornice normativa in materia di protezione dati è stata illustrata dai servizi giuridici della Commissione nel corso dell'ultima riunione dell'Autorità comune di controllo, in cui sono state esposte, in particolare, le funzioni e i legami fra i differenti organi di controllo competenti in materia. In tale occasione sono stati pure presentati i regolamenti che stabiliscono i criteri e i meccanismi di determinazione dello Stato membro responsabile dell'esame di una domanda di asilo e le modalità attuative, in particolare il funzionamento della rete DubliNET.

È stato inoltre evidenziato che la banca dati dell'Unità centrale aumenta costantemente di dimensioni, e che vengono alla luce anche doppie e triple "identificazioni positive", ciò che prova la reale utilità del sistema. La Commissione ha sottolineato l'alta qualità dei dati contenuti nella banca dati centrale ed ha evidenziato la necessità di un'analoga qualità in ambito nazionale al momento della raccolta delle impronte digitali inviate ad Eurodac per l'accertamento.

47 L'attività dell'Autorità nell'ambito del Consiglio d'Europa

47.1. I gruppi di esperti

Il Protocollo addizionale alla Convenzione n. 108 del 1981, che prevede l'istituzione di autorità di controllo indipendenti con compiti di verifica e controllo dei trattamenti, e disciplina i flussi transfrontalieri di dati, aperto alla firma l'8 novembre 2001, avendo raggiunto il numero di ratifiche necessario, entrerà in vigore il 1° luglio 2004.

L'Italia è tra i Paesi firmatari, ma non ha ancora presentato in Parlamento il disegno di legge di ratifica.

Per quanto riguarda le modifiche alla ricordata Convenzione n. 108 per consentire alle Comunità europee di aderirvi, l'Italia non ha firmato il relativo Protocollo emendativo. Essendo necessaria l'accettazione degli emendamenti da parte di tutti i Paesi dell'Unione europea, tali modifiche non sono quindi ancora entrate in vigore.

Nel quadro dell'attività del Consiglio d'Europa meritano di essere menzionati i lavori dei cd. gruppi di esperti: il Comitato CJ-PD, nato nell'ambito del Comitato per la cooperazione giudiziaria e soppresso a seguito del processo di razionalizzazione delle risorse utilizzabili, è riuscito comunque, nel corso della sua ultima riunione, svoltasi nel dicembre 2003, a portare a compimento i lavori sulle linee guida per l'uso delle carte intelligenti *(smart card)*.

Il Comitato T-PD

Il Comitato T-PD cd. convenzionale, in quanto costituito direttamente dalla Convenzione n. 108 e quindi non sopprimibile per decisione amministrativa, nell'unica riunione plenaria svoltasi anch'essa nel mese di dicembre 2003, si è trovato a valutare le problematiche derivanti dalla soppressione del CJ-PD e, in particolare, le modalità di prosecuzione dei lavori sul trattamento di dati biometrici, che il CJ-PD non ha potuto completare.

Proprio a causa dell'inserimento nei suoi lavori delle problematiche legate alla biometria, il TP-D ha poi dovuto rivedere le priorità stabilite per il 2003 e per il 2004, programmando un approfondimento sui seguenti temi:

- l'applicazione dei principi della Convenzione in relazione agli sviluppi tecnologici. Il Comitato si propone così di esaminare meglio, alla luce della Convenzione, come un indirizzo di posta elettronica o il numero di un telefono cellulare sia da considerare "dato personale". Intende inoltre valutare i rischi che derivano dalla diffusione di nuove tecnologie (molteplicità dei fini, conservazione dei dati da parte dei "nuovi media") come pure le opportunità che ne possono discendere in merito alla protezione dei dati personali (PETs, tecnologie non invasive, ecc);

- l'applicazione dei principi di protezione dei dati ad Internet, in relazione ai quali il TP-D ha preparato un progetto di mandato per uno studio preliminare da far effettuare ad un consulente.

48 Altre iniziative in ambito internazionale: Ocse

Nel periodo di riferimento il Garante ha continuato a seguire i lavori del *Working Party on Information Security and Privacy (Wpisp)* dell'Ocse, sottogruppo del *Committee for Information Computer and Communication Policy (Iccp)*.

Fra i problemi di maggior rilievo affrontati negli incontri svoltisi nel 2003 in relazione al trattamento dei dati personali, si debbono ricordare l'attuazione delle linee-guida sulla sicurezza, lo *spamming*, la biometria, e la creazione di un apposito gruppo che si occuperà di sicurezza nei viaggi internazionali *(travel security)*, gruppo a cui parteciperà questa Autorità. Le conclusioni raggiunte in sede Ocse su tali temi sono già state esposte in appositi paragrafi della *Relazione*, ai quali pertanto si rinvia per un'analisi dettagliata (v. parag. 41.1. e 41.2.).

49 Il sistema di informazione Schengen (Sis)

Nel corso dell'anno sono state sottoposte al Garante, quale autorità di controllo sulla sezione nazionale del Sistema informativo Schengen (Sis), numerose richieste di verifica in merito all'eventuale o corretta registrazione, negli archivi del Sis, di dati personali dei soggetti interessati ed alla liceità dei relativi trattamenti. Si tratta, in gran parte, di domande che attengono al diniego di visto, per lo più adottato a causa di segnalazioni, ai fini della non ammissione nella cd. area Schengen, di persone nei cui confronti sono stati emessi provvedimenti amministrativi sfavorevoli in materia di ingresso e soggiorno (espulsione, respingimento alla frontiera).

Si è registrato anche quest'anno un notevole incremento delle richieste pervenute, da attribuire pure alla procedura di regolarizzazione di cittadini extracomunitari introdotta dalla legge n. 189/2002; le richieste provengono soprattutto da Paesi dell'Est europeo e, in particolare, dalla Romania.

Nell'arco temporale che va dal 1° gennaio 2003 al 31 marzo 2004 le richieste sono state 480, di cui 464 già definite.

Per svolgere al meglio i propri compiti e fronteggiare più rapidamente anche le domande di chiarimenti sulla normativa di riferimento, nel febbraio 2003 il Garante ha nuovamente riassunto l'esatto ambito delle proprie competenze: ha così precisato che gli interessati possono rivolgere a questa Autorità richieste di verifica dei dati che li riguardano inseriti nel Sis, ovvero di aggiornamento, di rettifica o di cancellazione dei medesimi dati. Al Garante, invece, non sono conferiti compiti di adozione, revoca o controllo dei provvedimenti amministrativi che sono alla base delle segnalazioni contenute nel Sis.

Per rimediare poi a problemi insorti nei casi in cui erano state segnalate usurpazioni d'identità o omonimie, è stata ulteriormente sperimentata nel 2003, in colla-

borazione con il Dipartimento della pubblica sicurezza, una procedura di comparazione degli elementi identificativi della persona oggetto di usurpazione d'identità con quelli, anche dattiloscopici, della persona effettivamente segnalata nel Sis.

Sempre allo scopo di rilevare più agevolmente i casi di omonimia, è stata poi rafforzata la collaborazione con il Centro visti del Ministero degli affari esteri e con le divisioni Sirene ed N.Sis del Dipartimento della pubblica sicurezza.

La nuova disciplina di accesso al Sis

Su tale quadro complessivo si sono innestate, con effetto dal 1° gennaio 2004, le modifiche introdotte dal Codice circa le modalità di esercizio del diritto di accesso al Sis e degli altri diritti connessi (rettifica, integrazione o cancellazione), che possono essere ora esercitati direttamente nei confronti dell'autorità di polizia (cd. accesso diretto) e non più solo per il tramite del Garante (cd. accesso indiretto).

Il d.lg. n. 196/2003 ha infatti modificato la legge n. 388/1993, lasciando sostanzialmente inalterato il sistema dei controlli del Garante attribuiti all'Autorità dalla Convenzione e dalla legge n. 675/1996 (ora, artt. 53, 154, comma 2, lett. *a)*, e 160 d.lg. n. 196/2003), ma disciplinando in maniera innovativa il diritto dell'interessato di conoscere l'esistenza nel Sis di una segnalazione che lo riguarda ed i dati detenuti, nonché di ottenerne l'eventuale aggiornamento, rettifica o cancellazione (art. 173 d.lg. n. 196/2003).

In base alla nuova disciplina l'interessato ha il diritto di ottenere in tempi rapidi una risposta direttamente dall'autorità che ha la competenza centrale per la sezione nazionale del SIS, ai sensi dell'art. 108 della Convenzione, che in Italia è il Dipartimento della pubblica sicurezza, anziché per il tramite del Garante. Se necessario, all'esito di un intempestivo, mancato o inidoneo riscontro alla richiesta formulata al Dipartimento, l'interessato può proporre una segnalazione o un reclamo al Garante.

La scelta operata dal Codice è in linea con quella effettuata da gran parte dei Paesi dell'area Schengen ed introduce una procedura analoga a quella prevista per l'accesso diretto ai dati inseriti nel Centro elaborazione dati del Dipartimento della pubblica sicurezza.

L'Autorità ha richiamato l'attenzione del Ministero dell'interno sulla necessità di assumere ogni iniziativa utile ad assicurare a quanti richiedono l'accesso un riscontro idoneo e tempestivo, anche in relazione alla possibilità per l'interessato, confermata dal Codice, di richiedere, sulla base dei dati conosciuti, un'ulteriore tutela dei propri diritti rispetto all'aggiornamento, rettifica, o cancellazione dei dati, anche in sede giudiziaria (art. 11, comma 2, legge n. 388/1993 e art. 10, comma 5, legge n. 121/1981).

A tal riguardo il Garante ha pure indicato l'opportunità di alcuni accorgimenti per l'inoltro delle richieste e il loro riscontro, che possono risultare vantaggiosi per le stesse persone interessate.

Il Garante ha infine richiamato l'attenzione dell'Ufficio visti del Ministero degli affari esteri sulla necessità di sensibilizzare efficacemente in materia le ambasciate e le cancellerie consolari nei Paesi interessati, anche attraverso il ricorso a moduli prestampati o ad apposite diciture che orientino quanti richiedono il visto sulle modalità di esercizio del diritto di verifica delle segnalazioni esistenti nel Sis.

50 La trattazione dei ricorsi

50.1. Il ricorso come strumento diffuso di tutela

La crescita progressiva del numero dei formali ricorsi pervenuti al Garante, che già era stata registrata nelle relazioni degli ultimi anni, ha trovato conferma nel 2003, anno nel quale si può parlare addirittura di una vera e propria esplosione dell'utilizzo di questo strumento di tutela, come dimostrato dalle statistiche.

Mentre nel 2001 le decisioni sui ricorsi sono state 169, nel 2002 sono stati esaminati 390 ricorsi, per arrivare ai 608 ricorsi decisi nell'anno solare 2003 (per il periodo di riferimento 1° gennaio 2003-31 marzo 2004 il numero totale dei ricorsi decisi è 775). Un esame più approfondito del contenuto dei ricorsi dimostra che ormai, grazie anche all'attenzione che molte decisioni hanno ottenuto sulla stampa, così come nella letteratura specializzata, questo strumento di tutela è entrato nella coscienza sociale e costituisce parte del bagaglio professionale degli operatori forensi.

Varie sono le ragioni di questo incremento: la celerità della procedura, i costi contenuti, la possibilità per gli interessati di tutelare i propri diritti senza obbligo di assistenza da parte di un legale, ma soprattutto l'estrema duttilità dello strumento del ricorso che ha dimostrato di poter essere applicato ai campi più diversi. Ciò vale in particolare per il diritto di accesso ai dati personali, che trova ormai larga e comune applicazione ai settori più disparati (pubblica amministrazione, ambito sanitario, settori assicurativo, finanziario e creditizio, trattamenti connessi alla gestione del rapporto di lavoro, ecc.).

Le opposizioni ai provvedimenti del Garante

Per quanto concerne, invece, le opposizioni proposte contro le decisioni assunte dall'Autorità nell'anno trascorso, ne sono state proposte in numero estremamente contenuto, e comunque, sono state in larghissima parte rigettate dai tribunali o contraddette da una successiva giurisprudenza.

La competenza territoriale

Sul piano della corretta instaurazione del contraddittorio, merita di essere segnalata la decisione del Tribunale di Firenze (depositata in cancelleria il 15 aprile 2003), con la quale è stata accolta l'eccezione di incompetenza territoriale sollevata dall'Autorità, confermandosi il principio secondo cui, avverso i provvedimenti espressi del Garante sui ricorsi, nonché nelle ipotesi di rigetto tacito, il titolare o l'interessato possono proporre opposizione al tribunale del luogo ove risiede il titolare del trattamento (art. 29, comma 6, legge n. 675/1996; ora, artt. 151 e 152, d.lg. n. 196/2003).

Analoga eccezione, sollevata sotto altro profilo dall'Autorità in un giudizio instaurato dinanzi al Giudice di pace di Amantea con opposizione ad ordinanza di applicazione di sanzione amministrativa, è stata accolta dall'adito giudice che si è pertanto dichiarato incompetente.

Dati contenuti nelle perizie medico-legali

Altra significativa questione definita in sede di impugnativa davanti al giudice ordinario di una decisione del Garante su un ricorso (al termine, peraltro, di un complesso *iter* processuale), è stata quella della riconducibilità delle valutazioni espresse nelle perizie medico-legali alla nozione di dato personale (Tribunale di Roma, sentenza 17 luglio 2003). Allineandosi agli orientamenti espressi in alcune altre sedi giudiziarie e conformi a quelli enunciati dal Garante in più occasioni

(cfr. *supra,* parag. 7.9.), l'adito giudice si è discostato da alcuni circoscritti precedenti ed ha affermato che anche i giudizi valutativi devono considerarsi dati personali, in quanto, riferendosi ad un persona determinata, sono dotati di un'efficacia informativa tale da fornire un elemento aggiuntivo di conoscenza rispetto all'interessato. Una questione di legittimità costituzionale delle disposizioni relative alla nozione di dato personale e al diritto di accesso, sollevata con riferimento agli artt. 2 e 21 della Costituzione, è stata dichiarata quindi manifestamente infondata.

Si è pertanto riconosciuto che anche rispetto ai "dati valutativi" l'interessato può esercitare il diritto di accesso e alcuni altri diritti previsti dalla normativa in materia di protezione dei dati personali, ad esclusione dei diritti di rettificazione o integrazione (in tal senso dispone ora, come già detto, l'art. 8, comma 4, del Codice).

Gradi del giudizio di opposizione

Con la medesima pronuncia il tribunale ha inoltre ritenuto manifestamente infondata l'eccezione di costituzionalità delle disposizioni che disciplinano l'opposizione ai provvedimenti dell'Autorità, sollevata in relazione alla riconosciuta natura di rimedio non giurisdizionale (Cass. civ. 20 maggio 2002, n. 7341) del ricorso al Garante ai sensi dell'art. 29 della legge n. 675/1996 (ora, art. 145 del Codice). Da tale natura la giurisprudenza ha fatto derivare, infatti, la legittimazione di questa Autorità ad essere parte nei giudizi instaurati a seguito di opposizione ad un suo provvedimento. Di qui la proposizione, nella vicenda in esame, della questione di costituzionalità, per asserita violazione della regola del giusto processo, in quanto la possibilità di impugnare la decisione del giudice di primo grado sull'opposizione al provvedimento del Garante solo tramite ricorso per Cassazione sarebbe stata in contrasto con la regola del doppio grado di giudizio.

Nel respingere tale questione, il tribunale ha riconosciuto che ragioni di speditezza possono giustificare l'esistenza di procedimenti giurisdizionali semplificati in cui è previsto un unico sindacato di merito, in quanto nella Costituzione non è contenuta alcuna norma che garantisca espressamente il doppio grado di giudizio.

Va infine ricordata, sebbene non sia stata proposta avverso una decisione su ricorso, l'impugnazione del provvedimento del Garante del 19 marzo 2003 concernente la pubblicazione di foto segnaletiche. Di tale impugnazione, accolta dal Tribunale di Milano, si è già parlato in altra parte di questa *Relazione* (cfr. *supra*, parag. 15.2.). Qui occorre sottolineare che, nel relativo decreto, l'adito tribunale ha invece rigettato l'eccezione dei ricorrenti nella parte in cui lamentavano di non esser stati sentiti da questa Autorità prima dell'emissione del provvedimento, ritenendo infondata al riguardo ogni doglianza di costituzionalità. Secondo il tribunale, infatti, in certe situazioni possono essere necessari interventi immediati del Garante, salva la possibilità di contestarli e di ottenerne se del caso la sospensione degli effetti. Inoltre, sono state ritenute inapplicabili in via analogica all'intervento d'ufficio dell'Autorità le regole procedurali da osservare in sede di ricorso al Garante di cui all'art. 29 della legge n. 675/1996 (ora, art. 149 del Codice).

50.2. Le novità introdotte dal Codice in materia di protezione dei dati personali

Il d.lg. n. 196/2003 è intervenuto anche sulle disposizioni relative ai ricorsi, che sono ora contenute negli artt. 145 e s. del Codice.

Alla luce dell'esperienza maturata nei primi quattro anni di vigenza delle disposizioni attuative in materia di ricorsi, sono state apportate alcune importanti modifiche riguardanti, essenzialmente, l'ampliamento dei termini di durata del relativo procedimento, in funzione di prevenzione del contenzioso.

Anzitutto, l'art. 146 ha portato a quindici giorni (aumentabili fino a trenta in caso di riscontro di particolare complessità) il termine a disposizione del titolare o del responsabile per rispondere all'interpello preventivo che l'interessato deve necessariamente formulare prima di poter presentare il ricorso.

La modifica mira a consentire al titolare e al responsabile del trattamento di poter riscontrare adeguatamente le richieste di accesso ai dati personali presentate dall'interessato; ciò anche tenuto conto che le richieste riguardano a volte una complessa serie di dati, non sempre riportati, come pure sarebbe dovuto, su documenti o supporti prontamente reperibili per l'estrazione di tutte le informazioni rilevanti.

Il termine in precedenza fissato indirettamente in cinque giorni non agevolava in questi casi un riscontro tempestivo o adeguato e favoriva talora la presentazione del ricorso.

L'art. 150, comma 2, ha anche fissato in sessanta giorni il termine per la decisione sul ricorso: tale ampio spazio temporale a disposizione delle parti e dell'Autorità permette di articolare meglio, quando è necessario, gli accertamenti istruttori e consente di dare quindi maggiore effettività al principio del contraddittorio.

In questo quadro si colloca pure la nuova possibilità per l'Autorità di disporre una proroga fino a quaranta giorni dei termini per la decisione sul ricorso, non subordinata, come la più breve proroga prevista in precedenza, all'assenso di entrambe le parti.

Il Codice è poi intervenuto su due profili procedurali che avevano dato luogo ad alcuni problemi interpretativi.

È stata in questo quadro confermata la necessità dell'autenticazione della sottoscrizione apposta dal ricorrente in calce al ricorso, superando, con l'esplicita indicazione contenuta nell'art. 147, comma 4, le perplessità insorte in alcuni circa la compatibilità di tale obbligo con la disciplina in tema di autocertificazione.

Un'altra precisazione utile è venuta infine dal comma 6 dell'art. 150 del Codice il quale, in riferimento all'eventuale pronuncia sulle spese del procedimento, ha stabilito che la decisione del Garante costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 c.p.c.; resta invece ferma l'inammissibilità della proposizione innanzi a questa Autorità delle richieste di risarcimento dei danni.

50.3. Brevi cenni sulla casistica

Per sottolineare l'ampio spettro di questioni affrontate dal Garante in sede di decisione sul ricorso, è utile un cenno sommario ai settori in cui si è avuta la proposizione del maggior numero di ricorsi, rinviando comunque, per una trattazione più analitica delle relative problematiche, alle specifiche sezioni di questa Relazione.

Settore bancario e finanziario

Trattamenti svolti in ambito bancario e finanziario. A partire dalla seconda metà del 2003 in questo settore si è indirizzato il maggior numero di ricorsi, che si sono incentrati soprattutto sull'accesso degli interessati ai dati personali detenuti dagli istituti di credito o dalle società finanziarie. È importante notare come delicate vicende che hanno interessato il mondo finanziario nell'ultimo anno (i casi Cirio e Parmalat e la vicenda dei *bond* argentini) abbiano trovato immediata eco dinanzi all'Autorità, in conseguenza della presentazione di numerose richieste di accesso, mirate a conoscere l'insieme dei dati personali trattati nelle operazioni finanziarie in questione (profili di rischio, logica e modalità del trattamento, ecc.).

"Centrali rischi"

Trattamenti svolti dalle cd. centrali rischi private. È, questo, uno dei settori dove si riscontra una maggiore attenzione da parte dell'opinione pubblica, anche in conseguenza del forte impatto che ha avuto il provvedimento generale del Garante intervenuto in materia (*Provv.* 31 luglio 2002). Sono stati infatti proposti molti nuovi ricorsi in cui se ne lamentava l'inosservanza, chiedendo l'applicazione dei principi in esso affermati, con particolare riguardo ai tempi di conservazione dei dati.

Sono emersi peraltro, anche profili ulteriori, quali il problema della conservazione nelle banche dati delle "centrali rischi" private di dati concernenti le cd. segnalazioni positive o gli effetti della revoca del consenso al trattamento dei dati espressa dall'interessato nell'interpello o direttamente nell'ambito del ricorso (v., tra i tanti, *Provv.* 22 dicembre 2003).

Comunicazioni elettroniche e telefonia

Trattamenti di dati da parte di operatori di telecomunicazioni e problematiche relative ai trattamenti in rete. Il settore ha visto pervenire un numero elevato di ricorsi, anche in conseguenza di importanti decisioni dell'Autorità che hanno richiamato l'attenzione sulle garanzie in materia. Ciò con particolare riguardo all'invio di messaggi promozionali indesiderati e non sollecitati ad indirizzi di posta elettronica (cd. *spamming*), tenuto oltretutto conto che gli indirizzi di posta elettronica sono spesso acquisiti tramite rastrellamento in rete a mezzo di appositi *software.*

Peraltro, l'Autorità ha talora dichiarato inammissibili alcuni ricorsi in quanto formulati da soggetti non legittimati a proporli, trattandosi di persone diverse da quelle cui si riferivano i dati concernenti gli indirizzi di posta elettronica dei quali era lamentato l'illecito trattamento.

In materia di telefonia fissa e mobile, i casi più frequenti di ricorso hanno riguardato le richieste di accesso ai dati relativi al traffico in entrata e in uscita e le opposizioni al trattamento consistente nell'invio di comunicazioni promozionali e pubblicitarie (anche a mezzo di *sms*) in assenza di consenso dell'interessato. Con riferimento alla telefonia fissa, alcuni casi hanno riguardato anche l'opposizione alla divulgazione, da parte del gestore, di numeri telefonici per i quali era stato richiesto il carattere di numero riservato.

Ambito assicurativo

Dati conservati nelle perizie medico legali in ambito assicurativo. L'argomento, esaminato dal Garante fin dal 1999 ed oggetto anche di significative pronunce giurisprudenziali, si è riproposto in misura più contenuta rispetto agli anni precedenti. Nei casi esaminati l'Autorità è stata chiamata più volte a decidere sull'applicabilità della disposizione che, a certe condizioni, consente di differire l'esercizio del diritto di accesso in caso di pregiudizio all'esercizio del diritto di difesa del titolare del trattamento. Una riduzione del contenzioso al riguardo è probabilmente derivata pure dalla più moti-

vata e condivisibile giurisprudenza alla quale si è fatto riferimento poc'anzi (cfr. *supra*, parag. 50.1.), e dalle precise scelte operate dal Codice, cui ha fatto rinvio il d.m. 20 febbraio 2004, n. 74 sull'accesso agli atti delle imprese assicurative.

Trattamenti effettuati dalle pubbliche amministrazioni. I ricorsi proposti nei confronti delle pubbliche amministrazioni coprono una serie molto vasta e differenziata di ipotesi di trattamento dei dati, che sono già state ampiamente analizzate nei capitoli II e IV. In questa sede merita comunque di essere ricordato che in tale settore hanno assunto specifico rilievo alcune opposizioni formulate dagli interessati.

51 Attività ispettive e applicazione di sanzioni amministrative

51.1. Profili generali – Tipologia degli accertamenti ispettivi e criteri adottati

L'art. 154 del Codice consolida, in capo al Garante, il compito di controllare se i trattamenti siano effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione. A tal fine, l'Autorità continua ad esercitare anche una funzione ispettiva per mezzo del Dipartimento vigilanza e controllo, il cui personale riveste, nell'esercizio dei poteri attribuiti dalla legge, la qualifica di ufficiale/agente di polizia giudiziaria.

Le attività ispettive sono costituite anzitutto da accertamenti effettuati nei luoghi dove si svolgono i trattamenti, utilizzando i poteri previsti dal Codice (artt. 157–160).

In generale, le ispezioni possono essere originate da segnalazioni o reclami ricevuti dall'Autorità, da esigenze di approfondimento emerse nell'ambito dell'esame di ricorsi, d'iniziativa dell'Autorità in relazione, ad esempio, alle verifiche degli adempimenti da parte di determinate categorie di titolari o, ancora, sulla base di notizie comunque acquisite direttamente dal Garante.

Anche nella vigenza del Codice, l'esercizio dell'attività di controllo resta informato ai principi di proporzionalità, adeguatezza e gradualità, tenendo presente, di volta in volta, il contesto operativo di riferimento (rischio di dispersione o di alterazione degli elementi di prova) e la disponibilità o meno del soggetto controllato ad una collaborazione per lo svolgimento delle verifiche.

I controlli possono essere effettuati pure mediante richieste, sul posto o meno, di informazioni o di esibizione di documenti; possono inoltre svolgersi anche mediante accessi a banche di dati o altre ispezioni e verifiche nei luoghi dove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo stesso.

Ispezioni

Le ispezioni previste dall'art. 158 del Codice sono disposte quando, per acquisire gli elementi necessari alla definizione della vicenda, non sia idonea una mera richiesta di informazioni o di esibizione di documenti, nonché nei casi in cui non siano state fornite tempestivamente le informazioni o i documenti richiesti (o, se pervenuti, siano incompleti o non veritieri).

Si tratta di una potestà con caratteri inquisitori e i soggetti interessati agli accertamenti sono quindi tenuti a farli eseguire: l'accertamento è infatti eseguito anche in caso di rifiuto e in tale ultima ipotesi le eventuali spese sono poste a carico del titolare. Durante l'accertamento il titolare o il responsabile possono farsi assistere da persone di loro fiducia.

Autorizzazione dell'a.g.

L'autorizzazione da parte dell'autorità giudiziaria, diversamente da quanto stabilito dalla previgente disciplina, che contemplava in ogni caso tale autorizzazione, è oggi opportunamente richiesta dal Codice solo nel caso di accessi "svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze" (art. 158 cit.).

All'autorizzazione è equiparato l'assenso informato, che viene anche documentato per iscritto (cfr. *Provv.* n. 2 del 30 gennaio 2001).

Le attività effettuate durante l'ispezione sono riportate in un sommario verbale, nel quale sono registrati tutti gli elementi rilevanti occorsi durante le operazioni e menzionate le informazioni e la documentazione eventualmente acquisita.

Esiti del procedimento ispettivo

Nel corso o al termine del procedimento nel cui ambito vengono svolte le ispezioni, l'Autorità:

- prescrive ai titolari o responsabili del trattamento dei dati le modificazioni necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti (la disciplina previgente contemplava un potere analogo in forma di segnalazione);

- adotta ove necessario uno dei provvedimenti di divieto o blocco del trattamento (v. artt. 143, 144 e 154 del Codice);

- contesta le violazioni amministrative eventualmente constatate;

- nei casi più gravi previsti dalla legge, procede alla comunicazione di notizia di reato all'autorità giudiziaria per l'accertamento delle violazioni costituenti reato.

51.2. La collaborazione con gli organi dello Stato

Nello svolgimento dell'attività ispettiva, il Garante può avvalersi della collaborazione di altri organi dello Stato. Già da tempo si sono avute molteplici occasioni di collaborazione con le forze di polizia ed in particolare con la Guardia di finanza, in ragione delle peculiari competenze di quest'ultima nel campo delle attività di controllo in ambito amministrativo.

Collaborazione con la Guardia di finanza

Nell'ottica del potenziamento dell'attività di vigilanza e controllo, pertanto, nel mese di ottobre 2002 il Garante e la Guardia di finanza hanno siglato un protocollo d'intesa in base al quale è stata potenziata l'attività di collaborazione tra le due istituzioni (cfr. *Relazione 2002*, p. 145).

Successivamente al perfezionamento del protocollo di intesa, nel mese di gennaio del 2003 è stata effettuata un'intensa attività di formazione del personale del Corpo destinato a svolgere in via continuativa l'attività di collaborazione (venti unità circa

tra ufficiali, ispettori e sovrintendenti). Ciò ha consentito di avviare più rapidamente la collaborazione con la Guardia di finanza, che si è dimostrata estremamente proficua sia nella fase preparatoria degli interventi più delicati, grazie alle capacità investigative proprie del Corpo, sia nella fase realizzativa. Sono stati eseguiti, in particolare, 33 interventi, di cui 7 congiuntamente a personale dell'Autorità.

La collaborazione ha investito anche gli sviluppi investigativi dei casi oggetto di segnalazione all'autorità giudiziaria, i quali hanno comportato, nel 2003, l'esecuzione di 177 sommarie informazioni testimoniali, la ricezione di 12 querele e la segnalazione di 5 persone all'autorità giudiziaria.

I risultati raggiunti e l'esigenza di rispondere in maniera sempre più adeguata alle istanze di tutela provenienti da cittadini hanno indotto l'Autorità a chiedere per il 2004 un ulteriore rafforzamento del rapporto di collaborazione con la Guardia di finanza, allo scopo di potersi avvalere anche di personale, adeguatamente formato, in ogni regione.

Assai significative sono risultate pure le collaborazioni con la Polizia di Stato (specie per accertamenti nelle reti telematiche) e l'Arma dei carabinieri.

La collaborazione con le forze di polizia si è quindi confermata come un elemento essenziale di incremento dell'efficacia dell'azione di tutela dei diritti dei cittadini, che passa anche attraverso una più intensa attività di vigilanza e controllo.

51.3. I casi più significativi

Attivazione di schede telefoniche

Un caso rilevante tra quelli emersi ha portato alla segnalazione all'autorità giudiziaria dell'illecito trattamento di dati personali connesso all'attivazione di carte telefoniche effettuato da una società che gestisce numerosi punti vendita, situati nell'Italia centrale.

L'attività di accertamento dell'Autorità è partita dalla segnalazione di una persona che, dopo aver acquistato una scheda telefonica ricaricabile, era venuta casualmente a conoscenza di essere intestataria di altre sei utenze attivate a suo nome presso il medesimo esercizio commerciale.

L'attenzione del Garante si è concentrata quindi sulle attivazioni di schede telefoniche da parte di tali punti vendita, e in particolare sulle modalità e sulle finalità del trattamento dei dati personali forniti dai clienti.

Dalle ispezioni presso la sede della società, nonché da riscontri incrociati con i dati in possesso della società telefonica, è emerso che, nel solo breve periodo esaminato, presso i punti vendita erano state attivate quasi 800 schede telefoniche ricaricabili nei confronti di circa 200 persone, a loro insaputa. Tale prassi illecita è stata seguita nel quadro dei "piani di incentivazione per i rivenditori" che prevedevano, al superamento di determinate soglie di attivazioni prestabilite, il riconoscimento ai rivenditori stessi di un ulteriore compenso per ogni attivazione effettuata in più rispetto a quanto programmato. La società sarebbe pertanto riuscita a lucrare, pur nel solo breve periodo preso in esame, premi per oltre quarantamila euro.

Gli interessati avevano spesso acquistato una prima scheda telefonica presso uno degli esercizi della società ed erano ignari di essere intestatari di altre schede, utilizzabili in vari modi, anche illeciti. I dati personali erano stati ovviamente trattati senza il loro consenso espresso.

La vicenda, sulla quale l'autorità giudiziaria competente ha effettuato poi ulteriori accertamenti, si lega ad un'analoga indagine svolta dalla Guardia di finanza di Rovigo sotto la direzione della locale procura della Repubblica, i cui esiti sono stati comunicati al Garante. Dalla stessa emerge che, almeno in un certo periodo di tempo, rivenditori poco scrupolosi hanno adottato comportamenti lesivi dei diritti di molte persone, a nome delle quali sono state attivate migliaia di carte telefoniche.

Spamming

Un altro dei settori rilevanti dell'attività ispettiva del Garante è quello relativo al cd. *spamming*.

In uno degli accertamenti effettuati in tale settore è stato denunciato alla magistratura il titolare di un'impresa operante nel campo delle arti grafiche.

Alcuni cittadini avevano presentato ricorso al Garante lamentando di essere stati raggiunti da *e-mail* commerciali inviate dal titolare della tipografia senza il previo consenso informato dei destinatari. Nell'accogliere tutti i ricorsi pervenuti, il Garante ha ordinato al titolare dell'impresa di cancellare i nominativi dei ricorrenti e ha disposto il blocco dei dati personali trattati illecitamente, per prevenire ulteriori possibili violazioni della legge. L'Autorità ha poi disposto che l'impresa fornisse informazioni sull'origine dei dati, sull'avvenuta cessazione degli illeciti e sui nominativi dei responsabili del trattamento eventualmente designati.

Acquisiti elementi che dimostravano la continuazione dei comportamenti illeciti da parte del titolare del trattamento successivamente alla notifica del blocco, l'Autorità ha comunicato alla competente procura della Repubblica la notizia di reato in relazione all'inosservanza alle prescrizioni del Garante e all'illecito trattamento dei dati personali.

Servizi di e-banking

Un ulteriore settore di intervento ha riguardato le misure di sicurezza delle banche dati, con particolare riguardo ai servizi di *e-banking*. Tali servizi consentono a ogni cliente abilitato, previo inserimento di codici di autenticazione, di consultare via Internet i movimenti del proprio conto corrente e di visualizzare i dati che lo riguardano e gli estratti conto, creando un prospetto delle ultime operazioni effettuate da memorizzare o stampare.

Il Garante si è attivato a seguito del ricorso di un cliente di una banca *on line* che, nel consultare via Internet la propria posizione contabile, aveva avuto accidentalmente accesso ad informazioni riservate di altri correntisti ignari. Il caso, che ha assunto un notevole interesse per i suoi riflessi sul rapporto dei clienti con la banca, è stato già analizzato in altra parte di questa Relazione (cfr. *supra*, parag. 11.). Qui occorre solo puntualizzare che il Garante ha inoltrato denuncia alla magistratura ordinando contestualmente, con apposito provvedimento, di adottare adeguate misure di sicurezza per prevenire il ripetersi di tali illeciti. L'adempimento di tale prescrizione ha consentito alla banca di beneficiare dell'ammissione al pagamento di una ammenda con conseguente possibilità di beneficiare dell'estinzione del reato, così come previsto dal Codice (art. 169).

51.4. Riferimenti statistici

Grazie all'apporto fornito anche dalla collaborazione con la Guardia di finanza, l'attività ispettiva effettuata nel periodo fino al 31 marzo 2004 ha avuto un incremento significativo rispetto a quella svolta nel precedente periodo di riferimento.

Nell'ambito delle centinaia di procedimenti di controllo avviati dall'Autorità, 69 sono stati svolti anche mediante necessari accertamenti ispettivi *in loco*.

Le attività ispettive sono state avviate sulla base di:
- segnalazioni pervenute all'Ufficio (45%);
- autonomi accertamenti a seguito di ricorsi presentati al Garante (36%);
- accertamenti avviati di iniziativa (19%).

Gli accertamenti eseguiti hanno riguardato in prevalenza verifiche concernenti:
- le modalità di acquisizione del consenso, in molti casi connesse ad attività effettuate sulla rete Internet mediante l'invio di sollecitazioni commerciali non richieste via *e-mail*;
- il rispetto delle disposizioni di legge in relazione al trattamento di dati mediante sistemi di videosorveglianza;
- l'accertamento dell'origine dei dati oggetto di trattamento;
- le misure di sicurezza.

Le ispezioni sono state effettuate:
- in 61 casi mediante richieste di informazioni ed esibizione di documenti, formulate sul posto;
- in 8 casi mediante accessi a banche dati.

Con riferimento all'ambito territoriale la ripartizione è stata:
- nord (41%);
- centro (43%);
- sud (16%).

L'incidenza delle violazioni penali sui procedimenti amministrativi di controllo avviati è pari circa al 16%. Le violazioni segnalate riguardano ipotesi di trattamento illecito di dati personali, omessa adozione di misure di sicurezza, inosservanza dei provvedimenti del Garante e false dichiarazioni al Garante.

In generale le ispezioni hanno consentito di rilevare che nel settore privato le aziende più grandi stanno assumendo specifiche iniziative per adeguarsi alla normativa e agli indirizzi dell'Autorità, anche attraverso la costituzione di unità organizzative con deleghe specifiche e veri e propri "uffici *privacy*", mentre le aziende medio-piccole dimostrano un livello inferiore di adeguamento.

Nella pubblica amministrazione stenta di più ad affermarsi una vera e propria cultura della *privacy* applicata ai processi di lavoro e alla gestione delle pratiche di ufficio. Talvolta, ad un assetto formalmente corretto non corrisponde una piena consapevolezza dei doveri e delle responsabilità connesse al trattamento dei dati personali. Alcune delle attività ispettive hanno rivelato ancora preoccupanti fenomeni di superficialità nel trattamento dei dati, soprattutto per quanto riguarda la gestione degli archivi e le connesse misure di sicurezza.

Si è pure rilevata, nelle amministrazioni pubbliche, la frequente mancanza di articolazioni dedicate all'attuazione della normativa, dotate di autonomie decisionali e gestionali indispensabili per tradurre in pratica i programmi formalmente delineati.

51.5. L'attività sanzionatoria del Garante

Anche nel settore delle sanzioni amministrative il Codice in materia di protezione di dati personali ha introdotto novità di assoluto rilievo.

Le novità introdotte dal Codice

In modo significativo, il d.lg. n. 196/2003 inserisce nella Parte III, "Tutela dell'interessato e sanzioni" un apposito titolo dedicato alle "Sanzioni", a sua volta suddiviso nel Capo I ("Violazioni amministrative") e nel Capo II ("Illeciti penali", distinguibili in delitti e contravvenzioni).

Le violazioni amministrative previste dal Codice sono: 1) omessa o inidonea informativa all'interessato (art. 161); 2) cessione dei dati in violazione dell'art. 16, comma 2, o di altre disposizioni in materia di disciplina dei dati personali (art. 162, comma 1); 3) violazioni delle disposizioni in tema di comunicazione dei dati personali idonei a rivelare lo stato di salute, di cui all'art. 84, comma 1 (art. 162, comma 2); 4) omessa o incompleta notificazione del trattamento (art. 163); 5) omessa informazione ed esibizione di documenti al Garante (art. 164).

La nuova normativa mostra così di voler rafforzare ulteriormente, in termini di effettività della tutela degli interessati, gli strumenti idonei a sanzionare una serie di comportamenti illeciti sul piano amministrativo, che possono essere commessi sia nei confronti degli interessati, sia nei confronti del Garante.

Si è scelto quindi, da un lato, di dare maggior risalto (anche visivo) rispetto al passato ai comportamenti, omissivi e non, da cui può conseguire la contestazione solo di una violazione amministrativa, concentrandoli in un apposito capo, distinti da altri tipi di illeciti; dall'altro, di aggiornare gli importi delle relative sanzioni nei limiti consentiti dalla delega legislativa conferita al Governo.

Nel caso di omessa o incompleta notificazione, oltre alla sanzione pecuniaria amministrativa, è stata prevista specificamente la pena accessoria della pubblicazione dell'ordinanza-ingiunzione. Per le altre violazioni, l'applicazione della pena accessoria della pubblicazione è invece in facoltà dell'Autorità che può disporla quando il suo utilizzo risulti opportuno per le modalità e le finalità del trattamento, oltre che per la natura dei dati, ai fini della tutela dei diritti degli interessati.

Per quanto attiene al procedimento di applicazione, il Codice non ha invece apportato nessuna modifica rispetto a quanto già stabilito dalla disciplina previgente, fatto salvo il conferimento *ex novo* all'Autorità della competenza a contestare e applicare la sanzione amministrativa già prevista in materia di vendite a distanza (art. 179, comma 3, in riferimento al d.lg. n. 185/1999).

L'attività operativa svolta nel corso del 2003 relativamente alle contestazioni di violazioni amministrative è stata caratterizzata da un intenso ricorso allo strumento sanzionatorio. Ciò anche a seguito di indagini effettuate dall'Autorità in specifici settori e che hanno coinvolto, in qualità di titolari, soggetti pubblici e privati. Di

rilievo sono stati anche gli autonomi procedimenti di verifica del rispetto della normativa sui dati personali avviati a seguito di decisione sui ricorsi proposti innanzi all'Autorità, all'esito dei quali è stata spesso prevista la preliminare contestazione di violazione amministrativa.

Tipologia delle violazioni amministrative contestate

L'analisi in dettaglio delle violazioni contestate permette di individuare le operazioni di trattamento e le modalità che sono state oggetto di constatazione di infrazioni.

L'informativa all'interessato, in particolare, nelle attività effettuate per mezzo dei nuovi strumenti multimediali di comunicazione, è stata spesso omessa o è risultata incompleta al momento del raffronto con le modalità e finalità del trattamento perseguite di fatto in concreto dal titolare. Significativo, in proposito, è ad esempio il caso nel quale, a seguito della segnalazione di un interessato, si è accertato che i dati raccolti per mezzo della prenotazione ed acquisto di biglietteria marittima (per le operazioni effettuabili sul sito della compagnia di navigazione) venivano utilizzati anche per attività ulteriori rispetto a quelle per le quali era stata fornita l'informativa presente sul sito stesso. Altre violazioni in tema di informativa sono poi state accertate nell'ambito delle attività di promozione commerciale per mezzo di strumenti di comunicazione elettronica, a causa di trattamenti effettuati in modo difforme dalla previsione normativa, che prevede in argomento il rispetto del principio di *opt-in* (cfr. ora, art. 130, comma 4).

Per quanto riguarda invece i trattamenti di dati personali effettuati per mezzo di sistemi di videosorveglianza, si continuano ad accertare e sanzionare violazioni connesse ad informative assenti o carenti di qualsiasi riferimento alle modalità e finalità del trattamento in tal maniera effettuato.

A seguito di un ricorso proposto dall'interessato, è stata anche accertata e contestata la violazione, da parte di imprese assicuratrici, del principio più volte affermato dal Garante (ora disciplinato in modo parzialmente diverso dal Codice), in base al quale i dati personali in possesso delle imprese stesse e contenuti nelle perizie medico-legali dovevano essere comunicati all'interessato esclusivamente tramite un medico, designato dall'interessato stesso o dall'impresa che detiene i dati (art. 23, comma 2, legge n. 675/1996).

In tema di mancato riscontro alle richieste di informazioni ed esibizione di documenti, rivolte dall'Autorità (ora, ai sensi dell'articolo 157 del Codice), i soggetti pubblici –quali titolari del trattamento– sono risultati purtroppo spesso inadempienti e sono stati pertanto oggetto di varie contestazioni di violazione amministrativa ora prevista dall'articolo 164 (omessa informazione o esibizione al Garante). Merita di essere quindi ribadito in questa sede che la richiesta di informazioni o documenti in tali casi va inquadrata, nell'ambito dei rapporti tra istituzioni pubbliche, come attività strumentale all'imparzialità dell'azione amministrativa: per ben operare l'Autorità ha infatti necessità, nel valutare la fondatezza delle segnalazioni che ad essa pervengono ed al fine di accertare l'eventuale violazione degli obblighi di legge, di assumere una serie completa di elementi, tali da consentire una corretta decisione.

Sempre con riferimento ai trattamenti effettuati da soggetti pubblici, sono state pure accertate, all'esito della verifica presso il registro dei trattamenti sulla notificazione inviata all'Ufficio, violazioni concernenti l'omessa od incompleta notifica-

zione; di conseguenza, sono state predisposte anche in questo caso alcune contestazioni di violazioni amministrative.

Per quanto attiene poi ai provvedimenti di ordinanza-ingiunzione al pagamento di somme, nell'anno 2003 si sono predisposte, ai sensi dell'articolo 17 della legge n. 689/1981, alcune decine di rapporti necessari all'eventuale e successiva adozione del provvedimento medesimo.

Tale dato lascia prevedere che per il futuro, così come si è già verificato per il periodo preso in considerazione, sia ipotizzabile un ulteriore aumento delle attività relative al contenzioso amministrativo dell'Autorità, tra le quali anche quella di obbligatoria audizione delle parti (art. 18 l. n. 689 cit.).

52 L'attività di informazione e comunicazione

52.1. Profili generali

Il rischio di muoversi rapidamente verso una società della classificazione e della sorveglianza, la permanente attenzione ai problemi della sicurezza collettiva, nazionale ed internazionale, il ricorso sempre più massiccio a tecnologie di raccolta e conservazione di dati, il potenziale uso indiscriminato delle informazioni più delicate relative alle persone, hanno indotto il Garante, nel corso del 2003, ad intensificare la sua azione di informazione e comunicazione specie su queste tematiche. Un compito non facile, ma necessario in considerazione dell'obiettivo istituzionale di promuovere un diritto, quello alla protezione dei dati personali, che si è andato affermando come uno dei cardini della nuova cittadinanza elettronica fino ad essere riconosciuto nella sua piena autonomia dalla Carta dei diritti fondamentali dell'Unione europea e, in due disposizioni (artt. I-50 e II-8), dal progetto di Costituzione europea.

L'Autorità ha cercato di raggiungere un livello sempre più alto di produzione informativa riguardo all'intero spettro delle tematiche sulle quali si incentra la sua azione: la tutela della libertà e della dignità della persona, la gestione trasparente delle banche dati, l'uso non discriminatorio delle informazioni personali, specie di quelle sanitarie, fornendo al contempo a cittadini, imprese e istituzioni contributi esplicativi ed indicazioni operative per l'attuazione delle norme, specialmente in presenza del Codice entrato in vigore il 1° gennaio 2004.

Particolare significato ha assunto l'impegno costante rivolto dall'Autorità alla definizione di regole per il corretto utilizzo dei nuovi sistemi di comunicazione, così come l'attenzione posta ai rischi che possono derivare per la libertà delle persone dalle indagini genetiche, dall'uso sproporzionato delle tecniche biometriche, dalla raccolta dei dati *on line*, dalla localizzazione, dall'elaborazione dei profili dei consumatori.

Non è mancata l'attenzione alla promozione della *privacy* come "valore aggiunto" per imprese e pubbliche amministrazioni, al fine di instaurare un rapporto nuovo con cittadini, clienti, utenti e consumatori.

La ricerca di un corretto equilibrio tra diverse esigenze e tra diritti equivalenti ha caratterizzato, anche nel 2003, gli interventi del Garante, con particolare riguardo al diritto di cronaca e alla dignità delle persone.

Trasparenza, correttezza, tempestività, esaustività sono valori ai quali il Garante ha da sempre improntato la sua azione di informazione.

In linea con questi obiettivi, l'Autorità ha confermato la scelta di affidare la sua informazione ad un linguaggio rigoroso, ma attento ad una funzione divulgativa. Nel dar conto della propria attività e delle tematiche all'ordine del giorno, l'Autorità ha richiamato l'attenzione di quanti trattano dati personali sugli obblighi da attuare, sui rischi di violazione e sugli illeciti messi in atto.

52.2. I prodotti informativi ed editoriali del Garante

La tipologia dei prodotti informativi ed editoriali è ampia e differenziata, ma comunque nettamente caratterizzata, alla luce della precisa connotazione istituzionale dell'Autorità, e si fonda su una strategia integrata di comunicazione, nella quale spicca anche un aumentato utilizzo di *mass media* tradizionali, come radio e tv, nonché di *media on line*.

Nel periodo dal 1° aprile 2003 al 15 marzo 2004, sulla base della rassegna stampa prodotta dall'Ufficio, le pagine dei maggiori quotidiani e periodici nazionali ed internazionali e dei media *on line* che hanno dato spazio alle tematiche riguardanti generalmente la *privacy* sono risultate circa 7500, delle quali oltre 1700 dedicate specificamente all'attività del Garante. Le prime pagine dedicate ai temi della protezione dei dati personali sono state circa 700 (di cui oltre 300 riguardanti la sola Autorità). Numerose sono state le interviste pubblicate sulla carta stampata (83), su tv e radio nazionali e locali (130 nel complesso), e diverse su pubblicazioni *on line*.

I prodotti informativi

I prodotti informativi hanno offerto un ventaglio ampio di risposte alle esigenze informative dei cittadini.

La *Newsletter*

La *Newsletter* settimanale, al suo quinto anno di pubblicazione (per un totale complessivo di 205 numeri), è diventata ormai lo strumento di riferimento dell'attività di comunicazione del Garante. In particolare, essa riesce a coniugare un'illustrazione, in chiave giornalistica, dei provvedimenti e dell'attività dell'Autorità con l'esigenza di un'informazione di tipo più ampio ed approfondito. Nel corso degli anni, la *Newsletter* ha infatti dedicato una crescente attenzione a quanto avviene in campo comunitario ed internazionale, riguardo non solo ai temi della protezione dei dati, ma anche al più ampio ambito della tutela dei diritti fondamentali, fornendo un vasto panorama di questioni e problematiche.

La possibilità di consultare la *Newsletter on line* ha facilitato la diffusione delle informazioni.

Le *Newsletter* diffuse tra il 1° gennaio 2003 e il 31 marzo 2004 sono state 54, mentre i comunicati stampa 39.

Il *Cd-Rom*

Nel 2003 è giunto alla sua decima edizione l'archivio digitale ipertestuale "Cittadini e Società dell'informazione", che contiene in forma integrale e nell'originale

veste editoriale i provvedimenti del Garante, il Codice, la documentazione relativa alla normativa nazionale ed internazionale di riferimento e le pubblicazioni realizzate. Il *Cd-Rom*, che consente una consultazione con funzioni di ricerca *full-text*, rappresenta uno strumento ormai conosciuto e costantemente richiesto da parte di amministrazioni pubbliche, imprese, liberi professionisti e cittadini. Le recenti edizioni presentano caratteristiche di multimedialità, con l'inserimento di video divulgativi e dello *spot* televisivo e radiofonico, trasmesso dalle tre reti Rai nel marzo 2003, nonché miglioramenti tecnici e di contenuto che ne rendono ancora più funzionale l'uso.

Il Bollettino

Tra le attività di comunicazione resta il Bollettino che raccoglie i provvedimenti del Garante, la normativa emanata in materia, i comunicati stampa ed altra documentazione significativa, e che dal gennaio 2004 ha aggiornato la propria veste editoriale.

La necessità di sviluppare una sempre maggiore conoscenza delle norme sulla *privacy* e dei diritti oggi riconosciuti ai cittadini, ha spinto l'Autorità a sviluppare nuove modalità di informazione: oltre agli strumenti di comunicazione già utilizzati –da quelli tradizionali (comunicati, *Newsletter*, conferenze stampa, incontri periodici con la stampa) a quelli multimediali ed interattivi– l'Autorità ha realizzato nuovi significativi prodotti.

L'impegno per una comunicazione agile, immediata e diretta in primo luogo al cittadino ha trovato concreta attuazione nella realizzazione di *depliant* divulgativi in grado di illustrare, secondo un percorso ben preciso, i diversi aspetti connessi con la protezione dei dati. I pieghevoli finora pubblicati sono dedicati: il primo all'esercizio dei diritti riconosciuti dalla normativa; il secondo, all'attività e al ruolo del Garante; il terzo a come difendere la *privacy* in Internet.

Il progetto di comunicazione istituzionale proseguirà con la realizzazione di un quarto *depliant* sulla *privacy* nella telefonia.

I prodotti editoriali

Notevole sviluppo hanno avuto poi, nel periodo considerato, i prodotti editoriali dell'Autorità.

Il notiziario bimestrale

Il notiziario bimestrale, *"Garanteprivacy.it"*, che ha preso avvio nel dicembre 2002, è giunto al suo settimo numero. Il bimestrale è una pubblicazione destinata in particolare a personalità del mondo istituzionale ed imprenditoriale, caratterizzata da una comunicazione agile ed essenziale, in grado di sottolineare l'attività dell'Autorità nei diversi settori di intervento.

Allo scopo, inoltre, di contribuire all'approfondimento dei temi legati alla *privacy* e ai principi posti dalla normativa nazionale e comunitaria, il Garante ha deciso di dar vita ad un nuovo prodotto editoriale, la collana "Contributi". Sono attualmente disponibili i primi due volumi, il "Massimario 1997-2001", a cura di Luigi Pecora e Giuseppe Staglianò, relativo ai provvedimenti adottati dal Garante nel primo quadriennio di attività, e "Privacy e giornalismo", a cura di Mauro Paissan.

"Massimario 1997-2001"

Nel primo libro, l'attività di massimazione in chiave tecnico-giuridica dei provvedimenti assunti nel corso degli anni è stata preordinata alla formazione di una rassegna di "giurisprudenza" del Garante che, attraverso un'articolazione in voci e sottovoci, permetta la rapida e corretta individuazione degli argomenti trattati e delle decisioni assunte. L'opera, che arricchisce il panorama delle pubblicazioni curate dal

Garante e la cui edizione è imminente anche su supporto informatico, si indirizza in particolar modo ad una platea di utenti costituita da giuristi, operatori del diritto, ordini professionali, imprese ed istituzioni pubbliche e private.

"Privacy e giornalismo"

Il secondo volume raccoglie, invece, un'ampia scelta delle decisioni adottate dall'Autorità in materia di tutela della persona e libertà di manifestazione del pensiero. I provvedimenti sono organizzati per grandi temi e preceduti da un breve sommario che ne riassume i contenuti e mettendo in luce gli aspetti più significativi. Come in una sorta di manuale pratico per i giornalisti, ma anche per i cittadini, si possono agilmente rintracciare le decisioni riguardanti la tutela dei minori, i rapporti tra cronaca e giustizia, l'uso dei dati di personaggi pubblici, la trasparenza delle fonti pubbliche, i divieti e i rischi derivanti dalla diffusione dei dati sulla salute e sulla vita sessuale, l'uso di fotografie e foto segnaletiche.

È in preparazione un terzo volume, che affronterà il tema della protezione dei dati nelle attività produttive, a cura di Gaetano Rasi.

52.3. La partecipazione a manifestazioni e conferenze

L'attività dell'Autorità collegata con seminari, convegni ed altre iniziative ha visto, nel corso del 2003 e nei primi mesi del 2004, la conferma di un grande interesse da parte del pubblico. In linea con l'obiettivo di promuovere la conoscenza della legge e di diffonderla presso cittadini ed operatori pubblici e privati, il Garante ha confermato la sua presenza in importanti manifestazioni con il proprio *stand* e con la partecipazione dei suoi rappresentanti a dibattiti e convegni.

Forum P.A. 2003

Nell'ambito del *Forum* P.A.-edizione 2003, svoltosi a Roma dal 5 al 9 maggio, il Garante è stato chiamato ad affrontare il tema dei rapporti tra sicurezza e *privacy*, del rispetto delle norme sulla riservatezza da parte delle pubbliche amministrazioni, delle misure organizzative e tecnologiche da adottare per garantire la sicurezza dei dati personali. Gaetano Rasi, componente dell'Autorità, è intervenuto al convegno dedicato a "La sicurezza dei cittadini nello Stato federale". Affrontando il tema dei rapporti tra sicurezza e *privacy*, Rasi ha sottolineato che la tutela della collettività e le garanzie di libertà del singolo individuo sono certamente conciliabili, come sta a dimostrare, in particolare nel campo della videosorveglianza, la fattiva collaborazione con il Ministero dell'interno.

Il segretario generale dell'Autorità, Giovanni Buttarelli, ha tenuto un corso su "La gestione dei dati sensibili e la tutela della *privacy* nei rapporti tra cittadini e amministrazioni". Il corso al quale hanno partecipato centinaia di persone, si è articolato in una prima parte, a carattere illustrativo, dedicata alla evoluzione normativa e in una seconda parte, a carattere pratico, nella quale si è effettuata una verifica dell'applicazione della normativa sulla *privacy* nei diversi settori della p.a.

Com-p.a. 2003

L'Autorità garante è stata presente anche al Com-p.a. 2003, Salone della comunicazione pubblica di Bologna (dal 17 al 19 settembre). Nell'ambito della manifestazione dedicata al tema "Per il buon Governo. Dieci anni di Comunicazione Pubblica", il vice presidente del Garante, Giuseppe Santaniello, ha partecipato al convegno su "Comunicazione e diritto" con un intervento sul tema della protezione dei dati in quanto elemento costitutivo dell'informazione.

Il Com-p.a. ha offerto l'occasione per affrontare i temi legati alla protezione dei dati come elemento costitutivo dell'informazione resa al cittadino e per approfondire le novità più significative introdotte dal recentissimo Codice in materia di protezione dei dati personali.

Nell'ambito della manifestazione, l'Autorità garante ha ricevuto anche quest'anno, per la seconda volta consecutiva, il "Premio Qualità". Il premio è stato assegnato per "i progetti integrati di comunicazione al cittadino".

Smau 2003

L'Autorità ha partecipato inoltre alla 40ª edizione di Smau 2003, Esposizione internazionale di *ICT & Consumer Electronics*, che si è tenuta alla Fiera di Milano dal 2 al 6 ottobre.

L'Autorità è stata presente in tutte e tre le manifestazioni con un proprio *stand* presso il quale è stato programmato un video esplicativo sull'attività del Garante e sulle tematiche della *privacy*, e sono state distribuite le pubblicazioni curate dall'Ufficio, i *depliant* divulgativi e la nuova edizione del *Cd-Rom* "Cittadini e Società dell'informazione", aggiornata con il Codice.

La partecipazione alle conferenze internazionali

Per quanto riguarda l'attività internazionale, va ricordata anzitutto la partecipazione del Garante alla Conferenza di primavera delle autorità europee per la *privacy*, svoltasi dal 3 al 4 aprile 2003 a Siviglia. I temi affrontati nella Conferenza hanno riguardato il settore delle telecomunicazioni; il trasferimento internazionale dei dati; il ruolo delle Autorità di garanzia l'attuazione della direttiva "madre" sulla *privacy* del 1995; la situazione dei Paesi che entreranno a breve a far parte del Gruppo dei garanti Ue.

Stefano Rodotà, in qualità di presidente del Gruppo dei garanti europei, ha fatto il punto sull'attuazione della direttiva-madre europea e sul lavoro svolto dalle Autorità in un periodo che ha visto sul tappeto questioni rilevanti, quali la conservazione dei dati di traffico telefonico, i sistemi di autenticazione *on line*, la richiesta di accesso da parte delle autorità statunitensi alle banche dati delle compagnie aeree europee, nonché, ancora, sulle iniziative che il Gruppo intende prendere in futuro.

Giuseppe Santaniello ha tenuto un'articolata relazione sul nuovo Codice e sulla specifica novità, nel quadro delle fonti, dei codici deontologici italiani.

Mauro Paissan ha tenuto una relazione sulle più importanti decisioni adottate dal Garante in materia di telecomunicazioni, in particolare sull'uso di *Sms* e *Mms*, sul fenomeno dello *spamming* e sulle nuove tecnologie di comunicazione.

Infine, dal 10 al 12 settembre del 2003, l'Autorità ha partecipato alla 25ª Conferenza internazionale delle Autorità Garanti, svoltasi a Sydney. Della Conferenza, conclusasi con l'approvazione di cinque risoluzioni (riguardanti rispettivamente: il trasferimento dei dati dei passeggeri di voli aerei diretti negli Usa; il miglioramento delle informative ai cittadini; la protezione dei dati personali e il ruolo degli organismi internazionali; gli aggiornamenti automatici dei *software*; *Rfid)*, si è già parlato in modo approfondito nei paragrafi. 44.-44.5., ai quali si rinvia.

52.4. Il sito Internet dell'Autorità, il progetto NormeInRete *e le attività editoriali*

Per quanto riguarda il sito Internet del Garante, nell'anno appena trascorso si è consolidata la piattaforma tecnologica del nuovo sito e sono stati attivati alcuni nuovi servizi per il cittadino.

Va in primo luogo segnalata la procedura *web* per la notificazione per via telematica con firma digitale e per la connessa operazione di transazione con carta di credito ai fini del pagamento dei diritti di segreteria. A tale scopo sono state stipulate convenzioni con quattro tra i maggiori emettitori di carte, che potranno essere in futuro utilizzate anche in altre circostanze.

Come annunciato nella Relazione per l'anno 2003, l'Autorità ha poi aderito al progetto intersettoriale nazionale *NormeInRete* promosso dal Cnipa (Centro nazionale per l'informatica nella pubblica amministrazione, su proposta del Ministero della giustizia.

Il portale *www.normeinrete.it*

Il portale *www.normeinrete.it* offre un punto di accesso unitario alla normativa italiana ed europea pubblicata sui siti delle istituzioni aderenti e che (una volta marcata sulla base delle regole espresse in vari *Dtd-Document type definition* –utilizzando il linguaggio informatico *Xml-Extensible markup language*–), oltre a valorizzare ciascun documento per il suo contenuto giuridico, assegna una *Urn* (*Uniform resource names*), ovvero un "nome" univoco al singolo documento. Dal portale nazionale l'utente è così indirizzato verso i siti istituzionali che pubblicano l'informazione richiesta e risulta quindi amplificata la distribuzione della documentazione d'interesse per i cittadini.

La redazione del sito *web* del Garante si è posta peraltro l'ulteriore obiettivo di contribuire fattivamente al progetto *NormeInRete* studiando –in collaborazione con il gruppo di lavoro di *NormeInRete*– un nuovo e specifico standard *Dtd* per marcare i provvedimenti del Garante con modalità che potranno essere all'occorrenza utilizzate da altre autorità indipendenti, al fine di sfruttare l'amplificazione del portale *NormeInRete* ed incrementare le potenzialità del motore di ricerca interno.

Il sito *web* del Garante costituisce inoltre uno strumento volto ad offrire, in conformità all'art. 154, comma 1, lettera *h)* del Codice, la massima conoscenza tra il pubblico della disciplina del trattamento dei dati personali. Per questo, attraverso le sintetizzate tecniche di marcatura, verranno diffusi i testi normativi di riferimento nella versione consolidata.

La pubblicazione sul sito delle norme, dalla versione originaria della legge n. 675/1996 al Codice e agli ulteriori sviluppi normativi, consentirà di ottenere una rappresentazione completa delle modifiche intervenute sulle norme stesse nel tempo, nonché di visualizzare, sempre all'interno del sito, il *link* del provvedimento pubblicato con la versione vigente della norma alla data del documento.

A tal fine, l'anno appena trascorso ha visto la redazione del sito impegnata in uno studio di fattibilità per la piena integrazione tra la piattaforma tecnologica del sito e le peculiari necessità tecniche dettate da *NormeInRete*, nella predisposizione di un apposito capitolato tecnico-esecutivo e nella ricerca e selezione di un *partner* scientifico in grado di fornire un competente ausilio nella marcatura di un volume così alto di documenti. Il *partner* istituzionale ora individuato è il Cirsfid (Centro inter-

dipartimentale di ricerca in storia del diritto, filosofia e sociologia del diritto e informatica giuridica) dell'Università di Bologna che ha acquisito una consolidata esperienza scientifica nel trattamento dell'informazione giuridica in Internet.

Corollario di questo piano di lavoro è, poi, la completa messa *off-line* della precedente versione del sito *web* e il completamento del trasferimento di tutta la copiosa documentazione già disponibile.

Il sito dell'Acc Schengen

Sul piano internazionale è stato inoltre progettato, realizzato e arricchito di contenuti normativi e documentali, il sito dell'Autorità di controllo comune Schengen, durante il periodo di presidenza italiana di tale organismo. Progettato per ospitare contenuti in tutte le lingue dei Paesi che applicano la Convenzione Schengen, il sito è già disponibile in lingua inglese (indirizzo attuale, in vista di nuovi domini in ambito comunitario: *www.schengen-jsa.dataprotection.org*). Nello stesso contesto è stata anche prodotta la versione grafica, sempre in lingua inglese, della *"Newsletter JSA-ACC Schengen"* e del *depliant* della campagna informativa dell'Autorità Schengen.

Presso la redazione *web* continua ad essere infine seguita, oltre ai prodotti dell'editoria tradizionale con particolare riferimento alle relazioni annualli e al Bollettino ufficiale dell'Autorità, la cura editoriale –sino alla pre-stampa tipografica– delle pubblicazioni dell'Autorità (con particolare riferimento ai volumi cui si fa cenno in altre parti di questa *Relazione*, cfr. parag. 52.2).

52.5. Il rapporto con il pubblico: l'Urp e l'attività di formazione

Il rapporto diretto con la società riveste un'importanza fondamentale per l'Autorità che, fin dall'inizio della sua attività, ha inteso presentarsi come un'istituzione vicina ai cittadini, attenta alle nuove frontiere della protezione dei dati personali e dei nuovi diritti della persona. La messa a disposizione sul sito di una notevole quantità di documentazione, con continui aggiornamenti e *dossier* tematici, ha rappresentato uno strumento di informazione e "formazione" del pubblico.

L'interesse che suscita il diritto alla *privacy* è sempre maggiore e, per conseguenza, i motivi di contatto con il pubblico si moltiplicano: da tale riflessione è derivata la scelta dell'Autorità per un modello organizzativo che consenta di tenere adeguatamente conto della funzione di comunicazione, anche come momento di confronto e di dialogo continuo con i cittadini.

In questo quadro, ha assunto un rilievo fondamentale l'entrata in funzione a pieno regime, nel corso del 2003, dell'Ufficio per le relazioni con il pubblico, istituito nell'ambito della segreteria generale, che ha rivestito da subito un ruolo centrale nell'attuazione del progetto di sviluppo della comunicazione tra il Garante ed il pubblico: la sua centralità dipende, in effetti, dal rilevante fabbisogno degli utenti e dalla costante crescita delle aspettative ed esigenze degli utilizzatori di questo tipo di comunicazione ed informazione.

L'attivazione di tale Ufficio ha pure contribuito a garantire la qualità dell'azione amministrativa, permettendo all'Autorità di percepire il grado di soddisfazione dell'utenza per le risposte da essa date alle molteplici problematiche avanzate. Inoltre, ha creato un canale che permette di cogliere con immediatezza quali sono le tematiche di cui è più avvertita l'importanza da parte della collettività.

In proposito, le materie che nel periodo preso in esame hanno formato più spesso oggetto di quesiti rivolti all'Ufficio (o per le quali più di frequente è stato richiesto materiale informativo) sono state lo *spamming*, il trattamento dei dati da parte delle "centrali rischi" private, l'esercizio dei diritti previsti dall'art. 13 della legge n. 675/1996 (ora, dall'art. 7 del d.lg. n. 196/2003), la videosorveglianza, il trattamento dei dati nell'ambito del rapporto di lavoro e il trasferimento di dati all'estero.

Per le pubbliche amministrazioni, particolare rilievo dominante ha assunto il rapporto tra la normativa in materia di *privacy* e la legge n. 241/1990, nonché, per gli enti locali, quella del diritto di accesso dei consiglieri comunali e provinciali.

Peraltro, sebbene l'attività dell'Ufficio sia stata rivolta prevalentemente a fornire elementi su questioni per le quali si era già formato un consolidato orientamento del Garante, non sono mancate risposte a quesiti su aspetti di novità.

Nel corso del 2003 l'affluenza del pubblico in cerca di un contatto diretto con l'Autorità è aumentata in modo costante. I mezzi di comunicazione utilizzati per le risposte sono stati le lettere, l'invio di *fax*, le risposte telefoniche e le *e-mail*: questi ultimi due strumenti sono stati privilegiati, laddove possibile, per la loro agilità e speditezza.

In particolare, sono pervenuti allo specifico indirizzo di posta elettronica dell'Ufficio diverse migliaia di quesiti e richieste di documentazione; allo stesso modo, i riscontri forniti a mezzo *e-mail*, *fax* o lettera sono quantificabili in svariate migliaia. Ancora più numerosi sono stati i contatti telefonici (stimabili in oltre dodicimila), per brevi questioni o richieste di chiarimenti ed informazioni, cui è stata sempre data puntuale e rapida risposta.

Vi sono stati, poi, momenti di "picco" nei contatti del pubblico con l'Urp, che si sono verificati anche in occasione dello *spot* televisivo e radiofonico trasmesso nel marzo 2003 dalle reti Rai o di trasmissioni televisive su profili di interesse.

Rilievo particolare ha poi assunto il nuovo Codice che, sin dalla sua emanazione (giugno 2003), ha dato luogo ad un'intensa attività di comunicazione incentrata su aspetti interpretativi e applicativi, soprattutto per quanto riguarda le misure di sicurezza e gli adempimenti connessi alla notificazione. Tale attività, via via incrementatasi con l'avvicinarsi della data di entrata in vigore della nuova normativa, ha portato l'Ufficio a fornire sempre più spesso risposte, pur se con la necessaria prudenza, a questioni di carattere innovativo.

Infine, proprio attraverso il contatto diretto con i cittadini ha assunto ulteriore incisività il potere del Garante di intervenire tempestivamente in occasione di situazioni particolarmente lesive della *privacy* (ad esempio, con la misura cautelare del blocco dei dati trattati in violazione di legge, oppure con accertamenti e controlli).

I corsi di formazione

L'impegno, infine, di contribuire in maniera fattiva alla promozione della cultura della protezione dei dati presso aziende e pubbliche amministrazioni, nonché all'applicazione delle norme e alla corretta attuazione degli adempimenti nell'at-

tività quotidiana, ha portato il Garante ad avviare un'attività di formazione. L'iniziativa si è concretizzata nel primo corso, organizzato con successo il 2 aprile 2004, rivolto al mondo dell'impresa, al quale seguiranno presto quelli dedicati ad amministrazioni pubbliche e sanità da un lato, e alle comunicazioni elettroniche dall'altro.

VII - La gestione amministrativa dell'Ufficio

53 Le novità legislative e l'organizzazione dell'Ufficio

Il d.lg. n. 196/2003, nel capo II dedicato all' Ufficio del Garante, ha confermato l'impianto normativo già previsto dalla legge n. 675/1996 e successive modificazioni, conferendogli un ordine sistematico più razionale.

Nel nuovo quadro resta demandata ai regolamenti del Garante la definizione dell'organizzazione e del funzionamento dell'Ufficio, del trattamento giuridico ed economico del personale –pur con le limitazioni previste dal Codice–, nonché della gestione amministrativa e contabile.

L'organico dell'Autorità viene confermato nel limite senz'altro esiguo di cento unità.

L'art. 182 del Codice prevede che il Garante, in sede di prima applicazione e comunque non oltre il 31 marzo 2004, possa individuare i presupposti per inquadrare in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilità di organico, il personale in posizione di fuori ruolo o di comando presso l'Autorità in servizio presso l'Ufficio alla data di pubblicazione del Codice nella *Gazzetta Ufficiale* (29 luglio 2003). Di tale facoltà il Garante si è avvalso individuando i criteri in data 31 marzo 2004. Il Codice dispone inoltre che il Garante possa prevedere riserve di posti nei concorsi pubblici, nel limite del 30% dei posti disponibili in organico, per il personale non di ruolo che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

Le predette disposizioni sono finalizzate ad assicurare il buon andamento dell'Autorità, ma nel rigoroso rispetto dell'art. 97 Cost., evitando che vada disperso un patrimonio di conoscenze ed esperienze acquisite. Il personale interessato all'inquadramento è integralmente composto da dipendenti pubblici, reclutati esclusivamente tramite concorso pubblico.

In attuazione di tale disciplina il Garante ha pertanto bandito due nuovi concorsi pubblici (oltre quelli già banditi nel 2003 e che si potrebbero ulteriormente bandire nel 2004), riservando il 30% dei posti al personale non di ruolo (in posizione di fuori ruolo o a contratto) che abbia maturato i requisiti previsti (cfr. *infra*, parag. 55.).

La modifica della pianta organica

La pubblicazione dei bandi è stata preceduta da una riflessione sulle esigenze funzionali e organizzative dell'Autorità, a conclusione della quale si è deciso di ridurre l'area esecutiva da 9 a 3 unità e di redistribuire le residue 6 unità tra l'area direttiva (5 unità) e quella operativa (1 unità), con provvedimento di modifica della pianta organica pubblicato sulla *Gazzetta Ufficiale* e allegato alla presente *Relazione*.

La parziale modifica delle dotazioni organiche è finalizzata a potenziare e rafforzare l'Ufficio, dotandolo di personale di elevata qualificazione da destinare prevalentemente all'area giuridica, in considerazione dei nuovi compiti demandati all'Autorità dal Codice.

Il processo di consolidamento della struttura organizzativa dell'Autorità, avviato negli anni precedenti e continuato nel 2003, è confermato in particolare dalle nuove immissioni di personale reclutato all'esito delle procedure concorsuali e selettive indette dall'Autorità stessa.

Avvalendosi delle convenzioni Consip S.p.A., sono state conferite in *outsourcing* e *insourcing* alcune attività di natura esecutiva. È inoltre proseguita la gestione di un servizio di *inbound* telefonico, con funzioni di centralino.

Parallelamente, al fine di poter meglio adempiere ai nuovi e delicati compiti assegnatigli dal Codice, il Garante ha provveduto al rinnovo degli incarichi (previsti per la durata di due anni rinnovabili) ai dirigenti dell'Ufficio.

Per una migliore funzionalità dell'Ufficio e nel rispetto delle priorità istituzionali sono stati avviati graduali avvicendamenti negli incarichi dirigenziali, finalizzati anche alla valorizzazione delle esperienze dei singoli dirigenti.

Mediante l'istituzione di un'unità temporanea di vigilanza e controllo si è perseguito l'obiettivo di incrementare l'attività ispettiva, già notevolmente cresciuta nel 2003 con significativi risultati.

Il documento programmatico per il 2004

Nel quadro delle iniziative per migliorare efficienza, efficacia ed economicità dell'azione amministrativa, contestualmente all'approvazione del bilancio di previsione, il Garante ha come di consueto definito nel documento programmatico i principali obiettivi e le priorità per il 2004. La direttiva del Garante sarà seguita da ulteriori atti di indirizzo del segretario generale tendenti a specificare tempi e modalità di attuazione dei programmi di lavoro di ciascuna unità organizzativa e delle articolazioni interne all'Ufficio.

Per la definizione di parametri di valutazione e di indicatori per la verifica dei risultati dell'attività dell'Ufficio, oltre che per un controllo di regolarità della gestione contabile, è operante un servizio di controllo interno (al quale partecipano un magistrato contabile e due dirigenti di provata esperienza e competenza) ed è in fase di avanzata definizione un efficiente sistema di controllo di gestione, cui occorre ora accennare.

53.1. Gli interventi per il miglioramento dell'azione amministrativa

Nel corso del 2003 sono proseguiti gli interventi per il miglioramento dell'assetto organizzativo e degli obiettivi di efficacia, efficienza ed economicità dell'azione amministrativa, specialmente in considerazione dell'aumentato volume di compiti affidati dal Codice all'Ufficio del Garante, che è peraltro rimasto invariato nel suo assetto organico.

Gli interventi, attuati sulla base degli studi effettuati nell'anno precedente anche sulla base dei contributi di due società di consulenza, hanno riguardato in particolare:

- la costituzione, con delibera del gennaio 2003, del servizio di controllo interno;

- l'immissione in servizio dal mese di luglio di una nuova figura dirigenziale presso la segreteria generale con compiti delegati di coordinamento di talune attività amministrative (direttore di gestione);

- la progettazione di un sistema informativo direzionale per il controllo di gestione (Sid) coerente con il metodo della programmazione per funzioni obiettivo.

Il progetto Sid

Il progetto Sid è stato predisposto con risorse interne e si basa sulla cd. gestione per obiettivi, che costituisce un metodo di analisi largamente usato per la valutazione della gestione di ogni tipo di organizzazione, comprese le pubbliche amministrazioni.

Il sistema utilizza il criterio del grado di raggiungimento degli obiettivi per guidare ogni fase della gestione e per valutare, misurandole, le prestazioni delle unità organizzative e dei dirigenti ad esse preposti: per "obiettivi" si intendono, infatti, i risultati in termini di efficacia, economicità e qualità, espressi in numeri finiti, che si decide di conseguire in un tempo determinato.

I diversi livelli dell'Autorità sul piano strategico, direzionale ed operativo riceveranno flussi di informazione costanti e di elevata qualità sulla "produzione" realizzata e sull'assorbimento delle risorse umane e finanziarie. I *report* verranno forniti con brevi cadenze periodiche, in modo che sia possibile stimare tempestivamente gli scostamenti dai programmi e disporre in tempo utile gli interventi correttivi.

Si è scelto di basare la valutazione del sistema su prodotti e risorse, piuttosto che sulle attività, in quanto si tratta degli oggetti che più facilmente ed attendibilmente si prestano ad essere rilevati e contabilizzati. Viceversa, sui processi di lavoro verranno svolte in modo trasparente alcune analisi, utilizzando anche, laddove possibile, tecniche comparative *(benchmarking)*, per l'eventuale reingegnerizzazione dei processi e comunque per indurre miglioramenti in termini di qualità, costi e tempi di esecuzione. La progettazione è stata svolta partendo dalla considerazione della situazione attuale dell'Autorità, con particolare riferimento ai compiti istituzionali delineati dall'art. 154 del d.lg. n. 196/2003, al disegno della struttura organizzativa, alle caratteristiche quantitative e qualitative del personale dipendente, alla struttura delle spese e alle infrastrutture tecnologiche disponibili.

Peculiare attenzione è stata dedicata alle tipologie di processi di lavoro ed all'individuazione delle categorie di servizi offerti al pubblico. I processi di lavoro sono stati raggruppati nelle seguenti funzioni-obiettivo: informazione e regolazione preventiva, controllo e tutela, registro dei trattamenti, comunicazione istituzionale, cui si debbono aggiungere l'indirizzo politico-amministrativo e le attività per il funzionamento della struttura. L'archivio dei processi è configurato come un sistema che rileva l'assorbimento delle risorse umane nelle diverse linee di attività per centri di costo e per centri di responsabilità.

È previsto che la prima versione del Sid entri a regime entro il primo semestre del 2004 e che il sistema sia aggiornato periodicamente, in modo da consentirne la

crescita graduale e facilitare i dirigenti nella comprensione ed utilizzazione consapevole del nuovo strumento.

È importante sottolineare che il sistema non ha carattere ispettivo, ma mira espressamente a fornire un supporto ai processi decisionali, a favorire la crescita dell'organizzazione e ad ottenere la massima valorizzazione del personale, nonché a stimolare la collaborazione, l'automiglioramento e la condivisione delle conoscenze.

53.2. Lo sviluppo del sistema informativo e l'attività in ambito tecnologico-informatico

L'operato dell'Ufficio nel settore tecnologico e informatico è stato caratterizzato nel 2003, per quanto attiene alle attività negoziali, da un maggiore ricorso a servizi rispetto all'acquisizione di beni e attrezzature, nel segno di una progressiva integrazione dei sottosistemi precedentemente sviluppati e che nel loro insieme costituiscono il sistema informativo dell'Ufficio.

Nello stesso tempo si è sviluppata notevolmente la capacità di integrazione basata su risorse interne e tecnologie *software* di tipo *open source*. Questi strumenti sono stati utilizzati per significative realizzazioni, quali il sito *web* per il supporto al lavoro cooperativo del Servizio studi e documentazione, in precedenza, il sistema di gestione del contenzioso amministrativo.

Il Dipartimento risorse tecnologiche ha inoltre continuato a svolgere i propri compiti di gestione delle infrastrutture, di assistenza nei confronti degli utenti interni, di consulenza nei confronti dei dipartimenti giuridici e di altre articolazioni dell'Autorità, di contributo alla vita amministrativa dell'Ufficio, di progettazione e sviluppo di sistemi *software* di *database*, di *reporting*, di documentazione.

Il sistema informativo si è arricchito di nuove funzionalità o ha visto realizzate quelle che erano state delineate o progettate nell'anno precedente, nell'ottica del perseguimento di ancora più elevati livelli di efficienza, a vantaggio dell'azione amministrativa dell'Autorità.

Molte risorse sono state assorbite dalla manutenzione e dallo sviluppo dei sistemi di sicurezza a protezione della rete e delle risorse dell'Ufficio. Strumenti quali gli *antivirus* per le postazioni individuali, per i *gateway* di posta elettronica, per i *proxy server*, sono stati ulteriormente affinati, così come i sistemi di rilevamento delle intrusioni e i sistemi di protezione da accessi indesiderati.

È stata progettata e sviluppata internamente la procedura di notificazione telematica tramite *web* prevista dal Codice, che ha comportato la realizzazione di servizi *web* sicuri, con crittografia forte, avvalendosi di una autorità di certificazione ufficiale, al fine di garantire la riservatezza delle transazioni e la sicurezza dei pagamenti dei diritti di segreteria. Per la parte di sviluppo del *database* ci si è avvalsi del supporto di una ditta specializzata che ha curato la programmazione delle relative procedure. Questa attività è stata svolta in coordinamento con il Dipartimento registro dei trattamenti, con cui si è sviluppata una specifica collaborazione all'atto della definizione dei requisiti del nuovo sistema e nella successiva fase di realizzazione.

La procedura di notificazione telematica si avvale delle capacità di riconoscimento e controllo delle firme digitali previste dal nuovo sistema di gestione del pro-

tocollo informatico, la cui definizione ha impegnato il Dipartimento per tutto il secondo semestre del 2003, consentendo di avviare il nuovo sistema il 1° gennaio del 2004, in aderenza al dettato normativo.

L'introduzione del nuovo sistema di gestione del protocollo ha facilitato l'opera di controllo dello stato delle pratiche da parte dei dirigenti assegnatari. Il nuovo protocollo informatico consente anche una maggiore trasparenza amministrativa, sia per gli *standard* di sicurezza che garantiscono l'immodificabilità dei documenti registrati, sia per la possibilità di fare accedere per via telematica, con i cosiddetti codici Urp, il pubblico interessato e avente diritto a conoscere lo stato delle pratiche che lo riguardano. L'intera procedura è infatti di tipo *web oriented* ed è utilizzabile tramite un comune *browser*.

In parallelo all'adozione del nuovo sistema di protocollo si è proceduto alla registrazione dell'Autorità nell'indice delle pubbliche amministrazioni gestito dal Cnipa, accessibile con protocolli *Ldap* e interrogabile anche tramite interfaccia *web*.

A supporto del protocollo informatico, è stato realizzato in collaborazione con il Cnipa un sistema di posta elettronica certificata che consente l'interazione tramite posta elettronica, con pieno valore legale, con altre amministrazioni o cittadini che utilizzino servizi *e-mail* in un dominio di posta certificata.

Il Dipartimento ha poi dedicato un rilevante impegno alle procedure amministrative nell'ambito del procedimento di gara europea per aggiudicare il servizio di scansione ottica delle notificazioni di trattamento dei dati personali pervenute nel periodo 1997-2003.

Si è trattato di un lavoro molto impegnativo sia per la valutazione della complessità del servizio, che include l'archiviazione sostitutiva e la successiva eliminazione degli originali cartacei, sia per l'esigenza di un'approfondita ed equa comparazione dei progetti presentati.

Una delle più rilevanti innovazioni realizzate dal Dipartimento è l'introduzione di un servizio di posta elettronica per l'Ufficio che viene ora gestito interamente con risorse interne e con strumenti in dotazione. Il servizio svolto in proprio ha consentito infatti di pervenire ad elevatissimi livelli di efficienza, all'estensione delle funzionalità, all'incremento della sicurezza e della protezione dei dati, alla possibilità di gestire con la massima flessibilità tutte le politiche di trattamento dello *spam* e dei contenuti dannosi *(virus, warm, trojan)*. Tutto ciò con risparmio di risorse economiche da dedicare a servizi specialistici di diverso tipo relativi alle metodologie e alle procedure di sicurezza *(security assessment)*.

È stato portato in produzione l'ulteriore sistema informatico per la gestione amministrativo-contabile (Sigac) che, interagendo con altri sottosistemi, come il protocollo e il sistema di gestione del personale, costituisce il nucleo del complessivo sistema informativo dell'Ufficio. Con il Sigac è stato possibile predisporre in modo più efficiente la previsione di bilancio per l'esercizio 2004 e attivare le piene funzionalità del sistema, in modo da avviare il 1° gennaio 2004 la contabilità in modalità totalmente automatizzata.

Il personale del Dipartimento ha infine contribuito all'attività istituzionale del Garante in sede internazionale, in particolare partecipando al lavoro della *Internet Task Force* a supporto del Gruppo istituito ai sensi dell'art. 29 della direttiva europea, interessandosi in particolare dei sistemi di autenticazione a *single sign-on* e dei problemi di *privacy* derivanti dalla gestione dei servizi di *directory* di tipo *whois* associati alla gestione dei nomi a dominio.

54 Il bilancio, gli impegni di spesa e l'attività contrattuale

Il bilancio di previsione del 2003, riferito al settimo anno di attività del Garante, è stato elaborato secondo le direttive del regolamento del Garante n. 3/2000.

Le risorse finanziarie sono state indirizzate prevalentemente verso quei settori individuati nel documento programmatico di accompagnamento al bilancio di previsione che ha fissato gli obiettivi dell'Ufficio per l'esercizio 2003.

Il bilancio di previsione del 2003 è stato predisposto tenendo conto di tutto ciò e l'intensa attività del Garante è stata resa possibile, nel periodo considerato, non solo dalle risorse finanziarie assegnate ai servizi più impegnati su tali fronti, ma anche in relazione all'incremento delle risorse umane a disposizione dell'Ufficio, poiché a seguito dei concorsi espletati nel 2002 l'organico è stato implementato, dall'inizio dell'anno, di ventitré unità (cfr. parag. 55.).

Inoltre, con le due prime delibere adottate nel 2003, il Garante ha istituito il servizio di controllo interno previsto dall'art. 8, comma 5, del regolamento 1/2000 ed ha nominato i tre componenti che ne fanno parte. Il servizio interno, oltre ai compiti propri di un organo di controllo contabile, dovrà fornire al Garante elementi di valutazione dei risultati dell'attività dell'Ufficio e per la verifica della corretta ed economica gestione delle risorse pubbliche.

Le risorse a disposizione del Garante per il 2003 sono state accertate, nell'esercizio, per euro 11.709.701,00 di cui provenienti dal contributo dello Stato per euro 10.252.000,00. Le restanti risorse finanziarie sulle quali ha potuto contare l'Autorità per entrate proprie si riferiscono ai diritti di segreteria per le notificazioni, per i ricorsi e le autorizzazioni, ai rimborsi spese provenienti dal Consiglio d'Europa e dalle istituzioni comunitarie per la partecipazioni di rappresentanti del Garante a riunioni a Bruxelles e nelle altre sedi comunitarie, agli interessi maturati sui fondi relativi agli avanzi pregressi, alle entrate derivanti dalla sublocazione di alcuni locali dell'edificio di piazza di Monte Citorio 115, e ad entrate accertate per sanzioni pecuniarie. Il contributo dello Stato per il 2003 è stato ridotto rispetto al 2002 di quasi 600 mila euro e poiché il complesso delle uscite previsto per l'anno 2003 è stato superiore a circa 1.600 mila euro rispetto all'anno precedente, dovuto questo in gran parte agli oneri derivanti dai nuovi assunti, tali minori entrate, aggiunte alle maggiori spese, sono state compensate con un circoscritto ricorso all'utilizzo dell'avanzo di amministrazione. Nell'esercizio 2003 la spesa per il personale in servizio ha registrato un incremento del 4% sul totale delle spese, passando dal 61% del

2002 al 65% del 2003. Inoltre, l'esercizio che si è chiuso al 31 dicembre ha registrato per la prima volta un'eccedenza del totale delle spese impegnate sul totale delle entrate accertate. Come detto in precedenza lo sbilancio è stato coperto ricorrendo all'utilizzo dell'avanzo di amministrazione.

Le spese di funzionamento sono state ulteriormente contenute e razionalizzate, e seguitano ad essere limitate all'indispensabile poiché l'Autorità, dalla fine del 2002 e a seguito dell'emanazione del decreto legge n. 194 (convertito con la legge n. 246/2002) concernente la limitazione degli impegni di spesa non aventi carattere obbligatorio, ha proseguito nella politica di contenimento delle spese aventi tali finalità. Infatti, benché l'attività del Garante si sia notevolmente incrementata in qualità e in quantità, la percentuale delle spese di funzionamento sul totale delle spese in bilancio è leggermente diminuita passando dal 26,9% del 2002 al 26,4% del 2003.

Il costante decremento nello stanziamento pubblico per il Garante, passato da euro 11.362.000 del 2000 a 10.081.000 del 2004 e compensato parzialmente dall'incremento delle entrate proprie, induce l'Autorità a perseguire attualmente una politica di bilancio molto attenta che, per il momento, non intacca i servizi che sono giudicati prioritari, come l'elevato livello del sistema informatico e della sua rete interna. Tuttavia, come emerso anche dal dibattito parlamentare su una recente mozione, la dotazione di fondi e altre risorse a sostegno dell'Autorità non potrà non essere incrementata.

Il Dipartimento contratti e risorse finanziarie nel corso del 2003 ha dato seguito a molteplici richieste tese all'approvvigionamento di beni e servizi pervenute su indicazione dei vari uffici.

Gran parte di questa attività è stata dedicata al potenziamento delle strutture tecnologiche.

L'Autorità ha dato notevole impulso allo sviluppo del sistema informativo seguendo un programma di acquisizione curato dal Dipartimento risorse tecnologiche.

Il Dipartimento contratti e risorse finanziarie, su attivazione del Dipartimento registro dei trattamenti, anche sulla base delle nuove necessità emerse con l'emanazione del d.lg. n. 196/2003 in materia di notificazioni dei trattamenti al Garante, ha attivato le procedure necessarie a consentire l'automazione delle lavorazioni e velocizzare l'accesso alle notificazioni memorizzate, nonché a procedere all'adeguamento tecnologico necessario a consentire l'uso della firma digitale per tali adempimenti.

Nel 2003 è stata espletata la gara per l'acquisizione del servizio di scansione ottica delle notificazioni del trattamento dei dati personali e di memorizzazione di file contenuti nei *floppy disk*. La gara è stata bandita ai sensi del decreto legislativo 17 marzo 1995, n. 157, è stata pubblicata nella *Gazzetta Ufficiale C.E.* 28 novembre 2002, n. S231e nella *Gazzetta Ufficiale* 29 novembre 2002, n. 280. L'avviso di aggiudicazione è stato pubblicato nella *Gazzetta Ufficiale* 30 luglio 2003, n. 175. Il servizio ha reso possibile la visualizzazione diretta tramite registro dell'intera notificazione compresi gli allegati.

Inoltre, si è proceduto a sviluppare il *software* necessario per attivare il nuovo registro dei trattamenti con l'obiettivo di inviare telematicamente la notificazione superando i problemi connessi alla compilazione e all'invio dei modelli cartacei.

Tra le varie attività contrattuali espletate nel corso del 2003 è da citare anche la gara svolta per l'affidamento del servizio di noleggio delle autovetture con conducente. Il bando è stato pubblicato nella *Gazzetta Ufficiale*, parte seconda, 30 luglio 2003, n. 175 e nella *Gazzetta Ufficiale C.E.*, 2 agosto 2003, n. S147 (affidamento del servizio di noleggio di autoveicoli con conducente per il trasporto di persone per conto dell'Autorità, mediante il ricorso alla licitazione privata di cui all'art. 6, comma 1, lett. *b)*, d.lg. n. 157/1995). L'avviso di aggiudicazione è stato invece pubblicato nel Foglio delle inserzioni della *Gazzetta Ufficiale* 17 dicembre 2003, n. 292.

Come previsto dalla finanziaria 2003, nel quadro delle iniziative di razionalizzazione della spesa per beni e servizi della p.a., l'Autorità si è anche rivolta alla Consip S.p.A., che cura lo sviluppo e la gestione operativa del relativo programma, per acquisire alcuni beni e servizi necessari per le esigenze dell'Ufficio con la stessa appositamente concordati. Si è così proceduto a stipulare appositi contratti per i servizi di pulizia, per la raccolta e lo smaltimento dei rifiuti speciali, per la disinfestazione dei locali, la manutenzione degli impianti antincendio, nonché per reperire alcuni servizi quali quello di guardiania e *reception*. Sempre nell'ambito della convenzione Consip S.p.A. si è proceduto a rinnovare la convenzione per la fornitura dei buoni pasto e si è aderito alla convenzione Consip per alcuni servizi di telefonia.

Infine, nell'ambito del piano di razionalizzazione della spesa dell'Autorità, è da citare l'avvenuta adesione dell'Autorità al primo mercato elettronico della p.a. attivato da Consip S.p.A. su incarico del Ministero dell'economia e delle finanze e dal Dipartimento per l'innovazione e le tecnologie della Presidenza del Consiglio dei ministri.

55 Il personale e i collaboratori esterni

Nel periodo considerato è proseguito il processo di consolidamento dell'Autorità con l'immissione in servizio, agli inizi del 2003, dei vincitori di quattro concorsi pubblici espletati dall'Autorità per la copertura di complessivi 21 posti (dei quali 19 coperti), di cui n.1 per dirigente informatico, n. 2 per dirigente, n. 10 per funzionario e n. 8 per impiegato operativo (vedi *Relazione 2002*). Tale processo è stato rafforzato dal contemporaneo inserimento in servizio di altre 4 unità con contratto di specializzazione a tempo determinato, selezionate con una procedura bandita nell'agosto 2002.

Sono stati inoltre stipulati 4 contratti di *stage*, all'esito di una selezione che ha portato alla formazione di una graduatoria alla quale attingere periodicamente, al fine di offrire a giovani laureati la possibilità di un periodo di tirocinio presso il Garante.

Come accennato nel paragrafo 53., il Garante ha bandito di recente due nuovi concorsi pubblici per complessivi 13 posti, di cui 9 nel ruolo di funzionario, e 4 nel ruolo di impiegato operativo, riservando il 30% dei posti a concorso al personale non di ruolo in servizio presso l'Autorità che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno. A garanzia dell'imparzialità delle procedure concorsuali il Garante, come per il passato, ha chiesto e ottenuto dal Consiglio di presidenza della giustizia amministrativa la nomina dei presidenti delle due commissioni esaminatrici.

Contestualmente il Garante ha indetto una selezione per il reclutamento di un massimo di 3 giovani laureati in materie giuridiche, da assumere con contratto di specializzazione a tempo determinato.

Con i concorsi appena banditi, l'organico dell'Autorità sarà coperto al 90% circa. Attualmente infatti l'Ufficio dispone di 93 unità, di cui 59 appartenenti al ruolo organico, 18 (n. 2 a *part-time*) assunte con contratto a tempo determinato e 16 in posizione di fuori ruolo o comando da altre amministrazioni ed enti pubblici, come da prospetto allegato:

Area	Dotazione organica	Personale di ruolo	Personale fuori ruolo	Personale a contratto	TOTALE
Dirigenti	26	17	5		22
Funzionari	40	27	6		33
Operativi	25	15	5		20
Esecutivi	9				0
Personale a contratto	20			18	18
TOTALE	120	59	16	18	93

Personale in servizio

L'Autorità allo stato non si avvale della collaborazione di consulenti esterni. Nel periodo considerato si è peraltro reso necessario acquisire occasionali consulenze qualificate, per le problematiche concernenti il sistema informativo interno e il sito *web* del Garante, per l'attuazione del nuovo programma di gestione del bilancio e della contabilità e per la definitiva sistemazione della biblioteca e dell'ampio materiale documentale acquisito e prodotto dall'Autorità nel corso della sua attività. Sono da ultimo in corso due brevi incarichi di studio per necessari approfondimenti in alcune tematiche giuridiche.

56 La notificazione ed il registro dei trattamenti

La notificazione del trattamento dei dati personali ha subito profondi cambiamenti nella sua *ratio*, nei suoi contenuti e nelle sue modalità di compilazione a seguito dell'emanazione del Codice. Prima di affrontare questo aspetto, occorre soffermarsi sull'attività svolta nel 2003 e nei primi mesi del corrente anno in relazione al vecchio registro dei trattamenti istituito ai sensi dell'abrogata legge n. 675/1996.

Un profilo significativo è stato in primo luogo quello della sottoposizione a scansione ottica dell'enorme archivio cartaceo custodito nel magazzino messo a disposizione dalla Presidenza del Consiglio dei ministri-Dipartimento della protezione civile presso il centro polifunzionale di Castelnuovo di Porto. Tale attività comporterà indubbi vantaggi per il Garante, rendendo immediato il riscontro delle notificazioni, agevolando le attività tese alla regolarizzazione delle pratiche e consentendo il risparmio di spese di gestione e di manutenzione dell'archivio stesso.

Nel 2003 l'attività del Dipartimento registro generale dei trattamenti si è sviluppata su quattro direttive: proseguimento della memorizzazione delle notificazioni pervenute entro il 31 dicembre dello stesso anno; regolarizzazione delle notificazioni incomplete; riscossione dei diritti di segreteria inevasi; progettazione del nuovo registro dei trattamenti.

In particolare, il recupero dei diritti di segreteria inevasi ha fatto affluire nel bilancio del Garante più di 80.000,00 euro. Le richieste di regolarizzazione sono state circa 12.000. Si stanno tuttora esaminando alcune migliaia di posizioni, per le quali la verifica dovrebbe concludersi entro il mese di aprile del 2004.

La nuova notificazione

Per quanto riguarda la nuova notificazione, come già accennato, l'esperienza di sei anni ha indotto il Garante a rivederne completamente le caratteristiche.

Come si è già detto (cfr. *supra,* parag. 1.6.), a differenza di quanto previsto dalla legge n. 675/1996, dove tutti coloro che effettuavano il trattamento dei dati personali erano obbligati a notificare, salvo i casi di esonero per taluni titolari, con il nuovo sistema notificano solo i titolari dei trattamenti che sono elencati nell'art. 37 del Codice: si tratta di casi che, per la particolare delicatezza dei dati, le modalità di trattamento o le finalità perseguite, presentano rischi per i diritti e le libertà dell'interessato. In particolare, il Codice ha individuato sei categorie di trattamenti sottoposti ad obbligo di notificazione ed ha altresì attribuito al Garante il potere di incrementare o ridurre l'elenco dei trattamenti sottoposti a tale obbligo, con proprio provvedimento. A tal riguardo, il 31 marzo scorso il Garante ha emanato il provvedimento teso ad esonerare alcuni trattamenti dall'obbligo di notificazione, su cui cfr. *supra*, parag. 12.

Non sono stati previsti modelli differenziati di notificazione, essendosi scelto un'unico modello di notificazione, di semplice compilazione e di contenuto ridotto agli elementi davvero significativi.

L'attuale istituto della notificazione e le connesse procedure, fruibili solo *on line*, si ispirano ai seguenti obiettivi: grande flessibilità nell'individuazione di contenuti e tipologie dei trattamenti sottoposti ad obbligo di notificazione; richiesta delle sole notizie essenziali ed effettivamente utili all'attività di controllo da esercitare; semplificazione della procedura di notificazione; possibilità per gli interessati di consultare direttamente il registro.

I contenuti della notificazione sono stati determinati dal Garante stesso al momento in cui ne ha delineato il modello. Ciò consente un'estrema flessibilità e rapidità nell'adattare il modello di notificazione alle esigenze di tutela dei dati personali, senza dover ricorrere allo strumento normativo.

Per quanto riguarda la modalità di notificazione, l'art. 38 del Codice consente solo la compilazione e la trasmissione per via telematica, direttamente sul *server* del Garante. I diritti di segreteria possono essere corrisposti utilizzando *on line* la carta di credito (oppure tramite bonifico bancario o conto corrente postale). Infine, alla notificazione, prima della spedizione, deve essere apposta la firma digitale.

La procedura della notificazione

La procedura si sviluppa attraverso una sequenza di moduli *on line* che l'utente richiama entrando nel sito *web* del Garante e che sono corredati di spiegazioni, sia a carattere generale, sia sui singoli campi da compilare. L'utente può scegliere se consultare il registro, accedere alle istruzioni generali, procedere ad una notificazione (o modificarla), consultare le cd. *Faq*, accedere ad altri siti di interesse per la notificazione (es. elenco dei certificatori, organismi convenzionati).

La semplificazione per il notificante consiste nel fatto che, in qualsiasi Paese si trovi, può predisporre la notificazione, sospenderla, portarla a termine. In caso di mancanza di firma digitale, l'utente può recarsi presso operatori convenzionati (intermediari) ed utilizzare la loro firma digitale. Per permettere la notificazione tramite intermediari qualificati, il Garante ha stipulato apposite convenzioni con Poste S.p.A., l'Unione nazionale professionisti pratiche (Unappa) e l'Alar (Associazione lavoratori autonomi riuniti). È in fase di studio la stipula di altre convenzioni.

In caso di sospensione della notificazione, l'utente è in grado di riprenderla successivamente utilizzando un codice personale, che viene di volta in volta assegnato automaticamente. La procedura è validamente conclusa qualora sia stata completata l'apposita maschera con gli estremi del pagamento –il che permette di risolvere il problema del recupero dei diritti di segreteria non versati– e sia stata apposta la firma digitale.

La notificazione è *una tantum* e deve sempre precedere il trattamento; solo per i trattamenti di dati personali iniziati antecedentemente al 1° gennaio 2004, in sede di prima attuazione, è previsto il termine del 30 aprile per l'invio (art. 181, comma 1, lett. *c)* del Codice).

Al 31 marzo 2004 risultano regolarmente inviate n. 320 notificazioni, delle quali la gran parte sono prime notificazioni e provengono da soggetti privati.

Ovviamente i dati esposti sono provvisori e, allo stato attuale, non ancora altamente significativi; è difficile, infatti, fare al momento previsioni analitiche circa il preciso numero di notificazioni che andranno a costituire il registro dei trattamenti.

Il nuovo registro

Il nuovo registro, con la facoltà di interrogare l'intero archivio e di incrociare i dati dei singoli campi, offre un ausilio indispensabile al Garante per monitorare in maniera efficace il panorama dei trattamenti oggetto di notificazione, allo scopo di consentire sia il controllo da parte degli interessati, sia quello da parte della stessa Autorità, che può sfociare anche nell'adozione di specifici provvedimenti ad opera del Garante.

57 Il Servizio studi e documentazione

Il Garante ha ripreso e potenziato l'attività del Servizio studi e documentazione anche allo specifico scopo di promuovere indagini conoscitive volte all'acquisizione di informazioni provenienti dai diversi attori dei settori interessati all'applicazione della normativa sulla protezione dei dati.

L'Autorità considera infatti importante instaurare un dialogo con gli stessi operatori. Tale scambio consente, da una parte, a questi ultimi di ottenere chiarimenti sul sistema normativo in materia di tutela dei dati personali anche per orientare i propri investimenti in maniera conforme alla legge; dall'altra, è assai utile al Garante stesso per conoscere più approfonditamente le problematiche derivanti dall'applicazione della normativa sulla *privacy* nei diversi settori.

L'Autorità ha inoltre potenziato l'attività di documentazione e di ricerca promuovendo la formazione di *dossier* informativi su materie di interesse del Garante; la circolazione di tali *dossier* potrebbe, in prospettiva, essere pure allargata all'esterno dell'Ufficio.

L'attività di ricerca, tra l'altro, ha un ruolo determinante anche al fine di acquisire le conoscenze necessarie ogni qualvolta l'Autorità ritenga opportuno agire di proprio impulso, piuttosto che su attivazione esterna. Interventi di iniziativa propria del Garante appaiono del resto quanto mai opportuni alla luce dei molteplici eventi che ai vari livelli (normativo, scientifico, tecnologico) hanno delle ripercussioni sulla disciplina in materia di *privacy*.

È in questa prospettiva, ad esempio, che nel corso del periodo in esame si è ritenuta utile l'elaborazione di analisi variamente articolate in tema di *Radio frequency identification*, televisione interattiva, banche del cordone ombelicale e localizzazione.

Dati statistici

58 Prospetto analitico (*)

Attivitò Garante / Atti e provvedimenti

Richieste di informazione e quesiti telefonici	38.180
Segnalazioni e reclami pervenuti	7.109
Quesiti pervenuti	994
Richieste di parere pervenute (parere *ex* art. 31 comma 2)	22
Richieste di autorizzazione pervenute	21
Notificazioni dei trattamenti previste dagli articoli 7, 16 e 28	9.791
Autorizzazioni generali al trattamento dei dati sensibili (art. 22) rilasciate per categorie di titolari e di trattamenti (art. 41, comma 7)	7
Autorizzazioni rilasciate a singoli destinatari	2
Risposte a quesiti	834
Risposte a segnalazioni/reclami	4.080
Pareri rilasciati in base all'art. 31, comma 2	14
Provvedimenti istruttori ai sensi dell'art. 32 comma 1	227
Procedimenti contenziosi definiti sulla base di ricorsi (art. 29)	775
Elementi forniti per la risposta del Governo a interrogazioni parlamentari	5
Comunicati stampa e dichiarazioni alla stampa	39
Notiziari settimanali pubblicati dal Servizio relazioni con i mezzi di informazione	54
Richieste di accesso e/o di verifica di dati esistenti nel Sistema d'informazione Schengen	480
Procedimenti relativi alle richieste di accesso e/o di verifica di dati esistenti nel Sistema d'informazione Schengen già definiti	464
Seminari e conferenze internazionali	10
Procedimenti ispettivi	69
Segnalazioni all'autorità giudiziaria	16

Servizi ispettivi

Ispezioni effettuate:	69
sopralluoghi ex art. 32, comma 1	61
accessi alle banche dati con decreto dell'autorità giudiziaria	7
accessi alle banche dati con assenso informato	1
Segnalazioni all'autorità giudiziaria:	16
per trattamento illecito (art. 35)	5
per omessa adozione misure minime di sicurezza (art. 36)	6
per false dichiarazioni al Garante	2
per inosservanza dei provvedimenti al Garante (art. 37)	3

Ufficio relazioni con il pubblico

Risposte fornite nel 2003 con *e-mail*, fax o lettera	5.754
Totale chiamate telefoniche ricevute	12.600
Richieste *e-mail* evase	4.338
Richieste con lettera evase	144
Richieste con fax evase	90
E-mail pervenute alla casella urp	6.060

(*) I riferimenti normativi sono relativi alla legge n. 675/1996
Periodo di riferimento 1° gennaio 2003 - 31 marzo 2004

Registro generale dei trattamenti

Legge 31 dicembre 1996, n. 675:	
notificazioni presenti nel Registro	330.000
lettere inviate per la regolarizzazione dei versamenti in conto corrente	11.832
richieste di accesso al Registro	210
richieste di copie della notificazione	410
somma relativa ai diritti di segreteria recuperati (in euro)	83.000
Decreto legislativo 30 giugno 2003, n. 196:	
nuove notificazioni telematiche validamente effettuate	320
nuove notificazioni telematiche sospese e in via di completamento	853

Servizio ricorsi

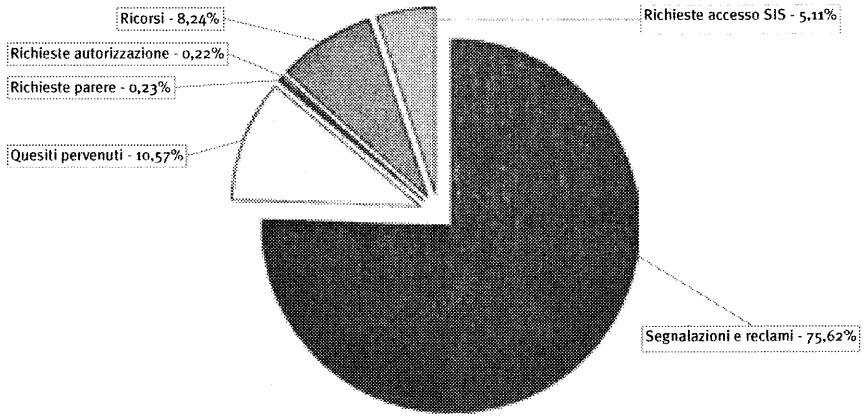
Decisioni al termine del procedimento	775
Tipo di decisioni adottate:	
non luogo a provvedere	331
inammissibilità	149
accoglimento	128
parziale accoglimento	110
infondati	57

Call-center [1]

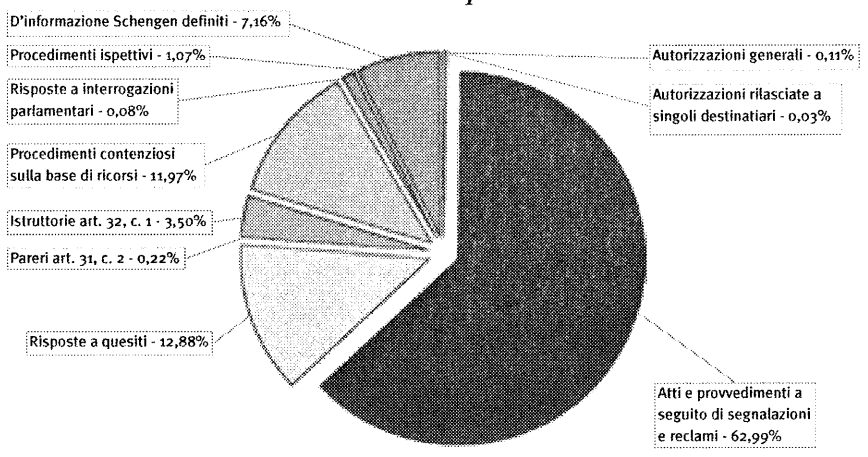
Quesiti sul nuovo codice	
Notificazioni (Obbligo, Compilazione, Modalità, etc.)	21
Documento programmatico sulla sicurezza	19
Quesiti sul codice in generale	13
Centrali Rischi Finanziarie	
Provvedimenti, richieste di cancellazioni, etc.	14
Tabulati telefonici in chiaro	
In entrata	8
In uscita	3
Richieste di accesso al S.I.S.	5
***Spamming* e comunicazioni commerciali e/o indesiderate**	
Provvedimenti e informazioni su cosa fare	9
Informazioni sulle pratiche	
In attivo	10
Concluse	4
Denunce su presunte violazioni	6
Informazioni su concorsi banditi	7
Varie richieste	
Partecipazione a seminari, convegni, corsi, etc.	2
Interviste, partecipazioni TV, etc...	1
Comunicare con segreterie e dipendenti dell'ufficio	14
Numeri telefonici, fax, *e-mail*	10
Informazioni sulle pubblicazioni (*Cd-Rom*, Bollettini, Libri, etc...)	5
Info generiche su ricorsi e notifiche (modulistica, c/c postali, etc...)	12
Altro	3

(1) Tipologia delle richieste medie su base giornaliera

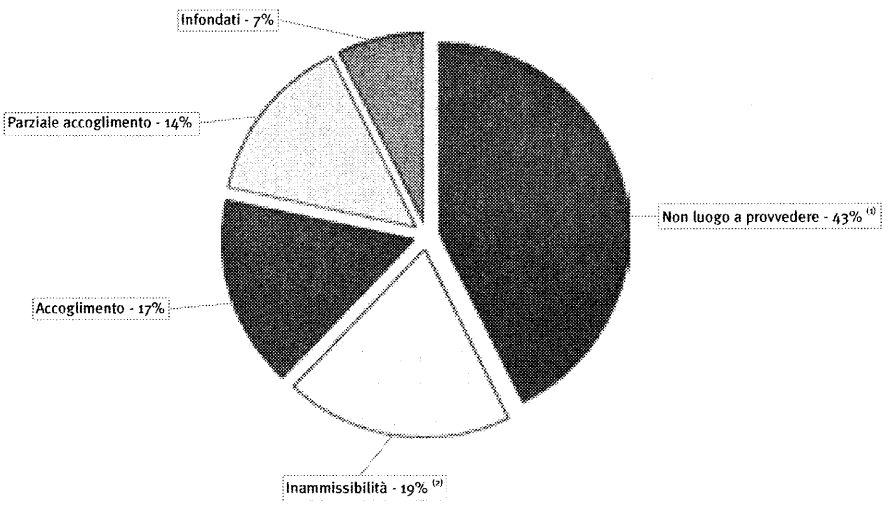
Atti e Provvedimenti richiesti
(esclusa assistenza telefonica e notificazioni)



Attività espletate



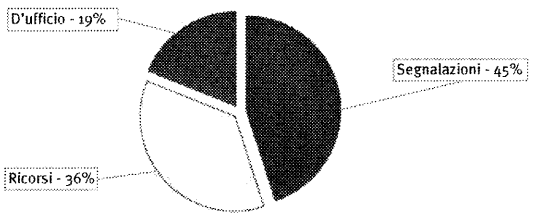
Statistica dei ricorsi

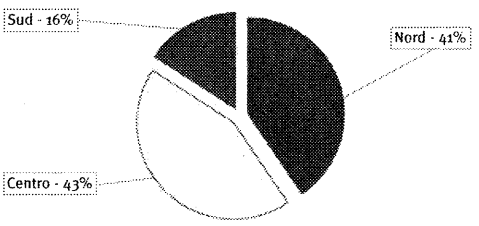


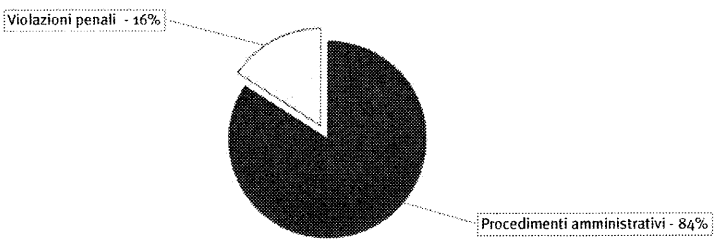
(1) Decisioni quasi integralmente riferite a casi nei quali il titolare/responsabile del trattamento ha aderito tardivamente alle richieste dell'interessato, nel caso del procedimento

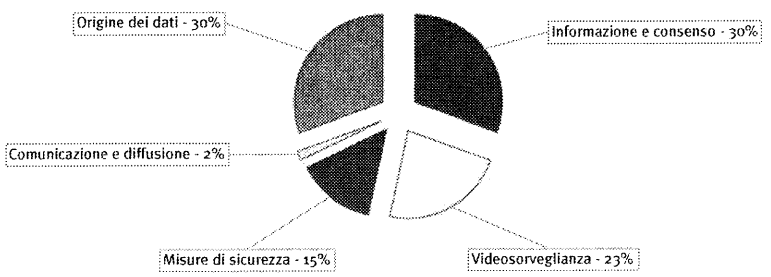
(2) Casi di ricorsi formalmente irregolari e non regolarizzati, o nei quali il titolare/responsabile del trattamentro non era stato preventivamente interpellato; casi di richieste non previste dalla legge o di trattamenti cui non si applica la disciplina sui ricorsi

Servizi ispettivi









DOCUMENTAZIONE

VIII - Provvedimenti del Garante

59 Differimento dell'efficacia delle autorizzazioni per il trattamento dei dati sensibili e giudiziari (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni, in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Viste le autorizzazioni per il trattamento dei dati sensibili e giudiziari numeri 1/2002, 2/2002, 3/2002, 4/2002, 5/2002, 6/2002 e 7/2002 rilasciate il 31 gennaio 2002 ai sensi degli articoli 22, 23, 24 e 41, comma 7, della legge n. 675/1996, pubblicate nella *Gazzetta Ufficiale* del 9 aprile 2002, n. 83 e in scadenza al 30 giugno 2003;

viste, altresì, le autorizzazioni in scadenza alla medesima data rilasciate su richiesta di singoli titolari del trattamento in casi particolari;

Considerato che la legge 24 marzo 2001, n. 127, ha previsto l'emanazione di un testo unico delle disposizioni in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali e delle disposizioni connesse, da adottarsi entro il termine del 31 dicembre 2002, prorogato sino al 30 giugno 2003 dall'articolo 26 della legge 3 febbraio 2003, n. 14;

Considerato che il 9 maggio 2003 è stato esaminato dal Consiglio dei ministri, in attuazione della legge n. 127 del 2001, uno schema di decreto legislativo recante il Codice in materia di protezione dei dati personali, di cui è prevista l'entrata in vigore il 1° gennaio 2004;

Ritenuta la necessità di differire il rilascio di nuove autorizzazioni ad un momento successivo all'emanazione del summenzionato codice ed alla sua entrata in vigore, al fine di armonizzare le prescrizioni già impartite alla nuova disciplina e di tenere conto dell'esperienza maturata nella fase di prima applicazione del Codice;

Ritenuta, pertanto, la necessità di differire sino a tutto il 30 giugno 2004 l'efficacia delle menzionate autorizzazioni in scadenza al 30 giugno 2003, e ciò per permettere la prosecuzione dei vari trattamenti di dati già autorizzati nei riguardi di diversi soggetti privati e pubblici;

Visti gli atti d'ufficio;

Viste le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000, pubblicato nella *Gazzetta Ufficiale* della Repubblica Italiana n. 162 del 13 luglio 2000;

Relatore il prof. Stefano Rodotà;

(*) Deliberazione n. 8 del 24 giugno 2003, in *Gazzetta Ufficiale* del 18 agosto 2003, n. 191

DELIBERA:

di differire sino al 30 giugno 2004 l'efficacia delle autorizzazioni per il trattamento dei dati sensibili e giudiziari numeri 1/2002, 2/2002, 3/2002, 4/2002, 5/2002, 6/2002 e 7/2002 rilasciate il 31 gennaio 2002 ai sensi degli articoli 22, 23, 24 e 41, comma 7, della legge n. 675/1996 e pubblicate nella *Gazzetta Ufficiale* del 9 aprile 2002, n. 83, nonché delle altre specifiche autorizzazioni indicate in premessa.

Il presente provvedimento sarà pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 24 giugno 2003

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

60 Modifiche alle dotazioni organiche dell'Autorità (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del dott. Mauro Paissan e del prof. Gaetano Rasi, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Vista la legge 31 dicembre 1996, n. 675, e successive modificazioni ed integrazioni;

Visto l'art. 156, comma 3, lettera c), del decreto legislativo 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali", il quale demanda al Garante la ripartizione dell'organico, con proprio regolamento, tra le diverse aree e qualifiche;

Visti i regolamenti del Garante numeri 1, 2 e 3/2000 e successive modificazioni ed integrazioni;

Vista la tabella n. 5 allegata al predetto regolamento n. 2/2000 con la quale è stato ripartito l'organico dell'ufficio tra le diverse aree e qualifiche;

Considerato che il 1° gennaio 2004 entrerà in vigore il citato "Codice in materia di protezione dei dati personali", e che il quadro istituzionale in esso delineato derivano effetti rilevanti sull'attività e l'organizzazione dell'Autorità, sulle competenze istituzionali attribuite al Garante e sui procedimenti amministrativi, i quali richiedono un potenziamento organizzativo e il reclutamento di personale di elevata qualificazione al fine di poter meglio adempiere ai compiti che la legge demanda al Garante e al relativo ufficio;

Rilevato che la dotazione organica dell'area direttiva e, in misura minore, dell'area operativa è divenuta carente in relazione ai nuovi compiti demandati all'Autorità, mentre risultano allo stato non coperti nove posti dell'area esecutiva;

Ritenuta la necessità, per poter far fronte alle esigenze organizzative prima richiamate, di procedere ad una circoscritta revisione dell'organico dell'Autorità mediante la riduzione da nove a tre posti della dotazione organica dell'area esecutiva e una contestuale redistribuzione delle predette unità tra l'area direttiva, nella misura di cinque posti, e di quella operativa, nella misura di un posto;

Accertata la disponibilità di fondi sui relativi capitoli di spesa e dato atto che gli oneri relativi alle predette modifiche delle dotazioni organiche graveranno interamente sui fondi stanziati per le spese di funzionamento del Garante;

Rilevato che sono state informate le organizzazioni sindacali del personale dipendente e visti gli atti relativi alla procedura di concertazione esperita presso l'Ufficio su richiesta delle stesse;

Ritenuta la necessità che le predette modifiche delle dotazioni organiche entrino in vigore il giorno successivo alla data della pubblicazione nella *Gazzetta Ufficiale*;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15, comma 1, del regolamento n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio;

Relatore il prof. Giuseppe Santaniello;

(*) Deliberazione n. 20 del 18 dicembre 2003, in *Gazzetta Ufficiale* del 30 gennaio 2004, n. 24

Delibera:

la tabella n. 5, allegata al regolamento del Garante n. 2/2000, recante la ripartizione del ruolo organico del personale dipendente del Garante, è sostituita dall'allegata tabella nella quale sono riportate, nei termini di cui in motivazione, le nuove dotazioni organiche dell'Autorità, che entrano in vigore il giorno successivo alla data di pubblicazione della presente deliberazione.

La presente deliberazione sarà trasmessa all'Ufficio pubblicazioni leggi e decreti del Ministero della giustizia per la pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 18 dicembre 2003

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello

IL SEGRETARIO GENERALE
Buttarelli

RUOLO ORGANICO DEL PERSONALE DIPENDENTE DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Area	Posti
Dirigenza	26
Direttiva	45
Operativa	26
Esecutiva	3
Totale	**100**

61 Disposizioni in materia di comunicazione e di propaganda politica (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORI il prof. Giuseppe Santaniello e il dott. Mauro Paissan;

Premesso

1. Finalità del provvedimento.

Le iniziative di propaganda elettorale intraprese da partiti, organismi politici, comitati promotori, sostenitori e singoli candidati costituiscono un momento particolarmente significativo della partecipazione alla vita democratica (art. 49 Cost.) che deve però rispettare i diritti e le libertà fondamentali delle persone cui si riferiscono le informazioni utilizzate.

Con l'approssimarsi di una tornata di consultazioni elettorali, l'Autorità ritiene necessario richiamare l'attenzione sulle garanzie vigenti dopo l'entrata in vigore del Codice in materia di protezione dei dati personali che ha sostituito la legge n. 675/1996 (d.lg. 30 giugno 2003, n. 196), e fornire in particolare indicazioni sull'informativa alle persone interessate.

A tal fine, verranno segnalati in questo provvedimento i casi in cui si possono utilizzare dati personali a fini di propaganda informando gli interessati, ma senza richiedere il loro consenso, e i casi in cui al contrario il consenso è necessario. Saranno poi evidenziati i diritti degli interessati di conoscere le modalità di utilizzazione dei dati che li riguardano e di far interrompere l'attività di propaganda nei propri confronti.

2. Dati tratti da registri o elenchi pubblici.

a) Quando si può prescindere dal consenso.
È possibile utilizzare dati personali senza il consenso degli interessati per la propaganda elettorale solo se i dati sono estratti da fonti "pubbliche" nel senso proprio del termine, ovvero conoscibili da chiunque senza limitazioni.

Questa ipotesi ricorre quando si utilizzano registri, elenchi, atti o documenti che sono detenuti da un soggetto pubblico, e al tempo stesso sono liberamente accessibili – senza discriminazioni – in base ad un'espressa disposizione di legge o di regolamento.

Se non ricorre questa condizione, l'amministrazione o l'ente pubblico che detiene i dati non può permetterne l'utilizzo a partiti, forze politiche o candidati, dovendo utilizzarli solo per svolgere funzioni istituzionali e osservando i presupposti e i limiti stabiliti, caso per caso, da norme generali o speciali contenute anche nel Codice (art. 18, commi 2 e 3, d.lg. cit.), che a volte rendono i dati "pubblici" solo per permetterne l'uso per alcune finalità.

Possono essere ad esempio utilizzate per la propaganda elettorale:
a) le c.d. *liste elettorali* (ovvero, le liste degli aventi diritto al voto detenute presso i

(*) Provvedimento 12 febbraio 2004, in *Gazzetta Ufficiale* del 24 febbraio 2004, n. 45

comuni), le quali *"possono essere rilasciate in copia per finalità di applicazione della disciplina in materia di elettorato attivo e passivo ... o per il perseguimento di un interesse collettivo o diffuso"* (art. 51 d.P.R. 20 marzo 1967 n. 223, come modificato dall'art. 177, comma 5, del d.lg. n. 196/2003);

b) gli *elenchi di iscritti ad albi e collegi professionali* (art. 61, comma 2, d.lg. n. 196/2003), e i dati contenuti in *taluni registri detenuti dalle camere di commercio*;

c) *altri elenchi e registri in materia di elettorato attivo e passivo*. Sebbene sia opportuno al riguardo un chiarimento normativo, risultano utilizzabili a fini di propaganda le seguenti fonti:

- *l'elenco degli elettori italiani residenti all'estero per le elezioni del Parlamento europeo* (formato sulla base dei dati contenuti nelle liste elettorali e trasmesso agli uffici consolari: art. 4, commi 1 e 5, d.l. 24 giugno 1994, n. 408, convertito con l. 3 agosto 1994, n. 483);
- *le c.d. liste aggiunte dei cittadini elettori di uno Stato membro dell'Unione europea* (istituite a livello comunale anche in riferimento ai dieci Paesi che vi faranno parte dal 1° maggio 2004), residenti in Italia e che intendano ivi esercitare il diritto di voto alle elezioni del Parlamento europeo (d.lg. n. 197/1996; circolare Min. interno 30 dicembre 2003, n. 134, in *Gazzetta Ufficiale* 8 gennaio 2004, n. 5; v. anche Com. della Commissione europea COM (2003) 174 def. dell'8 aprile 2003);
- *l'elenco aggiornato dei cittadini italiani residenti all'estero finalizzato alla predisposizione delle liste elettorali*, realizzato unificando i dati dell'anagrafe degli italiani residenti all'estero (AIRE) e degli schedari consolari (art. 5 l. 27 dicembre 2001, n. 459);
- *l'elenco dei cittadini italiani residenti all'estero aventi diritto al voto per l'elezione del Comitato degli italiani all'estero* (Comites), reso pubblico con modalità definite con un regolamento (artt. 13 e 26 l. 23 ottobre 2003, n. 286; art. 5, comma 1, l. 27 dicembre 2001, n. 459; art. 5, comma 1, d.P.R. 2 aprile 2003, n. 104).

Va comunque segnalato a chi utilizza fonti "pubbliche" la necessità di porre attenzione:

- alle modalità prescritte in alcuni casi per accedere ai dati (ad esempio, per identificare il soggetto che ne ottiene copia);
- alla circostanza che i dati siano accessibili al pubblico solo per finalità specifiche. Non possono ad esempio ritenersi utilizzabili a fini di propaganda le informazioni sugli studenti ricavabili dalla pubblicazione degli esiti di attività scolastiche, oppure gli elenchi di immigrati o affetti da determinate malattie o di beneficiari di provvidenze economiche concesse da amministrazioni comunali a portatori di *handicap*, invalidi e indigenti, le graduatorie per il ricovero in istituti di sostegno o in case di cura, le liste di assegnazione degli alloggi di edilizia residenziale pubblica, gli elenchi dei beneficiari di parcheggi riservati a persone con ridotta capacità motoria;
- alle condizioni e ai limiti eventualmente posti per stabilire come utilizzare i dati dopo averne ottenuta copia. Tale utilizzazione deve poi avvenire sempre in termini compatibili con gli scopi per i quali i dati sono stati raccolti e registrati (art. 11, comma 1, lett. b), d.lg. n. 196/2003), e che in alcuni casi è possibile solo se si indica la data della loro estrazione e l'origine.

Non sono invece utilizzabili per la propaganda elettorale altre fonti della pubblica amministrazione, quali, ad esempio:

1) atti anagrafici e dello stato civile.

I dati degli iscritti nelle anagrafi comunali della popolazione non possono essere forniti in alcun modo a privati per scopi di propaganda elettorale (tantomeno in forma elaborata di elenchi di intestatari di nuclei familiari), anche se il richiedente è un amministratore locale o il titolare di una carica elettiva.

Possono rivolgere una motivata richiesta di rilascio di elenchi solo le amministrazioni pubbliche per esclusivo uso di pubblica utilità (art. 34 d.P.R. n. 223/1989). Questa garanzia opera anche nei confronti del comune, il quale può utilizzare anch'esso i dati anagrafici che

detiene solo per usi di pubblica utilità, anche in caso di comunicazione istituzionale (art. 177 d.lg. n. 196/2003), sicché tali dati non possono essere utilizzati per la propaganda elettorale o per pubbliche relazioni di carattere personale.

Anche gli atti dello stato civile sono soggetti ad un regime ben diverso da quello delle liste elettorali (art. 450 cod. civ.; d.P.R. n. 396/2000) e non possono quindi ritenersi "pubblici" nel senso proprio del termine sopra indicato;

2) dati tratti dalle liste elettorali di sezione già utilizzate nei seggi.

Le liste elettorali di sezione già utilizzate nei singoli seggi e sulle quali sono stati annotati dati relativi alle persone che hanno votato non possono essere utilizzate a fini di propaganda. Tali liste contengono dati particolari a volte sensibili (idonei a rivelare l'effettiva partecipazione dei cittadini alle votazioni o, in tutto o in parte, a particolari consultazioni), e sono verificabili da ogni cittadino entro quindici giorni dal deposito in cancelleria, solo per il controllo sulla regolarità delle operazioni elettorali (art. 62 d.P.R. 16 maggio 1960 n. 570, recante il t.u. delle leggi per la composizione e l'elezione degli organi delle amministrazioni comunali, applicabile anche alle elezioni regionali ex art. 1, comma 6, l. 17 febbraio 1968, n. 108). A tali liste non è applicabile né la disciplina di cui al citato art. 51 del d.P.R. n. 223/1967, né il diritto di accesso riconosciuto ai titolari di cariche elettive ai fini dell'espletamento del relativo mandato;

3) dati annotati da scrutatori e rappresentanti di lista.

Scrutatori e rappresentanti di lista, nell'esercitare funzioni affidate o consentite dalla legge e connesse al regolare svolgimento delle operazioni di voto, possono venire a conoscenza di dati anche sensibili (quali quelli relativi a coloro che hanno votato o meno presso una determinata sezione), da trattare con ogni opportuna cautela anche a garanzia della libertà e segretezza del voto, soprattutto nei casi in cui (come i *referendum* abrogativi o le votazioni di ballottaggio) la partecipazione al voto o l'astensione può evidenziare di per sé una particolare opzione politica. In particolare, tali soggetti non possono compilare elenchi di persone astenutesi dal voto, specie al fine di invitarle a votare in successivi appuntamenti elettorali;

4) schedari istituiti presso gli uffici consolari.

Ai dati anagrafici dei cittadini iscritti negli schedari istituiti presso gli uffici consolari ai sensi dell'art. 67 del d.P.R. n. 200/1967, possono ritenersi applicabili le disposizioni sul rilascio degli atti anagrafici, che prevedono la possibilità di rilasciare elenchi degli iscritti nell'anagrafe della popolazione residente unicamente alle amministrazioni pubbliche che ne facciano motivata richiesta, per esclusivo uso di pubblica utilità.

3. Casi equiparati ai registri pubblici: elenchi telefonici.

La disciplina degli elenchi telefonici, cartacei ed elettronici, è stata oggetto di recenti modifiche che hanno mutato in radice la loro natura in attuazione di norme comunitarie.

Il nuovo regime sarà attuato prevedibilmente nella seconda metà del 2004 e la propaganda sarà possibile in futuro solo nei confronti di chi vi acconsenta.

Nel frattempo, gli elenchi della telefonia fissa (e non anche quelli della telefonia mobile) restano utilizzabili per la propaganda elettorale solo mediante invio di posta ordinaria o chiamate telefoniche effettuate da un operatore, a meno che gli interessati si siano opposti (cfr. art. 55 e 75 d.lg. 1 agosto 2003, n. 259).

4. Propaganda lecita con il consenso.

Fuori dei predetti casi, benché la propaganda elettorale abbia una sua specificità rispetto alla comunicazione commerciale e di *marketing*, non è possibile effettuarla senza un consenso preventivo e specifico dell'interessato, basato su un'informativa che evidenzi chiara-

mente l'utilizzo dei dati a tale fine (e sia espresso in forma scritta se, come si vedrà, i dati hanno natura sensibile), in particolare quando si ricorre ai seguenti mezzi:

a) invio di fax;

b) invio di messaggi Sms e Mms;

c) chiamate telefoniche senza l'intervento di un operatore.

Ci si riferisce all'utilizzo di sistemi automatizzati che effettuano chiamate vocali preregistrate senza l'intervento, caso per caso, di un operatore;

d) chiamate di ogni tipo a terminali di telefonia mobile.

Il regime transitorio menzionato per la telefonia fissa non riguarda la telefonia mobile.

Senza il consenso preventivo e informato dell'abbonato, o del reale ed unico utilizzatore della scheda di traffico prepagato, non è lecito effettuare chiamate vocali di propaganda a terminali mobili, automatizzate e non, o inviare -anche in questo caso- messaggi *Sms* o *Mms* anche tramite siti *web*.

La volontà dell'interessato deve essere manifestata prima della chiamata o del messaggio e non può essere elusa inviando senza consenso un primo messaggio con il quale si chieda di aderire all'invio di ulteriori messaggi di propaganda.

Il consenso deve essere espresso in forma chiara (specificando la finalità di propaganda specie quando è richiesto con una formula ampia, riferita anche a scopi commerciali e di *marketing*) e "positiva" (anziché con una modalità di silenzio-assenso);

e) indirizzi di posta elettronica.

Gli indirizzi di posta elettronica recano dati personali che non rientrano tra le fonti "pubbliche" liberamente accessibili da chiunque e sono utilizzabili solo sulla base di un libero consenso (artt. 24 e 130 d.lg. n. 196/2003; v. Provv. del Garante 29 maggio 2003 sul c.d. *spamming*, in *www.garanteprivacy.it*).

Il consenso è necessario anche quando gli indirizzi o altri dati personali:

- sono ricavati da pagine *web*;
- sono formati ed utilizzati automaticamente con un *software* senza l'intervento di un operatore, oppure in mancanza di una verifica della loro attuale attivazione o dell'identità del destinatario;
- quando gli indirizzi non sono registrati dopo l'invio dei messaggi.

La circostanza che gli indirizzi di posta elettronica possano essere reperiti con una certa facilità in Internet non comporta il diritto di utilizzarli liberamente per inviare messaggi di qualunque genere.

Il principio del consenso si applica anche per:

- i dati di utenti che prendono parte a *forum* o *newsgroup*, resi conoscibili in Internet per partecipare ad una determinata discussione e che non sono utilizzabili per fini diversi senza un consenso specifico (art. 11, comma 1, lettere a) e b), d.lg. n. 196/2003);
- gli indirizzi compresi nella lista "anagrafica" di abbonati ad un *Internet provider*, o pubblicati su siti *web* per specifici fini di informazione aziendale, comunicazione commerciale o attività istituzionale od associativa;
- comunicazioni inviate a gestori anche privati di siti *web* utilizzando gli indirizzi pubblicati sugli stessi siti, o che sono reperibili consultando gli elenchi dei soggetti che hanno registrato i nomi a dominio;

f) iscritti ad associazioni politiche o a partiti.

L'utilizzazione da parte di partiti o associazioni politiche di dati relativi a loro iscritti, a simpatizzanti o a partecipanti ad iniziative politiche in occasione delle quali si raccolgano informazioni sul loro conto (come pure di dati acquisiti sottoscrivendo petizioni, proposte di legge, richieste di *referendum* o raccolte di firme), comporta un trattamento di dati personali "sensibili".

In questi casi il consenso specifico deve essere manifestato per iscritto.

Quando il consenso è raccolto all'atto di adesione all'organizzazione, occorre un'idonea informativa collegata ad un chiaro contesto interno risultante dallo statuto o da altri atti dell'organizzazione noti agli interessati (v. comunicato stampa del Garante del 16 ottobre 1997, in *Bollettino* n. 2, p. 82). Particolare attenzione va prestata poi alla chiarezza dell'informativa e alla formula di consenso presenti su siti *web* che raccolgano dati sensibili di aderenti o simpatizzanti anche ai fini dell'invio di *newsletter* a contenuto politico.

Se i dati sono acquisiti nell'ambito di altri eventi politici, l'informativa deve evidenziare parimenti con chiarezza l'utilizzazione dei dati che si prevede in aggiunta alle finalità perseguite in via principale (ad esempio, nel caso in cui si intenda comunicare i dati a singoli candidati o a comitati elettorali delle medesime formazioni politiche).

Ogni eventuale comunicazione ad altri soggetti (organizzazioni di simpatizzanti, enti, associazioni, società e persone fisiche non direttamente connesse all'attività del titolare del trattamento), indipendente ed ulteriore rispetto alle finalità della raccolta dei dati, deve essere basata su un consenso distinto da quello previsto per il predetto trattamento "principale";

g) utenti o aderenti a organizzazioni non politiche.

Quando si presta un'attività (ad esempio, assicurativa) o un servizio (ad esempio, presso una casa di cura) o si svolge un'attività associativa *no-profit* a scopo diverso da quello politico, non è lecito utilizzare indirizzari o altri dati personali per propagandare candidati interni alla società, all'ente o all'associazione o da questi sostenuti (v. Provv. Garante del 5 ottobre 1999 e del 9 ottobre 2000, in *Bollettino* n. 14/15, p. 17 s.).

L'utilizzazione a fini di propaganda dei dati relativi agli iscritti ad associazioni sindacali, professionali, sportive e di categoria che non abbiano un'espressa connotazione politica, è possibile solo quando ricorrono le seguenti condizioni:

- venga disposta legittimamente in base all'ordinamento interno;
- le modalità di utilizzo dei dati a fini di propaganda siano compatibili con gli scopi principali perseguiti dall'associazione o altro organismo;
- sia prevista specificamente nell'informativa resa agli iscritti al momento dell'adesione o del suo rinnovo.

5. Dati acquisiti nell'esercizio di un mandato.

I titolari di alcune cariche elettive, nel corso del mandato e sulla base di specifiche disposizioni volte a favorire il suo pieno esercizio, possono venire lecitamente a conoscenza di dati personali (cfr., ad esempio, art. 37 d.lg. 18 agosto 2000, n. 267: cfr. anche parere del 20 maggio 1998, in *Bollettino* n. 4, pag. 7 s. e del 7 marzo 2001, in *Bollettino* n. 18, p. 24) da utilizzare, anche a fini di trasparenza e buon andamento, per scopi pertinenti all'esercizio del mandato che possono rendere legittimo anche un eventuale contatto con gli interessati.

È in questo quadro illegittima l'eventuale richiesta di ottenere dagli uffici dell'amministrazione o dell'ente la comunicazione di intere basi di dati, oppure la formazione di appositi elenchi "dedicati" da utilizzare per la propaganda anche dopo la scadenza dal mandato.

Possono al contrario essere utilizzati i dati personali raccolti direttamente dal titolare della carica elettiva, nel quadro delle relazioni interpersonali con cittadini ed elettori.

6. Uso di dati raccolti da terzi.

Diversi interessati divengono consapevoli solo a seguito di una loro contestazione che il consenso espresso in precedenza in modo generico è stato utilizzato anche per attività di propaganda elettorale.

Il candidato o l'organismo politico, quando acquisisce i dati da un privato che li ha raccolti in base a formule di consenso vaghe, riferite a scopi di vario tipo non meglio precisati (spesso, prevalentemente di tipo commerciale), ha l'onere di verificare in modo adeguato –anche con modalità a campione e avvalendosi della figura del mandatario elettorale: cfr. art. 7 l. 10 dicembre 1993, n. 515– che gli interessati siano stati informati in modo specifico e abbiano prestato un consenso idoneo, che è validamente espresso solo se è manifestato *"specificamente in riferimento ad un trattamento chiaramente individuato ... e se sono state rese all'interessato le informazioni di cui all'articolo 13"* del Codice (art. 23, comma 3, d.lg. n. 196/2003).

Tale consenso deve essere manifestato liberamente, in forma differenziata rispetto alla prestazione di beni e servizi, in modo esplicito e documentato per iscritto: altrimenti, il trattamento è illecito e i dati sono inutilizzabili (art. 11, comma 2, d.lg. n. 196/2003).

Sull'organismo politico o candidato grava altresì l'onere di verificare –anche avvalendosi del predetto mandatario– che l'informativa sia fornita in caso di servizi di propaganda curati da terzi che inviino lettere o messaggi di propaganda utilizzando fonti conoscitive accessibili a chiunque.

7. Informativa agli interessati.

Chi effettua attività di propaganda elettorale, anche se utilizza dati "pubblici" nel senso proprio del termine, deve fornire agli interessati la prevista informativa (art. 13 d.lg. n. 196/2003).

Si può adempiere a tale obbligo anche attraverso un'informazione sintetica, ma efficace, ed utilizzando, a titolo esemplificativo, una formula di tenore analogo al seguente:

> *"I dati che ci ha fornito liberamente (oppure: che sono stati estratti da ...) sono utilizzati da ... solo a fini di propaganda elettorale, anche con strumenti informatici, e non saranno comunicati a terzi (eventuale: salvo che all'organizzazione che cura le spedizioni). Può in ogni momento accedere ai dati, opporsi al loro trattamento o chiedere di integrarli, rettificarli o cancellarli, rivolgendosi a ... (indicare almeno un responsabile del trattamento, se è stato designato)".*

Questa informativa deve essere inserita nel materiale di propaganda caratterizzato da lettere o da messaggi di posta elettronica.

Analoghe formule sintetiche possono essere utilizzate in caso di chiamate a numeri estratti da elenchi telefonici, fornendo all'inizio della conversazione un'informativa che indichi subito chi effettua la propaganda, la finalità della chiamata e i diritti del ricevente.

Chi effettua propaganda, qualora non ritenga di inviare il predetto materiale potrebbe:
- estrarre i dati da pubblici registri, elenchi, atti o altri documenti conoscibili da chiunque senza contattare tutti gli interessati;
- oppure, potrebbe inviare materiale propagandistico di dimensioni ridotte che, a differenza di una lettera o di un messaggio di posta elettronica, non permetta di inserire efficacemente un'idonea informativa anche di tenore sintetico.

Limitatamente a questi ultimi due casi, il Garante ritiene proporzionato rispetto ai diritti degli interessati sollevare il soggetto che utilizza i dati per esclusivi fini di propaganda elettorale dall'obbligo di fornire l'informativa. Ciò solo per le consultazioni della primavera del 2004 conformemente a quanto già provveduto con il provvedimento del 7 febbraio 2001 (in *Gazzetta Ufficiale* n. 36 del 13 febbraio 2001, p. 65).

Questa misura evita anche che in un breve arco di tempo un alto numero di interessati riceva un elevato numero di informative analoghe da parte di più soggetti impegnati nella campagna elettorale e che utilizzano le medesime fonti conoscitive, in particolare le liste elettorali comunali.

La disciplina applicabile (art. 13, commi 4 e 5, lett. c), del d.lg. n. 196/2003) affida al Garante il compito di verificare se l'informativa comporti un impiego di mezzi sproporzionato rispetto al diritto tutelato, considerata la possibilità di prescrivere altre misure appropriate. La manifesta sproporzione può ravvisarsi caso per caso o in relazione a settori generali o tipi di trattamento.

Nel caso dell'attività di propaganda elettorale oggetto del presente provvedimento, l'integrale adempimento agli obblighi di informativa agli interessati può essere considerato sproporzionato rispetto al diritto tutelato, quando la persona cui si riferiscono i dati estratti da fonti pubbliche accessibili a chiunque non è contattata da chi utilizza i dati, oppure riceve materiale di propaganda che non permette un agevole inserimento dell'informativa.

Nel caso in cui, invece, l'interessato è contattato mediante l'invio di lettere, oppure di messaggi per posta elettronica, l'informativa – secondo la predetta formula – può essere inserita nella lettera o nel messaggio, anziché essere inviata all'atto della registrazione "interna" dei dati.

Resta fermo l'obbligo di informativa nel caso in cui i dati siano acquisiti direttamente presso l'interessato, anziché da fonti pubbliche conoscibili da chiunque.

8. MISURE DI SICUREZZA ED ALTRI ADEMPIMENTI.

Ciascun partito, movimento o comitato elettorale, nonostante non debba notificare al Garante il trattamento dei dati (cfr. artt. 37 e 38 d.lg. n. 196/2003), è tenuto, oltre che agli adempimenti di cui agli artt. 29 e 30 del Codice in ordine all'individuazione e alla designazione degli incaricati del trattamento e degli eventuali responsabili, ad adottare idonee misure di sicurezza per i trattamenti di dati cartacei e automatizzati e, comunque, quelle "minime" (artt. 31, 33, 34, 35 e allegato B) del d.lg. n. 196).

Restano ferme le specifiche prescrizioni che limitano la propaganda elettorale per talune consultazioni dopo la chiusura della campagna elettorale (v., ad esempio, art. 2 l. n. 515/1993).

9. GARANZIE PER GLI INTERESSATI.

La possibilità che l'interessato non debba acconsentire all'uso dei dati per finalità di propaganda elettorale, o possa non ricevere alle condizioni sopra indicate un'apposita informativa, non lo priva delle garanzie previste dal Codice come quella di chiedere al titolare del trattamento se vi sono dati che lo riguardano, di conoscerne il contenuto in modo intelligibile, l'origine, ecc.

L'interessato può opporsi in ogni momento al trattamento dei dati e, in particolare, alla propaganda, anche quando abbia manifestato un consenso.

Tali richieste obbligano i titolari del trattamento a darvi riscontro e, in caso di opposizione, a non recapitare più all'opponente ulteriori messaggi anche in occasione di successive campagne.

Qualora il titolare di trattamento non fornisca un riscontro idoneo ad una richiesta di esercizio dei diritti di cui al predetto art. 7, l'interessato può rivolgersi all'autorità giudiziaria o presentare un reclamo o un ricorso al Garante con le modalità previste dagli artt. 142 s. del d.lg. n. 196/2003.

10. USO DEI DATI DECORSO IL PERIODO DI ESONERO.

Decorsa la data del 30 giugno 2004, partiti, movimenti politici, comitati promotori, sostenitori e candidati potranno continuare a trattare (anche mediante mera conservazione) i dati estratti da fonti pubbliche accessibili a chiunque per finalità di propaganda elettorale o di connessa comunicazione politica, solo se informeranno gli interessati entro il 30 settembre 2004 nei modi previsti dall'art. 13 del Codice. Diversamente, i dati dovranno essere cancellati o distrutti non oltre la medesima data. Tali considerazioni non riguardano dati per i quali gli interessati siano stati invece informati nei termini sopra indicati.

TUTTO CIÒ PREMESSO IL GARANTE:

a) segnala ai titolari di trattamento interessati, ai sensi dell'art. 154, comma 1, lett. c), del d.lg. n. 196/2003, la necessità di conformare il trattamento ai principi richiamati nel presente provvedimento;

b) ai sensi dell'art. 13, comma 5, del d.lg. n. 196/2003, dispone che partiti e movimenti politici, comitati promotori, sostenitori e candidati i quali trattino dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque per esclusive finalità di propaganda elettorale e di connessa comunicazione politica in occasione delle consultazioni elettorali del primo semestre del 2004, possano astenersi dall'informare gli interessati alle condizioni indicate in motivazione;

c) dispone che il presente provvedimento sia pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana.

Roma, 12 febbraio 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Santaniello
Paissan

IL SEGRETARIO GENERALE
Buttarelli

62 Casi da sottrarre all'obbligo di notificazione al Garante (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

In data odierna, in presenza del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

VISTO l'art. 37, commi 1 e 2, del d.lg. 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali;

RILEVATO che tale Codice indica i trattamenti di dati da notificare al Garante e demanda a questa Autorità il compito di individuare, tra essi, quelli sottratti all'obbligo di notificazione purché non suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato in ragione delle modalità di trattamento o della natura dei dati (art. 37, comma 1);

RILEVATO che il medesimo Codice demanda altresì al Garante il compito di individuare ulteriori trattamenti in aggiunta a quelli elencati nella predetta disposizione;

VISTA la documentazione in atti;

RILEVATO in sede di prima applicazione del Codice che taluni trattamenti sono effettuati con modalità che permettono, allo stato, di sottrarli all'obbligo di notificazione, ferma restando l'osservanza degli ulteriori principi ed obblighi previsti dal Codice in materia di protezione dei dati personali;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il Prof. Stefano Rodotà;

DELIBERA:

A) di sottrarre all'obbligo di notificazione al Garante, tra i casi previsti dall'art. 37, comma 1, del d.lg. 30 giugno 2003, n. 196:

1) con riferimento ai casi di cui al comma 1, lett. a) di tale disposizione:
   a) i trattamenti non sistematici di dati genetici o biometrici effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica. Ciò limitatamente ai dati e alle operazioni, compresa la comunicazione, indispensabili per perseguire finalità di tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;
   b) i trattamenti di dati genetici o biometrici effettuati nell'esercizio della professione di avvocato, in relazione alle operazioni e ai dati necessari per svolgere le investigazioni difensive di cui alla legge n. 397/2000, o comunque per far valere o difendere un diritto anche da parte di un terzo in sede giudiziaria. Ciò sempre che il diritto sia di rango almeno pari a quello dell'interessato e i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
   c) i trattamenti di dati che indicano la posizione geografica di mezzi di trasporto aereo, navale e terrestre, effettuati esclusivamente a fini di sicurezza del trasporto;

2) con riferimento ai casi di cui al comma 1, lett. b) della medesima disposizione, i

(*) Deliberazione n. 1 del 31 marzo 2004, in *Gazzetta Ufficiale* del 6 aprile 2004, n. 81

trattamenti di dati idonei a rivelare lo stato di salute e la vita sessuale effettuati da esercenti le professioni sanitarie, anche unitamente ad altri esercenti titolari dei medesimi trattamenti:

a) a fini di procreazione assistita, di trapianto di organi e tessuti, indagine epidemiologica, rilevazione di malattie mentali, infettive, diffusive o di sieropositività. Ciò sempre che i trattamenti siano effettuati non sistematicamente, rispetto a dati non organizzati in una banca di dati accessibile a terzi per via telematica e limitatamente ai dati e alle operazioni indispensabili per la tutela della salute o dell'incolumità fisica dell'interessato o di un terzo;

b) ad esclusivi fini di monitoraggio della spesa sanitaria o di adempimento di obblighi normativi in materia di igiene e sicurezza del lavoro e della popolazione;

3) con riferimento ai casi di cui al comma 1, lett. c), i trattamenti di dati idonei a rivelare la sfera psichica di lavoratori:

a) effettuati da associazioni, enti od organismi a carattere sindacale per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di rapporto di lavoro o di previdenza, anche in tema di diritto al lavoro dei disabili;

b) effettuati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico o religioso riguardo a dati di propri dipendenti o collaboratori, per adempiere esclusivamente a specifici obblighi previsti dalla normativa in materia di rapporto di lavoro o di previdenza;

4) con riferimento ai casi di cui al comma 1, lett. d), i trattamenti di dati personali:

a) che non siano fondati unicamente su un trattamento automatizzato volto a definire profili professionali, effettuati per esclusive finalità di occupazione o di gestione del rapporto di lavoro, fuori dei casi di cui alla lettera e) del medesimo art. 37, comma 1;

b) che non siano fondati unicamente su un trattamento automatizzato volto a definire il profilo di un investitore, effettuati esclusivamente per adempiere a specifici obblighi previsti dalla normativa in materia di intermediazione finanziaria;

c) relativi all'utilizzo di marcatori elettronici o di dispositivi analoghi installati, oppure memorizzati temporaneamente, e non persistenti, presso l'apparecchiatura terminale di un utente, consistenti nella sola trasmissione di identificativi di sessione in conformità alla disciplina applicabile, all'esclusivo fine di agevolare l'accesso ai contenuti di un sito Internet;

5) con riferimento ai casi di cui al comma 1, lett. e), i trattamenti di dati sensibili effettuati:

a) al solo fine di selezione di personale per conto esclusivamente di soggetti appartenenti al medesimo gruppo bancario o societario;

b) da soggetti pubblici per adempiere esclusivamente a specifici obblighi o compiti previsti dalla normativa in materia di occupazione e mercato del lavoro;

c) da associazioni o organizzazioni di categoria al solo fine di svolgere ricerche campionarie relativamente a dati riguardanti l'adesione alla medesima associazione o organizzazione;

6) con riferimento ai casi di cui al comma 1, lett. f), i trattamenti di dati personali:

a) effettuati da soggetti pubblici per la tenuta di pubblici registri o elenchi conoscibili da chiunque;

b) registrati in banche di dati utilizzate in rapporti con l'interessato di fornitura di beni, prestazioni o servizi, o per adempimenti contabili o fiscali, anche in caso di inadempimenti contrattuali, azioni di recupero del credito e contenzioso con l'interessato;

c) registrati in banche di dati utilizzate da soggetti pubblici o privati per adempiere esclusivamente ad obblighi normativi in materia di rapporto di lavoro, previdenza o assistenza;

d) registrati in banche di dati utilizzate da soggetti pubblici al solo fine della

tenuta ed esecuzione di atti, provvedimenti e documenti, in tema di riscossione di tributi, applicazione di sanzioni amministrative, o rilascio di licenze, concessioni o autorizzazioni;

e) relativi a immagini o suoni conservati temporaneamente per esclusive finalità di sicurezza o di tutela delle persone o del patrimonio;

f) trattati, in base alla legge, dai soggetti autorizzati in relazione alle operazioni e ai dati necessari all'esclusivo fine di prestare l'attività di garanzia collettiva dei fidi e i servizi a essa connessi o strumentali ("confidi");

B) di inviare copia della presente deliberazione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia ai fini della sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 31 marzo 2004

IL PRESIDENTE
Rodotà

IL RELATORE
Rodotà

IL SEGRETARIO GENERALE
Buttarelli

IX - Unione europea

63 Direttiva 2003/98/CE del Parlamento europeo e del Consiglio del 17 novembre 2003, relativa al riutilizzo dell'informazione nel settore pubblico (*)

L 345/90 IT Gazzetta ufficiale dell'Unione europea 31.12.2003

DIRETTIVA 2003/98/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 17 novembre 2003
relativa al riutilizzo dell'informazione del settore pubblico

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 95,

vista la proposta della Commissione (1),

visto il parere del Comitato economico e sociale europeo (2),

visto il parere del Comitato delle regioni (3),

deliberando secondo la procedura di cui all'articolo 251 del trattato (4),

considerando quanto segue:

(1) Il trattato prevede l'instaurazione di un mercato interno e l'istituzione di un regime inteso a garantire l'assenza di distorsioni della concorrenza sul mercato interno. L'armonizzazione delle normative e delle prassi seguite negli Stati membri in relazione allo sfruttamento delle informazioni del settore pubblico contribuisce al conseguimento di tali obiettivi.

(2) L'evoluzione verso la società dell'informazione e della conoscenza incide sulla vita di ogni cittadino della Comunità, consentendogli, tra l'altro, di ottenere nuove vie di accesso alle conoscenze e di acquisizione delle stesse.

(3) In tale evoluzione i contenuti digitali svolgono un ruolo importante. La produzione di contenuti ha comportato negli ultimi anni la rapida creazione di posti di lavoro e continua ad agire in questo senso. Nella maggior parte dei casi i posti di lavoro vengono creati nel contesto di piccole imprese emergenti.

(4) Il settore pubblico raccoglie, produce, riproduce e diffonde un'ampia gamma di informazioni in molti settori di attività, ad esempio informazioni di tipo sociale, economico, geografico, climatico, turistico, informazioni in materia di affari, di brevetti e di istruzione.

(5) Uno degli obiettivi principali della realizzazione del mercato interno è la creazione di condizioni propizie allo sviluppo di servizi su scala comunitaria. Le informazioni del settore pubblico sono un'importante materia prima per i prodotti e i servizi imperniati sui contenuti digitali. Esse diventeranno una risorsa contenutistica ancora più importante con lo sviluppo dei servizi di contenuti via comunicazioni mobili. In tale contesto sarà fondamentale anche un'ampia copertura geografica oltre i confini nazionali. Più ampie possibilità di riutilizzo delle informazioni del settore pubblico dovrebbero, tra l'altro, consentire alle imprese europee di sfruttarne il potenziale e contribuire alla crescita economica e alla creazione di posti di lavoro.

(6) Le normative e le prassi seguite negli Stati membri in relazione allo sfruttamento delle risorse di informazione del settore pubblico sono caratterizzate da notevoli differenze costituenti delle barriere che impediscono a queste risorse essenziali di esprimere appieno il proprio potenziale economico. Le tradizioni degli enti pubblici in materia di utilizzazione delle informazioni del settore pubblico si sono sviluppate in direzioni molto diverse e di questo occorrerebbe tener conto. Sarebbe opportuno quindi avviare un'armonizzazione minima delle normative e delle prassi nazionali relative al riutilizzo dei documenti del settore pubblico, nei casi in cui le differenze tra dette normative e prassi nazionali o la mancanza di chiarezza ostacolano il buon funzionamento del mercato interno e l'adeguato sviluppo della società dell'informazione nella Comunità.

(7) In assenza di un'armonizzazione minima a livello comunitario, inoltre, l'attività legislativa nazionale, già avviata in vari Stati membri in risposta alla sfide tecnologiche, potrebbe determinare soluzioni normative ancora più discordanti. Con l'ulteriore sviluppo della società dell'informazione, che ha già prodotto un notevole incremento dello sfruttamento delle informazioni oltre i confini nazionali, si accentueranno le conseguenze di tali differenze e incertezze sul piano legislativo.

(8) Affinché il riutilizzo dei documenti del settore pubblico avvenga in condizioni eque, adeguate e non discriminatorie, le modalità di tale riutilizzo devono essere soggette ad una disciplina generale. Gli enti pubblici raccolgono, producono, riproducono e diffondono documenti in adempimento dei loro compiti di servizio pubblico. L'uso di tali documenti per altri motivi costituisce riutilizzo. Le politiche degli Stati membri possono spingersi oltre le norme minime stabilite dalla presente direttiva, consentendo un più ampio riutilizzo.

(1) GU C 227 E del 24.9.2002, pag. 382.
(2) GU C 85 dell'8.4.2003, pag. 25.
(3) GU C 73 del 26.3.2003, pag. 38.
(4) Parere del Parlamento europeo del 12 febbraio 2003 (non ancora pubblicato nella Gazzetta ufficiale), posizione comune del Consiglio del 26 maggio 2003 (GU C 159 E dell'8.7.2003, pag. 1) e posizione del Parlamento europeo del 25 settembre 2003 (non ancora pubblicata nella Gazzetta ufficiale). Decisione del Consiglio del 27 ottobre 2003.

(*) Prima pagina del documento, rinvenibile in *Gazzetta Ufficiale dell'Unione europea* del 31 dicembre 2003, L 350/90. www.europa.eu.int/eur-lex/

64 Relazione della Commissione. Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) (*)

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 15.5.2003
COM(2003) 265 definitivo

RELAZIONE DELLA COMMISSIONE

Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE)

INDICE

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /eur-lex/pri/it/dpi/rpt /doc/2003 /com2003_0265it01.doc

65 EC Study on Implementation of Data Protection Directive. Comparative Summary of National Laws (*)

EC STUDY ON IMPLEMENTATION OF DATA PROTECTION DIRECTIVE
(Study Contract ETD/2001/B5-3001/A/49)

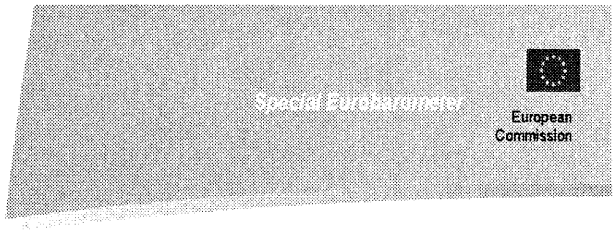
comparative summary of national laws

Human Rights Centre
University of Essex
Colchester (UK)

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/lawreport /consultation /univessex-comparativestudy_en.pdf

Cambridge (UK) September 2002

66 Eurobarometro - Data Protection (*)



EUROBAROMETER

DATA PROTECTION

Fieldwork: September 2003

Publication: December 2003

Special Eurobarometer 196 – Wave 60.0 – European Opinion Research Group EEIG

This survey was requested by Directorate General Internal Market, Unit E4 - Media and data protection - and coordinated by Directorate General Press and Communication

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/public_opinion /archives/ebs /ebs_196_data_protection.pdf

67 Eurobarometro - Data Protection in the European Union (*)

EUROBAROMETER

Flash Eurobarometer

European Commission

Flash Eurobarometer 147 - Taylor Nelson Sofres Coordination – EOS Gallup Europe

Data Protection in the European Union

Fieldwork 15 September - 03 October 2003

Publication December 2003

This survey was requested by Directorate General "Internal Market" and coordinated by Directorate General Press and Communication

This document does not represent the point of view of the European Commission. The interpretations and opinions contained in it are solely those of the authors.

(*) Prima pagina del documento, rinvenibile in http://europa.eu.int/eur-lex/pri/it/oj/dat/2003/l_308/l_30820031125it00270028.pdf

68 Decisione della Commissione, del 21 novembre 2003, sulla adeguata protezione dei dati personali in Guernsey (2003/821/CE) (*)

[notificata con il numero C(2003) 4309]
(Testo rilevante ai fini del SEE)
(2003/821/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], e in particolare l'articolo 25, paragrafo 6, della medesima, consultato il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali [2], considerando quanto segue:

(1) Ai sensi della direttiva 95/46/CE gli Stati membri devono far sì che il trasferimento di dati personali a un paese terzo abbia luogo solo se il paese in questione garantisce adeguati livelli di tutela e dopo aver accertato, prima del trasferimento, che siano soddisfatte le norme degli Stati membri che attuano altre disposizioni della direttiva.

(2) La Commissione può accertare che un paese terzo garantisce adeguati livelli di tutela. In tal caso, gli Stati membri possono trasferirvi dati personali senza la necessità di ulteriori garanzie.

(3) Secondo la direttiva 95/46/CE il livello di tutela dei dati va accertato alla luce di tutte le circostanze che accompagnano la, o le, operazioni di trasferimento dei dati, dando particolare rilievo agli elementi del trasferimento di cui all'articolo 25, paragrafo 2 della medesima.

(4) Data la diversità degli approcci alla tutela dei dati nei paesi terzi, la valutazione dell'adeguatezza va effettuata - e ogni decisione ai sensi dell'articolo 25, paragrafo 6 della direttiva 95/46/CE va presa e applicata - senza discriminazioni ingiustificate o arbitrarie contro o tra paesi terzi in cui esistono condizioni simili e senza creare ostacoli mascherati al libero scambio, nel rispetto degli attuali impegni internazionali assunti dalla Comunità.

(5) Il Baliato (Bailiwick) di Guernsey è una dipendenza della Corona britannica (senza essere una zona del Regno Unito né una colonia) ma completamente indipendente, tranne che per le relazioni internazionali e la difesa, di competenza del governo britannico; il Baliato di Guernsey va dunque considerato un paese terzo ai fini della direttiva.

(6) Dall'agosto 1987, la ratifica, da parte del Regno Unito, della convenzione del Consiglio d'Europa sulla tutela delle persone con riguardo al trattamento automatico dei dati personali (Convenzione n. 108), è stata estesa al Baliato di Guernsey.

(7) Nel Baliato di Guernsey, le norme giuridiche a tutela dei dati personali, basate sulle norme della direttiva 95/46/CE, sono regolate dalla Data Protection (Bailiwick of Guernsey) Law, 2001, entrata in vigore il 1° agosto 2002.

(8) Nel 2002, Guernsey ha anche approvato altri sedici strumenti normativi (Orders) che regolano questioni specifiche come l'accesso dei titolari dei dati, l'elaborazione dei dati sensibili e la notifica all'autorità di protezione dei dati. Tali strumenti completano la legge suddetta.

(*) *Gazzetta Ufficiale dell' Unione europea* del 25 novembre 2003, n. L 308, p. 27-28

(1) G.U. 23 novembre 1995, n. L 281, p. 31

(2) Parere 5/2003 sul livello di protezione dei dati personali a Guernsey, adottato dal Gruppo di lavoro in data 13 giugno 2003, disponibile presso: http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm

(9) Le norme giuridiche applicabili in Guernsey contengono tutti i principi di un adeguato livello di tutela delle persone fisiche. La loro applicazione è garantita dal ricorso giurisdizionale e dal controllo indipendente di autorità come il Data Protection Commissioner, dotato di poteri di ricerca e d'intervento.

(10) Si ritiene pertanto che Guernsey fornisca adeguati livelli di tutela dei dati personali ai sensi della direttiva 95/46/CE.

(11) Per salvaguardare la trasparenza e la capacità delle competenti autorità degli Stati membri di garantire la tutela delle persone riguardo all'elaborazione dei dati personali di quest'ultime, vanno precisate le circostanze eccezionali che giustificano la sospensione di particolari flussi di dati, nonostante l'esistenza di un'adeguata tutela.

(12) Le misure di cui alla presente decisione sono conformi al parere del Comitato istituito ai sensi dell'articolo 31, paragrafo 1, della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Per le finalità di cui all'articolo 25, paragrafo 2, della direttiva 95/46/CE, il Baliato di Guernsey è ritenuto fornire un livello adeguato di tutela dei dati personali trasferiti dalla Comunità.

Articolo 2

Questa decisione riguarda l'adeguatezza della tutela fornita a Guernsey rispetto ai requisiti dell'articolo 25, paragrafo 1, della direttiva 95/46/CE e non influisce su altre condizioni o restrizioni cui possa dar luogo l'attuazione di altre disposizioni della stessa direttiva sull'elaborazione di dati personali in seno agli Stati membri.

Articolo 3

1. A prescindere dai loro poteri di intervento per conformarsi a disposizioni nazionali approvate ai sensi di norme diverse dall'articolo 25 della direttiva 95/46/CE, per proteggere le persone riguardo all'elaborazione dei loro dati personali, le autorità competenti degli Stati membri possono esercitare i loro attuali poteri di sospendere i flussi di dati a un destinatario in Guernsey:

a) se un'autorità competente di Guernsey stabilisce che il destinatario infrange norme di protezione in vigore; oppure

b) se è molto probabile che le norme di protezione siano infrante; se esistono fondati motivi per credere che l'autorità competente di Guernsey non prenda o non prenderà provvedimenti adeguati e tempestivi per comporre il caso in questione; se il persistere del trasferimento dà luogo a rischi imminenti di danno grave ai titolari dei dati e in tale circostanza le autorità competenti nello Stato membro hanno compiuto ragionevoli sforzi per avvisare i responsabili dell'elaborazione in Guernsey e dar loro l'opportunità di rispondere.

2. La sospensione cesserà non appena le norme di protezione siano ripristinate e ne venga informata l'autorità competente dello Stato membro interessato.

Articolo 4

1. Gli Stati membri informano immediatamente la Commissione dei provvedimenti adottati ai sensi dell'articolo 3.

2. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui gli organismi di Guernsey preposti a garantire la rispondenza alle norme di tutela non riescono ad assolvere tale compito.

3. Se le informazioni raccolte ai sensi dell'articolo 3 e dei paragrafi 1 e 2 del presente articolo provano che in Guernsey nessun organo preposto a garantire la rispondenza alle norme di tutela adempie efficacemente il suo ruolo, la Commissione ne informa la competente autorità di Guernsey e, se necessario, propone contromisure ai sensi della procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE al fine di abrogare o sospendere la presente decisione o di limitarne il campo d'applicazione.

Articolo 5

La Commissione controlla il funzionamento della presente decisione e riferisce al comitato di cui all'articolo 31 della direttiva 95/46/CE ogni pertinente conclusione e, in particolare, tutto quanto possa influire sulla constatazione, di cui all'articolo 1 della presente decisione, di adeguatezza della tutela in Guernsey ai sensi dell'articolo 25 della direttiva 95/46/CE ed eventuali prove che la decisione venga attuata in modo discriminatorio.

Articolo 6

Gli Stati membri adottano i provvedimenti necessari a conformarsi alla presente decisione entro quattro mesi dalla data della sua notifica.

Articolo 7

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 21 novembre 2003

Per la Commissione
Frederik Bolkestein
Membro della Commissione

69 Decisione della Commissione, del 30 giugno 2003, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina (2003/490/CE) (*)

(Testo rilevante ai fini del SEE)
(2003/490/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) Conformemente alla direttiva 95/46/CE gli Stati membri sono tenuti ad operare affinché il trasferimento di dati personali verso paesi terzi possa avvenire solo se il paese terzo in questione garantisce un livello adeguato di tutela e se, prima del trasferimento, viene rispettata la legislazione dello Stato membro che attua altre disposizioni della direttiva.

(2) La Commissione può constatare che un paese terzo garantisce un livello adeguato di tutela. In tal caso gli Stati membri vi possono trasferire dati personali senza richiedere ulteriori garanzie.

(3) Conformemente alla direttiva 95/46/CE, il livello di tutela dei dati deve essere valutato tenendo presenti tutte le circostanze in cui si svolgono le operazioni di trasferimento dei dati, con una particolare attenzione per gli aspetti relativi al trasferimento elencati nell'articolo 25, paragrafo 2. Il gruppo di lavoro sulla tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito indicazioni per effettuare tale valutazione [2].

(4) Data la diversità degli approcci alla protezione dei dati nei paesi terzi, è opportuno che la valutazione dell'adeguatezza avvenga e che ogni decisione, basata sull'articolo 25, paragrafo 6 della direttiva 95/46/CE, sia presa ed attuata senza dar luogo a discriminazioni arbitrarie o ingiustificate verso o tra paesi terzi in cui esistono condizioni analoghe e senza costituire una barriera occulta per gli scambi commerciali, visti gli attuali impegni della Comunità a livello internazionale.

(5) Per quanto riguarda l'Argentina, le norme giuridiche relative alla tutela dei dati personali sono state inserite in norme a carattere generale e in norme settoriali, tutte giuridicamente vincolanti.

(6) Le norme a carattere generale sono stabilite dalla costituzione, dalla legge sulla tutela dei dati personali n. 25 326 e dal regolamento approvato con decreto n. 1558/2001 (in prosieguo la "legislazione argentina").

(7) La costituzione argentina prevede un ricorso giurisdizionale speciale relativo alla

(*) *Gazzetta Ufficiale delle Comunità europee* del 5 luglio 2003, n. L 168, p.19-22

(1) *Gazzetta Ufficiale delle Comunità europee* del 23.11.1995, n. L 281. p. 31.

(2) Parere 12/98 adottato dal Gruppo di lavoro il 24 luglio 1998: Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva comunitaria sulla tutela dei dati (DG MARKT D/5025/98), disponibile su Europa, il sito Web della Commissione europea, al seguente indirizzo: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_98.htm

tutela dei dati personali, denominato "habeas data". Si tratta di una sottocategoria della procedura prevista dalla costituzione per la tutela dei diritti costituzionali che eleva quindi la tutela dei dati personali a diritto fondamentale. A norma dell'articolo 43, paragrafo 3 della costituzione argentina, ciascuno ha il diritto, a norma dell'"habeas data" di prendere conoscenza del contenuto di tutti i dati che lo riguardano e della loro finalità, che figurino in banche dati o archivi pubblici, o in quelli privati destinati a fornire dei rapporti informativi. In base a detto articolo, in caso di informazioni false o utilizzate a scopo discriminatorio, l'interessato può richiedere la cancellazione, la correzione, la qualificazione dei dati come riservati o l'aggiornamento dei dati contenuti negli archivi di cui sopra. Tale articolo non concerne la segretezza delle fonti d'informazione giornalistiche. La giurisprudenza argentina riconosce l'"habeas data" come diritto fondamentale e direttamente applicabile.

(8) La legge sulla tutela dei dati personali 25 326 del 4 ottobre 2000 (in prosieguo "la legge") sviluppa ed approfondisce le disposizioni costituzionali. Essa contiene disposizioni relative ai principi generali di tutela dei dati, ai diritti delle persone interessate, agli obblighi dei responsabili del trattamento dei dati e degli utilizzatori, all'autorità o organo di controllo, alle sanzioni e al regolamento interno concernenti il ricorso giurisdizionale all'"habeas data".

(9) Il regolamento approvato con decreto n. 1558/2001 del 3 dicembre 2001 (in prosieguo "il regolamento") stabilisce le modalità d'applicazione della legge, ne completa le disposizioni e chiarisce i punti che possono essere oggetto di interpretazioni divergenti.

(10) La legislazione argentina concerne la tutela dei dati personali registrati in archivi, registri, basi di dati o altri strumenti tecnici gestiti da enti pubblici, così come la tutela dei dati personali registrati in archivi, registri, banche di dati o altri strumenti tecnici gestiti da privati, destinati a fornire dei rapporti informativi. Si tratta degli strumenti non limitati all'uso esclusivamente personale e di quelli destinati alla cessione o al trasferimento dei dati personali, indipendentemente dal fatto che la circolazione dei rapporti o delle informazioni prodotte sia gratuita o a pagamento.

(11) Alcune disposizioni della legge si applicano uniformemente a tutto il territorio nazionale. Si tratta di provvedimenti generali e provvedimenti relativi alla tutela generale dei dati, principi, diritti degli interessati e obblighi dei responsabili del trattamento dei dati e degli utilizzatori di archivi, registri e banche di dati, sanzioni penali, nonché dell'esistenza e delle modalità principali del ricorso giurisdizionale all'"habeas data" definito nella Costituzione.

(12) Altre disposizioni della legge riguardano i registri, gli archivi, le basi o le banche di dati che siano collegati in reti diffuse a livello intergiurisdizionale (ossia "interprovinciale"), nazionale o internazionale e considerati di competenza della giurisdizione federale. Dette disposizioni riguardano il controllo esercitato dalle autorità di controllo, le sanzioni che possono essere imposte dall'autorità di controllo e le norme di procedura che disciplinano il ricorso giurisdizionale in materia di "habeas data". Altri tipi di registri, archivi, basi o banche di dati devono essere considerati di competenza della giurisdizione provinciale. Le province possono emanare disposizioni normative nelle dette materie.

(13) Disposizioni relative alla tutela dei dati figurano anche in numerosi strumenti giuridici relativi a diversi settori, quali le transazioni tramite carta di credito, le statistiche, le operazioni bancarie o la sanità.

(14) La legislazione argentina contempla tutti i principi basilari necessari per un adeguato livello di tutela delle persone fisiche, anche se prevede eccezioni e restrizioni al fine di salvaguardare importanti interessi pubblici. L'applicazione di tali norme è garantita da uno specifico ricorso giurisdizionale, semplificato e veloce, relativo alla tutela dei dati personali, denominato "habeas data", così come dai ricorsi giurisdizionali generali. La legge prevede l'istituzione di un organo di controllo della tutela dei dati incaricato di prendere tutte le misure necessarie al rispetto delle disposizioni e degli obiettivi previsti ed è dotato di poteri d'indagine e d'intervento. Conformemente al regolamento, la Direzione nazionale per la tutela dei dati personali è stata istituita come organo di controllo. La legislazione argentina prevede sanzioni

efficaci e dissuasive, sia amministrative che penali. Inoltre le disposizioni della legislazione argentina concernenti la responsabilità civile (contrattuale ed extra-contrattuale) sono applicate in caso di trattamento illegale dei dati che reca pregiudizio alle persone interessate.

(15) Il governo argentino ha fornito spiegazioni e garanzie relative all'interpretazione della legislazione argentina ed ha assicurato che le norme concernenti la tutela dei dati sono applicate conformemente a tale interpretazione. La presente decisione si basa su tali spiegazioni e garanzie, dalle quali di conseguenza dipende. La presente decisione si riferisce segnatamente alle spiegazioni e alle garanzie fornite dalle autorità argentine in merito all'interpretazione della legislazione argentina, nonché alle situazioni che rientrano nel campo d'applicazione della legislazione argentina relativa alla tutela dei dati.

(16) Si ritiene pertanto che l'Argentina fornisca un adeguato livello di tutela dei dati personali di cui alla direttiva 95/46/CE.

(17) Nell'interesse della trasparenza e al fine di salvaguardare la capacità delle autorità competenti negli Stati membri di garantire la tutela delle persone fisiche per quanto concerne il trattamento dei dati personali che li riguardano, è necessario specificare nella decisione le circostanze eccezionali in cui, nonostante la constatazione di un livello di protezione adeguato, può essere giustificata la sospensione di trasferimenti di dati specifici.

(18) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito un parere sul livello di protezione dei dati personali in Argentina di cui si è tenuto conto nella preparazione della presente decisione [3].

(19) Le misure previste dalla presente decisione sono conformi al parere del comitato di cui all'articolo 31, paragrafo 1 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, si ritiene che l'Argentina fornisca un adeguato livello di tutela dei dati personali trasferiti dalla Comunità.

Articolo 2

La presente decisione riguarda soltanto l'adeguatezza della protezione fornita in Argentina al fine di soddisfare i requisiti di cui all'articolo 25, paragrafo 1 della direttiva 95/46/CE e non produce alcun effetto su altre condizioni o restrizioni conseguenti all'attuazione di altre disposizioni della direttiva riguardanti il trattamento dei dati personali all'interno degli Stati membri.

Articolo 3

1. Fatti salvi i poteri di intervento al fine di garantire il rispetto dei provvedimenti nazionali adottati in applicazione di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri hanno facoltà di sospendere i trasferimenti di dati verso destinatari in Argentina, al fine di proteggere i cittadini nell'ambito del trattamento dei loro dati personali nei casi in cui:

a) un'autorità competente argentina abbia constatato che il destinatario non rispetta le norme applicabili relative alla protezione;

b) sia fortemente probabile una violazione delle norme relative alla protezione; vi siano motivi ragionevoli di ritenere che le autorità competenti argentine non adottino o non intendano adottare misure adeguate e tempestive per risolvere il caso in questione; la continuazione del trasferimento dei dati comporti un rischio imminente di grave pregiudizio per le persone interessate e le autorità competenti degli Stati membri abbiano fatto il possibile, date le circostanze, per avvertire il responsabile del trattamento in Argentina e dargli la possibilità di replicare.

(3) Parere 4/2002 sul livello di protezione dei dati personali in Argentina - WP 63 del 3 ottobre 2002 disponibile al seguente indirizzo: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

La sospensione cessa non appena sia garantito il rispetto delle norme di protezione e ne sia informata l'autorità competente della Comunità.

2. Gli Stati membri informano immediatamente la Commissione dell'adozione di provvedimenti in base al paragrafo 1.

3. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui l'azione degli organismi argentini responsabili per il rispetto delle norme di protezione non sia sufficiente a garantire tale rispetto.

4. Ove risulti provato, dalle informazioni di cui ai paragrafi 1, 2 e 3, che gli organismi argentini incaricati di garantire il rispetto delle norme di protezione non svolgono la loro funzione in modo efficace, la Commissione avverte le autorità argentine competenti e, se necessario, presenta progetti di misure, con la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di abrogare o sospendere la presente decisione o di limitarne il campo d'applicazione.

Articolo 4

1. La presente decisione può essere modificata in qualsiasi momento, per tener conto delle esperienze relative alla sua applicazione o di cambiamenti intervenuti nella legislazione argentina, nella sua applicazione ed interpretazione.

La Commissione verifica l'applicazione della presente decisione e comunica qualsiasi informazione utile al comitato istituito dall'articolo 31 della direttiva 95/46/CE, in particolare ogni elemento rilevante ai fini della valutazione di cui all'articolo 1 della presente decisione circa l'adeguatezza della protezione argentina ai sensi dell'articolo 25 della direttiva 95/46/CE e ogni elemento che dimostri che la presente decisione è applicata in modo discriminatorio.

2. Se necessario, la Commissione presenta progetti di misure con la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE.

Articolo 5

Gli Stati membri adottano le misure necessarie per conformarsi alla presente decisione entro centoventi giorni dalla notifica della stessa.

Articolo 6

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 30 giugno 2003

Per la Commissione
Frederik Bolkestein
Membro della Commissione

70 Risoluzione del Parlamento europeo sul trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici (*)

P5_TA(2003)0097
B5-0187/2003

Trasmissione dei dati personali da parte delle compagnie aeree in occasione di voli transatlantici

Il Parlamento europeo,

– visti la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonchè alla libera circolazione di tali dati [1] e il regolamento del Consiglio CEE n. 2299/89 del 24 luglio 1989 su un codice di condotta per i sistemi telematici di prenotazione [2],

A. consapevole del fatto che dopo l'11 settembre 2001 gli Stati Uniti hanno riformato profondamente la legislazione al fine di garantire la propria sicurezza interna anche nel settore dei trasporti e che, il 19 novembre 2001, hanno adottato "l'Aviation and Transportation Security Act (ATSA)" [3], e il 5 maggio 2002 "l'Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV)"4 nonché altre misure connesse che riguardano, per i soli voli transatlantici, circa 10/11 milioni di passeggeri l'anno,

B. considerando che inizialmente l'amministrazione degli Stati Uniti si era limitata a richiedere alle compagnie aeree la trasmissione dei dati relativi ai passeggeri e ai membri dell'equipaggio ("Passenger Manifest Information") (nota finale1) attraverso "l'Advance Passenger Information System (APIS)", che in seguito

[...]

(*) Prima pagina del documento, rinvenibile in www3.europarl.eu.int /omk/omnsapir.so /calendar?APP=PDF&TYPE= PV2&FILE=P5_TA(20030313) 0097it.pdf&LANGUE=IT

(1) GU L 281 del 23.11.1995, pag. 31.

(2) GU L 220 del 29.7.1989, pag. 1.

(3) "Aviation and Transportation Security Act" del 19 novembre 2001 (107-71), norme provvisorie del Dipartimento del tesoro (dogane) - dati relativi a passeggeri e equipaggi richiesti per i voli passeggeri nel trasporto aereo dall'estero verso gli Stati Uniti (registro federale, 31 dicembre 2001) e trasmissione del registro dei nomi dei passeggeri richiesta per i passeggeri di voli internazionali da o verso gli Stati Uniti (registro federale, 25 giugno 2002).

71 Risoluzione del Parlamento europeo sul trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici: stato dei negoziati con gli Stati Uniti (*)

P5_TA(2003)0429
B5-0411/2003

Trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici

Il Parlamento europeo,
– visto l'articolo 42, paragrafo 5, del suo regolamento,

A. considerando la sua risoluzione del 13 marzo 2003 sulla trasmissione di dati personali da parte delle compagnie aeree in occasione di voli transatlantici1,

B. considerando che, dopo l'11 settembre 2001, gli USA hanno attuato differenti misure volte a rafforzare i controlli alle proprie frontiere; rilevando, in particolare, che dal 1° ottobre 2003 soltanto i passeggeri provvisti di un "passaporto leggibile a macchina" possono entrare senza visto e che nel prossimo futuro i passeggeri dovranno presentare un passaporto contenente dati biometrici,

C. considerando le verifiche svolte dalla Commissione nel corso degli ultimi mesi, sia a livello amministrativo che politico, al fine di accertare se le misure adottate e previste dalle autorità statunitensi garantiscono un'adeguata protezione dei dati, in conformità delle disposizioni della direttiva 95/46/CE2 nonché dei principi sanciti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dalla Carta dei diritti fondamentali dell'Unione europea,

D. considerando le informazioni fornite dalla Commissione e il fatto che attualmente non è possibile ritenere adeguata la protezioni dei dati assicurata dalle autorità statunitensi perché:

(a) l'obiettivo che giustificherebbe l'acquisizione e la conservazione dei dati permane oscuro e non è limitato alla lotta contro il terrorismo; di conseguenza, sussiste il rischio che i dati possano essere utilizzati per altri scopi, ivi compreso il loro trasferimento ad altri servizi dell'amministrazione statunitense oppure a terzi,
(b) il numero di dati richiesti (39 elementi diversi del codice di prenotazione del passeggero) appare eccessivo ed è in ogni caso sproporzionato rispetto all'obiettivo perseguito,
(c) la conservazione dei dati (6/7 anni) appare ingiustificata, in particolare rispetto ai dati riguardanti persone che non costituiscono una minaccia per la sicurezza del

[...]

(*) Prima pagina del documento, rinvenibile in www3.europarl.eu.int /omk/omnsapir.so /calendar?APP=PDF&TYPE=PV2&FILE=P5_TA(20031009)0429it.pdf&LANGUE=IT

72 Risoluzione del Parlamento europeo sulla prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) del 9 marzo 2004 (COM(2003) 265 - C5-0375/2003 - 2003/2153(INI)) (*)

P5_TA-PROV(2004)0141
A5-0104/2004

Il Parlamento europeo,

- vista la Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) (COM(2003) 265 - C5-0375/2003),

- visti i testi di diritto internazionale a tutela del diritto alla vita privata e, in particolare, l'articolo 12 della dichiarazione universale dei diritti dell'uomo del 10 dicembre 1948, l'articolo 17 del patto internazionale relativo ai diritti civili e politici del 16 dicembre 1966, l'articolo 8 della convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950(1), la convenzione per la protezione delle persone rispetto al trattamento automatico dei personali del 28 gennaio 1981(2) e le raccomandazioni adottate dal Consiglio d'Europa,

- visti l'articolo 6 del trattato UE sul rispetto dei diritti dell'uomo e delle libertà fondamentali nell'Unione, l'articolo 286 del trattato CE, nonché gli articoli 7 e 8 della Carta europea dei diritti fondamentali dell'Unione dedicati rispettivamente al rispetto della vita privata e della vita familiare e alla protezione dei dati di carattere personale,

- viste le disposizioni del diritto comunitario a tutela del diritto alla vita privata e alla protezione dei dati, in particolare la direttiva 95/46/CE, 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati(3), e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)(4),

- visti gli altri strumenti UE relativi alla protezione dei dati nell'ambito del terzo pilastro, in particolare il progetto di documento di lavoro della Presidenza greca su norme comuni per la protezione dei dati personali nel quadro del terzo pilastro e l'annuncio del Commissario Vitorino relativo alla presentazione, nel 2004, di uno strumento giuridico in proposito(5),

- visti i pareri del gruppo di lavoro sulla privacy istituito dall'articolo 29 della direttiva 95/46/CE (gruppo 'Articolo 29'),

[...]

(*) Prima pagina del documento, rinvenibile in www3.europarl.eu.int

73 Risoluzione del Parlamento europeo sul progetto di decisione della Commissione che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR-Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti del 31 marzo 2004 (2004/2011(INI)) (*)

P5_TA-PROV(2004)0245

Protezione dei dati personali dei passeggeri aerei

Il Parlamento europeo,

– visti la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche don riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], e in particolare il suo articolo 25, nonché il regolamento (CE) n. 2289/99 del Consiglio, del 24 luglio 1989, relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione [2],

– visto il progetto di decisione della Commissione che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR-Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (C5-0124/2004),

– visti il parere espresso il 29 gennaio 2004 dal gruppo di lavoro di cui all'articolo 29 della direttiva 95/46/CE sulla tutela dei dati personali e quello espresso il 17 febbraio 2004 dal comitato di cui all'articolo 31 della direttiva sopra citata,

– vista la sua risoluzione del 9 marzo 2004 [3] sull'applicazione della direttiva 95/46/CE,

– vista la posizione espressa dai parlamenti nazionali al riguardo,

– visti il parere della commissione belga per la privacy su due casi relativi al trasferimento da parte di tre compagnie aeree dei dati personali di alcuni passeggeri transatlantici - tra cui quelli di un deputato europeo - secondo il quale sono stati violati il diritto nazionale ed europeo in materia di privacy; la constatazione del Consiglio secondo la quale le misure USA confliggono potenzialmente con la legislazione comunitaria e degli Stati membri sulla protezione dei dati (2562ª sessione del Consiglio Affari Generali - Bruxelles, 23 febbraio 2004); il documento interno della Commissione che conferma l'effettiva esistenza di tale conflitto; la condanna da parte del Parlamento europeo della flagrante violazione della legislazione sulla privacy; il fatto che le maggiori responsabilità incombono alla Commissione, agli Stati membri nonché a talune autorità garanti della privacy,

(*) p. 198-205

(1) G.U. L 281 del 23 novembre 1995, p. 31 Direttiva modificata dal regolamento (CE) n. 1882/2003 (G.U. L 284 del 31 ottobre 2003, p. 1).

(2) G.U. L 220 del 29 luglio 1989. Regolamento modificato da ultimo dal regolamento (CE) n. 323/1999 (G.U. L 40 del 13 febbraio 1999, p. 1).

(3) P5_TA(2004)0141.

– visto l'articolo 8 della decisione 1999/468/CE del Consiglio, del 28 giugno1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione [3],

– visto l'articolo 88 del suo regolamento,

A. ricordando che l'amministrazione USA, in applicazione del Transport Security Act (Legge sulla sicurezza dei trasporti) e dei relativi provvedimenti di attuazione, come l'Aviation Security Screening Records [4] (Registri di controllo della sicurezza aerea) ha imposto alle compagnie aeree che operano in Europa di consentire l'accesso ai dati commerciali contenuti nelle pratiche passeggeri (PNR), al fine di stabilire preventivamente la minaccia potenziale che ogni passeggero potrebbe rappresentare e di garantire che terroristi o individui responsabili di gravi crimini siano identificati e arrestati o che sia loro negato l'ingresso negli Stati Uniti,

B. constatando che è necessario un chiaro quadro giuridico se si vuole consentire tale accesso è illegale secondo il diritto nazionale ed europeo sulla privacy, e che ciononostante né la Commissione, né gli Stati membri, né le autorità garanti della privacy e dotate di poteri vincolanti hanno operato per assicurare l'applicazione della legge,

C. ricordando che, nel settore dei trasporti aerei, la pratica passeggeri (PNR) è un archivio contenente una serie di informazioni commerciali che riguardano in particolare:

a) i dati che consentono di individuare il passeggero, le persone che lo accompagnano e coloro che hanno chiesto la prenotazione per suo conto, l'agenzia o il dipendente che l'hanno effettuata e/o che hanno emesso il biglietto, ecc.,
b) i dati concernenti il percorso per il quale è stato emesso il biglietto, ma anche tutti gli altri segmenti che costituiscono l'itinerario completo di un percorso composto a diverse tratte che implicano quindi più biglietti,
c) i dati concernenti i mezzi di pagamento, il numero di carta di credito del passeggero, le condizioni speciali concesse a categorie particolari (frequent flyers, membri di categorie speciali), gli indirizzi e-mail nonché gli indirizzi fisici e i numeri di telefono privati e/o professionali dichiarati al momento della prenotazione, le persone da avvisare, ecc.,
d) i dati relativi ad un servizio particolare connesso alle condizioni di salute della persona, alle sue preferenze alimentari, ecc.,
e) le osservazioni specifiche effettuate dal personale della compagnia aerea,
f) se del caso, dettagli sulle prenotazioni di un'automobile a noleggio e stanze d'albergo,

D. considerando che i dati PNR variano a seconda delle pratiche commerciali seguite da ogni compagnia aerea e sono trattati da centri di prenotazione e che, di conseguenza, le compagnie aeree dovrebbero mettere a punto programmi adeguati per estrapolare i dati che potrebbero legittimamente essere trasferiti,

Quanto ai principi di tutela dei dati da parte dell'Europa

E. considerando che l'articolo 8, paragrafo 2 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come viene interpretato dalla Corte europea dei diritti dell'uomo (CEDU)[5], ammette un'ingerenza nella vita privata solo quando "... sia prevista dalla legge [6], sia necessaria [7] in una società democratica [8] per perseguire scopi legittimi e non sia sproporzionata [9] in rapporto all'obiettivo perseguito",

F. consapevole che, in questa fase, non esiste una base giuridica nell'Unione europea che consenta di utilizzare a fini di sicurezza pubblica i dati commerciali PNR e che tale base giuridica è indispensabile per modificare la finalità per cui i dati sono stati originariamente raccolti e per autorizzare l'utilizzazione di questi dati a scopi di sicurezza pubblica,

G. ricordando che questa base giuridica deve definire esattamente i dati da raccogliere, le norme da seguire per la loro elaborazione e le responsabilità di tutte le parti interessate

(3) G.U. L 184 del 17 luglio 1999, p. 23.
(4) FEDERAL REGISTER 68 FR 2101 "il TSA intende utilizzare questo sistema di registrazioni per agevolare il passeggero TSA e il programma di verifica della sicurezza aerea ai sensi dell'Aviation and Transportation Security Act. Il TSA intende usare il sistema CAPPS II per effettuare valutazioni dei rischi al fine di garantire la sicurezza dei passeggeri e dei voli.
(5) CEDU, sentenza Amann contro Svizzera del 16 febbraio 2000, raccolta delle sentenze e decisioni 2000-II, par. 65, e Rotaru contro Romania del 4 maggio 2000, raccolta delle sentenze e delle decisioni 2000-V, par. 43).
(6) Il ricorso a una "legge" è tanto più giustificato quando si tratta della protezione di un diritto fondamentale e tale protezione non può essere lasciata a misure di tipo amministrativo o a semplici provvedimenti di attuazione. Una "legge" deve inoltre essere elaborata con precisione sufficiente per consentire ai destinatari delle sue disposizioni di conformarvi la propria condotta e rispondere all'esigenza di prevedibilità che deriva dalla giurisprudenza della Corte europea dei diritti dell'uomo (vedasi in particolare CEDU, sentenza Rekvényi contro Ungheria del 20 maggio 1999, raccolta delle sentenze e decisioni 1999-III, par. 34).

/ segue

(passeggeri, compagnie aeree e autorità pubbliche),

H. considerando che il Consiglio ha di recente approvato il mandato negoziale della Commissione per un accordo internazionale in questo settore ,

...e da parte degli Stati Uniti

I. considerando che negli Stati Uniti la protezione della vita privata, pur essendo citata dal quarto emendamento alla Costituzione, non è considerata come un diritto fondamentale,

a) ma è disciplinata da disposizioni specifiche (che tuttavia non contemplano il settore dei trasporti) e dal Freedom of Information Act (Legge sulla libertà di informazione),
b) permette ai soli cittadini USA e ai residenti legali di beneficiare di una protezione dei dati e, in particolare, del diritto di accesso e di rettifica relativamente ai soli dati detenuti dalle autorità pubbliche federali (Privacy Act del 1974), in modo che
c) nessuna tutela giuridica è attualmente garantita per i dati dei passeggeri non americani e in particolare europei, né alcun diritto di ricorso giurisdizionale contro eventuali abusi delle misure restrittive della libertà di circolazione,

Quanto all'impatto giuridico di una decisione in materia di adeguatezza a norma dell'articolo 25 della direttiva 95/46/CE

J. consapevole del fatto che il progetto di decisione presentato dalla Commissione:

a) è una misura di semplice esecuzione della direttiva 95/46/CE che non può avere l'effetto di ridurre i criteri di protezione dei dati garantiti nella UE come stabilito dalla direttiva 95/46/CE,
b) riguarda una situazione caratterizzata ancora da un limbo giuridico sia negli Stati Uniti (poiché gli "impegni" presi dagli Stati Uniti non in tutti i casi hanno effetti giuridici) che in Europa (poiché non è stata ancora adottata nessuna base giuridica che consenta il legittimo trasferimento di dati PNR ad autorità pubbliche),
c) una volta adottato, priverà in pratica gli Stati membri (attualmente responsabili di garantire la protezione delle persone quanto ai dati PNR) di ogni possibilità di bloccare i trasferimenti per garantire i diritti dei loro cittadini,

K. deplorando che, per tutto il 2003, la Commissione non abbia tenuto conto delle ripetute richieste del Parlamento europeo e delle autorità di controllo dei dati che la invitavano:

a) a definire i dati che potrebbero essere trasferiti legittimamente senza rischi (vedasi l'elenco dei 19 punti proposti il 13 giugno 2003 dal Gruppo di cui all'articolo 29 della direttiva 95/46/CE)[10],
b) a sostituire immediatamente il sistema "PULL" (utilizzato senza base giuridica dall'amministrazione USA e senza filtri per i dati sensibili o per i voli non transatlantici) col sistema "PUSH" (che permette a ogni compagnia aerea di trasferire solo i dati legittimi e per i soli voli con destinazione USA),
c) a negoziare un accordo internazionale con gli USA che preveda garanzie reali per i passeggeri o quantomeno la stessa protezione di cui beneficiano i cittadini USA,

L. facendo proprie gran parte delle riserve formulate all'unanimità dalle autorità di controllo dei dati riunite in seno al gruppo di lavoro previsto dall'articolo 29 della direttiva 95/46/CE, precisamente il 29 gennaio 2004 [11],

1. ritiene che la decisione della Commissione del ... , che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR - Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti, esuli dalle competenze di esecuzione conferite alla Commissione, in quanto:

/ segue nota (8)
Nel caso in questione, la legge deve anche comportare disposizioni esplicite e dettagliate sulle persone autorizzate a consultare i fascicoli, la natura di tali fascicoli, la procedura da seguire e l'uso che può essere fatto delle informazioni così ottenute (vedasi CEDU, sentenza Rotaru contro Romania, 4 maggio 2000).
(7) Il concetto di "necessità" implica l'esigenza sociale imperiosa che la misura adottata sia proporzionata allo scopo legittimo perseguito (vedasi in particolare CEDU, sentenza Gillow contro Regno Unito del 24 novembre 1986, Serie A n. 109, par. 55) e che, in questa prospettiva, il legislatore usufruisca di un margine di valutazione "la cui ampiezza non dipende solo dalla finalità ma anche dal carattere proprio dell'ingerenza" (vedasi CEDU, sentenza Leander contro Svezia del 26 marzo 1987, Serie A n. 116, par. 59).
(8) Il criterio di società "democratica" si applica alle relazioni tra poteri pubblici e cittadini ed è da considerare tanto più presente quando sono i cittadini a controllare le istituzioni e non il contrario. Evidentemente, qualunque sia la natura di tali relazioni, in ogni democrazia è essenziale valutare con molta cautela ogni forma di raccolta e di stoccaggio sistematico dei dati, soprattutto qualora tali dati riguardino persone che non rappresentano un pericolo per la collettività.
(9) Il criterio di proporzionalità si applica a tutti i parametri
/ segue

Per quanto riguarda la base giuridica e la forma

1.1. il progetto di decisione non è (e non potrebbe essere):

a) una **base giuridica** che possa, in seno all'Unione europea, modificare le finalità per cui sono stati raccolti dati nel PNR e permetterne il trasferimento totale o parziale a terzi da parte delle compagnie aeree [12]; esso può avere però quale probabile risultato una riduzione dei criteri di protezione dei dati previsti dalla direttiva 95/46/CE all'interno dell'UE o la creazione di nuovi criteri d'intesa con paesi terzi;

b) un accordo internazionale in applicazione del quale la Commissione sarebbe tenuta ad autorizzare il trasferimento di tali dati; non si può che deplorare l'ambigua formulazione di alcune clausole della decisione e degli impegni corrispondenti (come quelle relative alla durata, ai meccanismi di controllo, ai casi di sospensione o revoca della decisione, alle condizioni di intervento degli Stati membri, ecc.) che potrebbero indurre falsamente a ritenere che tale testo sia suscettibile di creare alcuni obblighi in quanto sono esplicitamente esclusi dalla clausola 47 la quale stipula che "tali impegni non creano alcun diritto o vantaggio per alcuna persona o parte, privata o pubblica";

Per quanto riguarda il contenuto

1.2. il progetto di decisione si fonda su "impegni" la cui obbligatorietà è lungi dall'essere evidente:

a) sia per la fonte che è puramente amministrativa (e quindi soggetta a possibili ristrutturazioni interne al Departement of Home Security (DHS - Ministero della sicurezza interna) che renderebbero obsolete le separazioni tra strutture interne);

b) sia per il contenuto in quanto, da una parte, si fa riferimento a garanzie che non sono ancora una base giuridica negli USA e, dall'altra, si mantiene la possibilità di modificare la regolamentazione in qualsiasi momento, in particolare per quanto riguarda le modalità di utilizzazione e riutilizzazione dei dati;

1.3. il sistema "pull" di accesso ai dati PNR mette a repentaglio eventuali limitazioni che possano essere state convenute e deve essere sostituito da un sistema "push" dotato di filtri adeguati;

2. ritiene che l'importanza della questione sia tale che l'Unione europea debba regolarla con gli Stati Uniti sulla base di un vero accordo internazionale che, nel pieno rispetto dei diritti fondamentali, definisca:

a) i dati che possono essere trasferiti in modo automatizzato (APIS) e i dati che possono essere trasferiti caso per caso;

b) l'elenco dei reati gravi per cui è possibile avanzare una richiesta supplementare;

c) l'elenco delle autorità e delle agenzie che potrebbero condividere i dati e le condizioni di tutela dei dati da rispettare:

d) il periodo di conservazione per i due tipi di dati, fermo restando che i dati relativi alla prevenzione di reati gravi devono essere scambiati sulla base dell'accordo UE/USA sulla cooperazione giudiziaria e l'estradizione;

e) il ruolo che le compagnie aeree devono svolgere nel trasferire i dati dei passeggeri e gli strumenti previsti (APIS, PNR, ecc.) a fini di sicurezza pubblica;

f) le garanzie da fornire ai passeggeri per consentire loro di correggere i dati che li riguardano o fornire spiegazioni in caso di discordanze tra i dati connessi a un contratto di viaggio e i dati figuranti nei documenti di identità, nei visti e nei passaporti;

g) le responsabilità delle compagnie aeree nei confronti dei passeggeri e delle autorità pubbliche in caso di errori di trascrizione o di codificazione e per quanto concerne la tutela dei dati trattati;

h) il diritto di far ricorso ad un'autorità indipendente e a meccanismi di rimedio in caso di violazione dei diritti dei passeggeri;

3. si dichiara disposto a esaminare in base alla procedura d'urgenza un accordo internazionale che rispetti i suddetti principi; ritiene che, se fosse adottato tale accordo, la

/ segue nota (9)
del trattamento dei dati (ad esempio in che momento i dati vengono trasferiti, quali dati sono trasferiti, a chi, per fare cosa, durata della conservazione, durata della deroga). Nel quadro del diritto europeo tali valutazioni devono anche essere fatte tenendo presente le esigenze di sussidiarietà che disciplinano i rapporti tra gli Stati membri e l'Unione europea. Ciò è tanto più necessario nel caso in cui gli Stati membri venissero privati della possibilità di intervenire da un atto di un'Istituzione

(10) "I dati dovrebbero includere le informazioni seguenti: "PNR record locator code", data di prenotazione, data/e prevista/e del viaggio, nome del passeggero, altri nomi presenti nel PNR, l'itinerario di viaggio, le coordinate dei biglietti gratuiti, biglietti di sola andata, "ticketing field information", dati "ATFQ (Automatic Ticket Fare Quote)", numero del biglietto, data in cui il biglietto è stato emesso, "no show history", numero di bagagli, numero identificativo dei bagagli, "no show information", numero di bagagli per ogni segmento, modifiche volontarie o involontarie di classe, dettagli delle modifiche effettuate sui dati PNR e riguardanti gli elementi precedentemente menzionati".

(11) www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs/2004 /wp87-fr.pdf.

(12) Peraltro, l'obbligo imposto alle compagnie aeree dalla legislazione

/ segue

Commissione potrebbe legittimamente dichiarare che i dati sarebbero adeguatamente protetti negli USA;

4. invita la Commissione a presentare al Parlamento una nuova decisione in materia di adeguatezza, a chiedere al Consiglio il mandato per un nuovo e rigoroso accordo internazionale nel rispetto dei principi enunciati nella presente risoluzione;

5. invita, in attesa di una soluzione legislativa definitiva o della conclusione di uno o più accordi internazionali:

a) gli Stati membri a imporre immediatamente il rispetto del diritto nazionale ed europeo sulla privacy, richiamando in particolare l'attenzione sull'obbligo fatto, a norma dell'articolo 26, paragrafo 1, lettera a) della direttiva 95/46/CE, alle compagnie aeree e alle agenzie di viaggio di ottenere dai passeggeri il consenso per il trasferimento dei dati; tale consenso deve essere concesso spontaneamente e i passeggeri devono essere informati in merito alle possibilità di scelta per influenzare il contenuto del proprio PNR, alle conseguenze di un mancato consenso e all'assenza di un livello adeguato di protezione negli Stati Uniti;

b) la Commissione ad intervenire per assicurare l'applicazione del regolamento (CE) n. 2289/99 e, nella fattispecie, a verificare che i dati non siano trasferiti, in particolare attraverso i sistemi telematici di prenotazione (CRS), senza il consenso del passeggero e che le amministrazioni di paesi terzi non abbiano accesso a tali sistemi;

6. invita la Commissione a bloccare:

a) il sistema "PULL" a partire dal 1° luglio 2004 e, dopo tale data, ad applicare il sistema "PUSH" con i 19 punti proposti il 13 giugno 2003 dal gruppo di lavoro di cui all'articolo articolo 29 della direttiva 95/46/CE;

b) le iniziative concernenti l'istituzione di una gestione centralizzata europea dei dati PNR come delineato nella Comunicazione COM(2003) 826 e come è stato recentemente confermato dal Commissario competente alla commissione parlamentare, in quanto tali iniziative violano per il momento i principi di proporzionalità e di sussidiarietà;

7. si riserva comunque il diritto di adire la Corte di giustizia qualora il progetto di decisione venga adottato dalla Commissione; ricorda alla Commissione l'obbligo di cooperazione leale tra istituzioni previsto all'articolo 10 del Trattato e la invita a non adottare, durante il periodo elettorale, una decisione come quella esaminata dalla presente risoluzione;

8. si riserva il diritto di adire la Corte di Giustizia per verificare la legalità del previsto accordo internazionale e, in particolare, la sua compatibilità con la tutela di un diritto fondamentale;

9. ritiene estremamente importante che l'esito dei negoziati non sia adottato come modello per le ulteriori attività dell'UE in ordine al varo delle proprie misure finalizzate alla lotta contro la criminalità, alla memorizzazione dei dati nonché alla tutela della privacy;

10. invita la Commissione a ritirare il progetto di decisione;

* * *

11. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione, ai parlamenti e ai governi degli Stati membri, nonché al Congresso degli Stati Uniti.

/ segue nota (12)

americana non può essere considerato come un obbligo legale sufficiente ai sensi dell'articolo 7, lettera c) della direttiva 95/46/CE che va interpretato alla luce dei diritti fondamentali i quali, secondo una giurisprudenza costante, fanno parte integrante dei principi generali del diritto di cui la Corte di giustizia delle Comunità europee assicura il rispetto (cfr. in particolare sentenza del 6 marzo 2001, Connolly/Commissione, C-274/99 P, Rec. p. I-1611, punto 37).

74 Ethical Aspects of Genetic Testing in the Workplace (*)

OPINION OF THE EUROPEAN GROUP ON ETHICS

IN SCIENCE AND NEW TECHNOLOGIES

TO THE EUROPEAN COMMISSION

No 18 **Final – 28th July 2003**

Original in English

****

ETHICAL ASPECTS OF GENETIC TESTING IN THE WORKPLACE

Reference: Initiative of the Group

Rapporteurs: Peter Whittaker and Nicos C. Alivizatos

****

The European Group on Ethics in Science and New Technologies (EGE),

Having regard to the Treaty on European Union as amended by the Treaty of Nice, and in particular Article 6 of the common provisions, concerning the respect for fundamental rights;

Having regard to the EC Treaty and in particular Article 137 concerning the working conditions and health and safety at work;

Having regard to the Charter on Fundamental Rights of the European Union, approved by the European Council in Biarritz on October 14th 2000 and proclaimed solemny in Nice by the European Parliament, the Council and the Commission on December 7th 2000, in particular Article 8 on the "Protection of personal data", Article 15 on the "Freedom to choose an occupation and right to engage in work", Article 21 prohibiting discrimination based, among others, on genetic features, and Article 31 on "Fair and just working conditions";

Having regard to the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data;

Having regard to the Directive 2000/78/EC of the European Council of 27 November 2000 establishing a general framework for equal treatment in employment and occupation;

(*) Prima pagina del documento, rinvenibile in http://europa.eu.int/comm/european_group_ethics/docs/avis18EN.pdf

75 Sentenza della Corte di giustizia delle Comunità europee del 20 maggio 2003, *Österreichischer Rundfunk e.a.* (*)

"Tutela delle persone fisiche con riguardo al trattamento di dati personali - Direttiva 95/46/CE - Tutela della vita privata - Divulgazione dei dati sui redditi di dipendenti di enti sottoposti al controllo del Rechnungshof"

Nei procedimenti riuniti C-465/00, C-138/01 e C-139/01,

aventi ad oggetto tre domande di pronuncia pregiudiziale proposte alla Corte, a norma dell'art. 234 CE, rispettivamente dal Verfassungsgerichtshof (C-465/00) e dall'Oberster Gerichtshof (C-138/01 e C-139/01) (Austria) nelle cause dinanzi ad essi pendenti tra

[...]

domande vertenti sull'interpretazione della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31),

[...]

LA CORTE,

pronunciandosi sulle questioni sottopostele dal Verfassungsgerichtshof, con ordinanza 12 febbraio 2000, e dall'Oberster Gerichtshof, con ordinanze 14 e 28 febbraio 2001, dichiara:

1) **Gli artt. 6, n. 1, lett. c), e 7, lett. c) ed e), della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, non ostano ad una normativa nazionale come quella di cui trattasi nelle cause principali, a condizione che sia provato che l'ampia divulgazione non solo dell'importo dei redditi annui, laddove questi superino un certo limite, delle persone impiegate presso enti soggetti al controllo del Rechnungshof, ma anche dei nomi dei beneficiari di tali redditi, è al contempo necessaria ed appropriata all'obiettivo di buona gestione delle risorse pubbliche perseguito dal costituente. La verifica di ciò spetta ai giudici del rinvio.**
2) **Gli artt. 6, n. 1, lett. c), e 7, lett. c) ed e), della direttiva 95/46 sono direttamente applicabili, nel senso che essi possono essere fatti valere da un singolo dinanzi ai giudici nazionali per evitare l'applicazione delle norme di diritto interno contrarie a tali disposizioni.**

(*) Estratto del documento, rinvenibile in www.europa.eu.int /servlet/portail /CuriaServlet?curiaLink=%26lang%3DIT%26ident%3D79969479C19010139%26model%3Ddoc_curia

76 Sentenza della Corte di giustizia delle Comunità europee del 6 novembre 2003, *Bodil Lindquist* (*)

"Direttiva 95/46/CE - Ambito di applicazione -Pubblicazione dei dati personali su Internet - Luogo della pubblicazione - Nozione di trasferimento di dati personali verso paesi terzi - Libertà d'espressione - Compatibilità con la direttiva 95/46 di una protezione più ampia dei dati personali da parte della normativa di uno Stato membro"

Nel procedimento C-101/01,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, a norma dell'art. 234 CE, dalla Göta Hovrätt (Svezia), nel procedimento penale dinanzi ad essa pendente contro

Bodil Lindqvist,

domanda vertente, in particolare, sull'interpretazione della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31),

LA CORTE

[...]

pronunciandosi sulle questioni sottopostele dalla Göta Hovrätt con ordinanza 23 febbraio 2001, dichiara:

1) L'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un «trattamento di dati personali interamente o parzialmente automatizzato», ai sensi dell'art. 3, n. 1, della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

2) Un siffatto trattamento di dati personali non rientra in alcuna delle eccezioni che figurano nell'art. 3, n. 2, della direttiva 95/46.

3) L'indicazione del fatto che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisce un dato personale relativo alla salute ai sensi dell'art. 8, n. 1, della direttiva 95/46.

4) Non si configura un «trasferimento verso un paese terzo di dati» ai sensi dell'art. 25 della direttiva 95/46 allorché una persona che si trovi in uno Stato membro inserisce in una pagina Internet - caricata presso una persona fisica o giuridica che ospita («web hosting») il sito Internet nel quale la pagina può essere consultata e che è stabilita nello Stato stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi.

5) Le disposizioni della direttiva 95/46 non pongono, di per sé, una restrizione incompatibile con il principio generale di libertà di espressione, o con altri diritti e libertà vigenti all'interno dell'Unione europea e che trovano corrispondenza,

(*) Estratto del documento, rinvenibile in www.europa.eu.int /servlet/portail /CuriaServlet?curiaLink=%26lang%3DIT%26ident%3D79968893C19010101%26model%3Ddoc_curia

tra l'altro, nell'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950. Spetta alle autorità e ai giudici nazionali incaricati di applicare la normativa interna che traspone la direttiva 95/46 garantire il giusto equilibrio tra i diritti e gli interessi in gioco, ivi compresi i diritti fondamentali tutelati dall'ordinamento giuridico comunitario.

6) Le misure adottate dagli Stati membri per garantire la protezione dei dati personali devono essere conformi tanto alle disposizioni della direttiva 95/46 quanto al suo obiettivo, consistente nel mantenere un equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata. Per contro, nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, qualora non vi osti alcun'altra disposizione del diritto comunitario.

X - Consiglio d'Europa

77 Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (20-23 May 2003)

INTRODUCTION

The Council of Europe's data protection committees wished to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe therefore asked a consultant, Dr Giovanni BUTTARELLI (Secretary General of the Italian Data Protection Authority), to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context. It was therefore agreed to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account in relation to video surveillance.

After examination of Mr Buttarelli's report and guiding principles, the CJ-PD agreed to re-elaborate and specify some of these guiding principles, and prepared the following text.

Many public and private entities have increasingly been using surveillance systems in different sectors for various purposes, in particular in order to control the movement of persons and goods and access to property, as well as events, situations and conversations - whether by telephone, over electronic networks or at a physical location.

Surveillance systems often result in the collection of personal data even though their collection and/or storage is sometimes not the aim of the surveillance data controller.

A considerable portion of these activities is performed by means of video surveillance devices, which raises specific issues as regards data protection.

Information collected during video surveillance activities often includes data (in the form of images and sounds) which directly or indirectly permit the identification of individuals, and the monitoring of their conduct. Moreover, video surveillance systems are increasingly converging with other technologies that raise new privacy and data protection concerns. These include the recording of sounds, wireless and high-speed computer networks used to transfer images; facial recognition systems integrated with computerised databases which can identify and track individuals; and devices that search under clothing and through walls, for example heat recognition devices or infra-red devices.

Video surveillance activities entailing the processing of personal data fall within the scope of application of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No.108] (hereinafter Convention 108) -which was prepared when it became apparent that in order to ensure the effective legal protection of personal data it would be necessary to develop more specifically and systematically the general reference to respect for private life in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter ECHR).

Additional rights and safeguards are laid down in various Council of Europe Recommendations, in particular:

- Recommendation No. R(87) 15 on the use of personal data in the police sector;
- Recommendation No. R(89) 2 on the protection of personal data used for employment purposes;
- Recommendation No. R(95) 4 on the protection of personal data in the telecommunications sector;
- Various other recommendations which - though not expressly referring to video surveillance - include safeguards and rules that are relevant in terms of personal data protection as also related to data communication and transborder data flows.

Video surveillance is not expressly covered in these instruments. In view of the increase in the use of and technological developments in video surveillance, this subject needs to be addressed.

These guiding principles, therefore, expand and further specify the safeguards applying to data subjects contained in the provisions of those earlier instruments as regards the processing of personal data collected by video surveillance. They cover any type of video surveillance activity allowing (by means of technical equipment) the systematic observation, collection and/or storage of personal data relating to one or more individuals in particular in respect of their conduct, presence and/or movement. These guiding principles should cover systematic observation, whether permanent or on the occasion of a specific event, whether personal data are processed wholly or partly by automatic means, and whether they form part of an archive system or constitute non-automatic systematic processing.

Some guidelines anticipate new possibilities of information technology that will allow easy access and correction without revealing the personal data of third parties.

Attention should be drawn to the fact that, to the extent that these guiding principles contain safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, as established by Articles 5, 6 and 8 of Convention 108 and Article 8 of the ECHR, derogations from such rights, in accordance with Article 9 of Convention 108, which were elaborated on the basis of Article 8 of the ECHR, are possible where they are provided for by law and constitute a necessary measure in a democratic society in the interests of:

- protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;
- protecting the data subject or the rights and freedoms of others.

These guiding principles are intended for the widest possible dissemination among individuals who may be the subject of video surveillance and the users of video surveillance systems, devices and techniques. They are also addressed to member States, manufacturers, dealers, service and access providers and researchers with a view to developing software and technologies that pay greater attention to data subjects' fundamental rights with regard to video surveillance. Council of Europe member States should ensure that these guiding principles are applied as consistently as possible.

These guiding principles could also serve as a framework for other surveillance activities that are not based on the use of video surveillance devices.

GUIDING PRINCIPLES

Any video surveillance activity should be undertaken by taking such measures as are necessary in order to ensure that this activity complies with personal data protection principles, in particular:

1) by ensuring that it is carried out in a fair and lawful manner for legitimate, specific, and explicit purposes. Personal data collected by means of video surveillance should not be

further processed in a way incompatible with the purposes for which they were collected;

2) by only using video surveillance if, depending on the circumstances, the purpose cannot be attained by measures which interfere less with privacy, provided that the alternative measures would not involve disproportionate cost;

3) by making use of video surveillance in an adequate, relevant and non-excessive way with regard to the determined and specific purposes sought in the individual cases where there is a demonstrable need, in order to avoid any unintentional and unjustified infringement of the data subject's rights and fundamental freedoms, for example, the freedom of movement, and to ensure in particular respect of his privacy, even in public places; [1]

4) Video surveillance should be carried out in a way that does not make the persons recorded recognisable if the purpose of the processing does not require their possible identification;

5) by preventing the data collected from being indexed, matched or kept unnecessarily. When it proves necessary to keep data, these data must be deleted as soon as they are no longer necessary for the determined and specific purpose sought;

6) by refraining from video surveillance activities where the processing of the data would result in discrimination against certain data subjects or groups of data subjects exclusively on account of their political opinions, religious beliefs, health or sexual life, racial or ethnic origin;

7) by making clearly discernible in an appropriate manner that video surveillance is taking place, its purpose and the identity of the controller [2] or by informing the data subject beforehand of the above. Other information, [3] having regard to the specific circumstances, should be provided to the data subject, where this is necessary to guarantee fair processing of personal data and does not jeopardise the purpose of the surveillance;

8) by ensuring that during the storage period, the right of access to the data, and, where appropriate, the right of rectification, blocking and/or erasure, is granted to the data subject unless this would entail disproportionate effort;

9) by taking all technical or organisational measures necessary to safeguard the integrity [4] of the collected information ;

10) In case of storage by the police of personal data by automatic means resulting from video surveillance, the principles of Recommendation No. R (87) 15 on the use of personal data in the police sector should furthermore be taken into account;

11) by limiting the use of video surveillance systems in the workplace to organisational and production requirements or to occupational safety purposes. This system should not be aimed at the systematic surveillance of the quality and quantity of individual performance in the workplace.

Employees or their representatives should be informed or consulted before the introduction or adaptation of a video surveillance system. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity their agreement [5] should be sought. In the event of a lawsuit or counterclaim, employees should be able to ground them on the recording made.

12) If personal data are recorded and kept, this should be done as far as possible in a way that allows data subjects to exercise their right of access, in accordance with data protection legislation, without obtaining information about other people.

(1) Therefore, those responsible for such systems are invited to assess to what extent the video surveillance systems are adapted to their information requirements in relation to the geographical location of the cameras (which areas of the city, which streets and why), and to choose which technology should be used according to these same requirements (image definition, zoom capacity, camera miniaturization...) without using excessive measures.
(2) In some cases the purpose and the identity of the controller are clear from the circumstances. However, in certain limited cases (e.g. traffic management) it may not be feasible to make the identity of the controller available beforehand.
(3) The information to be provided to the data subject may also include technical specifications of the chosen system.
(4) This is of special importance in cases of digitisation since the alteration of data cannot be easily detected. Collected information should only be modified for adequate and justified reasons, the modified information collected should be labelled as such and the original information should be retained.
(5) For example, this agreement could be given, in accordance with the relevant domestic law procedures, by trade unions or labour councils.

XI - Autorità comune di controllo dell'Europol

78 Rapporto sull'attività ottobre 1998 - ottobre 2002

Prefazione

In qualità di presidente dell'autorità di controllo comune (ACC) dell'Europol, sono lieto di presentarne la prima relazione di attività. Le misure qui illustrate debbono molto alle iniziative avviate da coloro che mi hanno preceduto, i signori Fergus Glavey ed Alex Turk, come pure al signor Peter Hustinx, primo presidente del comitato per i ricorsi, nonché alla competente ed entusiastica collaborazione di tutti i membri dell'ACC.

L'interesse manifestato dalla stampa e dal grande pubblico per il ruolo svolto dall'autorità di controllo comune è in chiaro aumento. Segno probabilmente del fatto di essere ora un organismo promettente e pienamente operativo grazie, tra l'altro, all'istituzione di un segretariato generale in comune con l'ACC di Schengen e l'ACC per le doganale. In taluni Stati membri, il ruolo svolto dall'Europol al pari del suo funzionamento e delle sue modalità di controllo sono discussi in sede parlamentare.

Per altro verso resta probabilmente altrettanto vero che i tragici eventi del settembre 2001 negli Stati Uniti hanno accresciuto la consapevolezza dei nostri concittadini europei circa l'importanza dei problemi trattati dall'Europol e, di conseguenza, dei compiti dell'autorità di controllo comune. Quest'ultima è chiamata a svolgere un'opera continua di mediazione tra gli obblighi nascenti dalla tutela dei dati personali e le legittime esigenze dell'Europol all'interno della cooperazione con i propri omologhi americani nella lotta contro il terrorismo.

Concludo esprimendo l'auspicio che, nel 2004, al momento di pubblicare la seconda relazione di attività, ci sia dato affermare il trionfo dei valori umanitari sulle forze dell'oscurantismo.

Klaus Kalk

I. La protezione dei dati e l'Europol

Da tempo è noto che la lotta contro la criminalità sarà realmente efficace soltanto quando le forze di polizia collaboreranno a livello nazionale ed internazionale. La convenzione Europol è l'espressione del forte desiderio all'interno dell'Unione europea di incoraggiare tale cooperazione. Sebbene la cooperazione internazionale non si possa definire un fenomeno nuovo nel campo delle forze di polizia, la convenzione Europol segna la creazione di un organismo europeo che mette a disposizione una piattaforma per varie forme di cooperazione tra le forze di polizia.

In generale tutti convengono che gli sviluppi in tale campo debbono avvenire all'interno di un quadro giuridico che rispecchi la salvaguardia dei diritti dell'individuo. Tale esigenza è espressa nella premessa della convenzione Europol in cui si riconosce:

> *"la necessità di rivolgere anche nel campo della cooperazione tra forze di polizia, particolare attenzione alla tutela dei diritti dei singoli individui e in particolare alla protezione dei dati di carattere personale".*

Le disposizioni riguardanti la protezione dei dati contenute nella convenzione Europol

constano di due elementi. Innanzitutto stabiliscono che nel quadro dell'applicazione della convenzione Europol (articolo 14 convenzione Europol), per quanto riguarda il trattamento dei dati di carattere personale in archivi, ciascuno Stato membro deve aver adottato le disposizioni di diritto interno sulla protezione dei dati. Inoltre il livello di protezione dei dati previsto dal diritto interno deve essere almeno pari a quello derivante dall'applicazione dei principi della convenzione del Consiglio d'Europa del 28 gennaio 1981 e deve tenere conto della raccomandazione R(87) 15, del 17 settembre 1987, del Comitato dei ministri del Consiglio d'Europa relativa all'uso dei dati di carattere personale da parte delle autorità di polizia.

In secondo luogo, le disposizioni della stessa convenzione Europol fissano numerosi principi di protezione dei dati. Tali norme creano un equilibrio tra le responsabilità dell'Europol in qualità di organismo incaricato del controllo dei dati, da un lato, e i diritti degli individui, dall'altro, prendendo in considerazione la posizione dell'Europol nelle varie forme di cooperazione.

Alcune di queste norme sulla protezione dei dati della convenzione Europol possono essere definite un incentivo all'armonizzazione delle norme sulla protezione dei dati applicabili agli archivi di polizia negli Stati membri dell'Unione. La convenzione Europol contempla alcuni diritti fondamentali della protezione dei dati - come il diritto di accesso œ che generalmente devono essere esercitati conformemente alle leggi sulla protezione dei dati dello Stato membro interessato. Nella pratica ciò può probabilmente condurre a un'ulteriore armonizzazione delle norme di protezione dei dati riguardanti le autorità di polizia.

La protezione dei dati non può avvenire soltanto a livello teorico. L'Europol è tenuto ad applicare le disposizioni indicate nella convenzione e quindi ad aver dimestichezza con i principi chiave della protezione dei dati. Sulla base dell'esperienza degli ultimi quattro anni, si può affermare che l'Europol ha in dovuta considerazione le proprie responsabilità di controllore dei dati.

II. I QUATTRO ANNI DELL'AUTORITÀ DI CONTROLLO COMUNE, IL SUO RUOLO E LA SUA EVOLUZIONE.

Dalla sua istituzione, l'autorità di controllo comune (ACC) si è riunita in assemblea plenaria 21 volte. La prima riunione costitutiva si è tenuta a l'Aia il 9 ottobre 1998. L'ACC si riunisce almeno quattro volte l'anno; peraltro, fin dagli esordi, si è manifestata in maniera evidente la necessità di riunioni ulteriori. L'ACC è composta da due membri o rappresentanti di ciascuna autorità di controllo nazionale degli Stati membri. (1)

Il compito dell'ACC è specificato nell'articolo 24 della convenzione Europol. Essa è, in linea generale, incaricata di vigilare sulle attività dell'Europol per accertarsi che la memorizzazione, il trattamento e l'utilizzazione dei dati detenuti dai servizi dell'Europol non ledano i diritti delle persone. L'ACC controlla inoltre la legittimità della trasmissione dei dati provenienti dall'Europol, esamina le questioni relative all'applicazione e all'interpretazione della convenzione e affronta problemi che possono sorgere all'atto dei controlli condotti dalle autorità di controllo nazionali. Oltre a ciò l'ACC ha facoltà di formulare proposte armonizzate in vista di soluzioni comuni.

Chiunque ha il diritto di chiedere all'ACC di verificare la legittimità e la correttezza dell'eventuale memorizzazione, rilevamento, trattamento ed utilizzazione di dati di carattere personale che lo riguardano, effettuati presso l'Europol.

(1) Austria, Belgio, Danimarca, Finlandia, Francia, Germania, Grecia, Irlanda, Italia, Lussemburgo, Paesi Bassi, Portogallo, Spagna, Svezia e Regno Unito

Ulteriori compiti specifici figurano agli articoli 12, 18, 19 e 20 della convenzione Europol. Essi riguardano la decisione costitutiva degli archivi, la trasmissione di dati a Stati e organismi terzi nonché una procedura di ricorso concernente il diritto di accesso e il diritto di rettifica e cancellazione dei dati.

Per svolgere le sue funzioni l'ACC si è dotata di un regolamento interno in occasione della seconda riunione avvenuta il 23 novembre 1998. Il Consiglio dell'Unione europea ha succes-

sivamente approvato tale regolamento con la decisione del 22 aprile 1999 (cfr. punto VII, allegato C).

Attualmente l'ACC è l'unico organismo di controllo comune dotato di un proprio bilancio. Altre autorità di controllo, infatti, come l'autorità di controllo comune di Schengen e l'autorità di controllo comune doganale, sono finanziate dalle normali strutture del Consiglio dell'Unione europea. Potendo disporre di un proprio bilancio, l'ACC è in grado di operare con un certo grado di flessibilità, svolgendo così le sue funzioni nel modo che meglio ritiene opportuno.

Inizialmente l'ACC disponeva di un segretariato composto da personale del segretariato generale del Consiglio dell'Unione europea. Tuttavia, in seguito ad una proposta per istituire un segretariato indipendente e la conseguente decisione del Consiglio, del 17 ottobre 2000, il 1o settembre 2001 è stato creato un segretariato permanente ed indipendente (cfr. punto VII, allegato D).

Resta indubbio che se l'ACC deve svolgere tutte le sue funzioni nel campo sempre più impegnativo della cooperazione fra le autorità di polizia, è necessario che il carico di lavoro sia gestito in modo efficiente. Fin dalla sua istituzione, l'ACC ha dovuto sviluppare metodi di lavoro che le avrebbero permesso di operare come un'autorità di controllo indipendente. Sono stati in tal modo creati gruppi di lavoro per risolvere problemi di informatica, questioni riguardanti i rapporti con Stati ed organismi terzi, per svolgere pubbliche relazioni nonché valutare le decisioni costitutive di archivi. Il lavoro svolto da questi gruppi ha consentito di preparare le riunioni dell'ACC. Nel contempo quest'ultima ha investito nell'ampliamento delle sue conoscenze in materia di cooperazione delle autorità di polizia e sull'operato dell'Europol.

L'ACC ha anche istituito un comitato per i ricorsi (cfr. successivo paragrafo V).

Il successo dell'ACC dipende dalla capacità di partecipazione delle autorità di controllo nazionali. La sempre maggiore necessità di ricevere pareri dell'ACC costringe le delegazioni, e quindi indirettamente le autorità di controllo nazionali, a mettere a disposizione risorse che talvolta sono in contrasto con le priorità nazionali. La creazione di un segretariato permanente può supplire soltanto in parte a questa situazione, ammesso che sia dotato di un organico adeguato. L'obiettivo dell'ACC è quello di essere un'organizzazione trasparente ed accessibile. A tal fine, si auspica di riuscire a presentare un sito Web nel corso del 2003.

III. Attività

A. Pareri

1. Decisioni costitutive di archivi

Le decisioni costitutive specificano la natura di uno dei tipi di archivi che sono trattati dall'Europol: l'archivio di analisi (articolo 10, convenzione Europol). La costituzione di un archivio di analisi è possibile soltanto previa approvazione del consiglio di amministrazione della decisione costitutiva di tale archivio (articolo 12, paragrafo 1, convenzione Europol). Prima che il consiglio di amministrazione possa decidere in merito alla costituzione di un archivio, il direttore dell'Europol deve informare l'ACC del suo progetto di richiesta di approvazione della decisione costitutiva di siffatto archivio. L'ACC, a sua volta, può decidere di consigliare il consiglio di amministrazione in merito alla costituzione dell'archivio. Rientra nelle politiche dell'ACC esprimersi sulla costituzione di ogni archivio di analisi.

Il Consiglio dell'Unione europea ha adottato le norme applicabili agli archivi di analisi dell'Europol con l'atto del Consiglio del 3 novembre 1998 (GU C 26 del 30.1.1999).

Se la questione per cui è necessario l'archivio di analisi è così urgente da precludere la possibilità di ottenere l'approvazione del consiglio di amministrazione prima della costituzione di detto archivio, il direttore può decidere, con decisione motivata, di costituire un archivio.

La normale procedura di adozione della decisione, incluso il ruolo consultivo dell'ACC, è quindi avviata immediatamente dopo la decisione di seguire la procedura d'urgenza.

In tutte le procedure d'urgenza sollecitate dal direttore dell'Europol, l'ACC ha sempre obiettato sulla necessità di ricorrere a questa procedura. L'utilizzo della procedura d'urgenza deve essere messa in relazione a un caso particolare e alla necessità dell'Europol di agire rapidamente considerata la natura del caso stesso. Nella pratica è invece risultato che la procedura d'urgenza era utilizzata principalmente per evitare la normale procedura di costituzione di un archivio di analisi, che talvolta richiede mesi. L'ACC ha riconosciuto la necessità di una procedura che richieda meno tempo ed ha istituito un gruppo di lavoro per la costituzione di archivi in modo da ridurre al minimo eventuali ritardi all'interno dell'ACC. È stato inoltre suggerito al consiglio di amministrazione dell'Europol di fare lo stesso (parere dell'8 maggio 2000, n. 00-07).

Per la costituzione di archivi l'Europol utilizza un modello che è stato adottato dopo aver consultato l'ACC. L'utilizzo di questo modello fornisce una chiara visione generale dello scopo e dei dati da trattare.

L'ACC esegue controlli per garantire che lo scopo dichiarato dell'archivio di analisi ricada tra le aree di competenza dell'Europol. Inoltre l'ACC compie indagini per accertare se i dati trattati siano o meno necessari al raggiungimento dello scopo dell'archivio, valutando del pari se tali dati rientrino nell'ambito dell'articolo 6 dell'atto del Consiglio. Qualora, prima di adottare un parere sulla costituzione di un archivio, l'ACC reputi necessarie ulteriori informazioni, essa provvederà a farne richiesta presso il direttore dell'Europol.

L'ACC ha espresso pareri per il consiglio di amministrazione in merito a 24 decisioni costitutive d'archivio di analisi. Due di questi casi riguardavano la modifica di una decisione costitutiva esistente. Al momento 16 di questi archivi di analisi sono tuttora in corso.

L'impiego di un modello di decisione costitutiva si è rivelato efficace. L'ACC è stata così in grado di valutare tali decisioni in tempo ragionevole, utilizzando il gruppo di lavoro per le decisioni costitutive per la preparazione dei pareri dell'ACC. Una buona parte di decisioni costitutive, talvolta anche in seguito a una richiesta di ulteriori informazioni, non ha dato luogo ad osservazioni. In alcuni campi, tuttavia, l'ACC ha riscontrato un certa contrapposizione tra l'intento di utilizzo degli archivi di analisi dell'Europol e le norme che li regolano.

Prevenzione

In relazione al mandato dell'Europol, nell'articolo 10 della convenzione Europol si specifica che lo scopo di un archivio di analisi deve riguardare reati che sono stati commessi oppure che potrebbero esserlo sulla base di gravi ragioni. Tali gravi ragioni devono sempre essere specificate prima della costituzione di un archivio di analisi a scopo preventivo.

Abuso di droga

I dati medici sono considerati alla stregua di dati sensibili. Il trattamento di questi dati, pertanto, è sottoposto a restrizioni ai sensi dell'articolo 10, paragrafo 1, della convenzione Europol, e deve essere classificato di conseguenza nella decisione costitutiva. In alcune circostanze le informazioni relative all'uso di droghe illegali sono considerate dei dati medici. Tali circostanze sono strettamente legate al contesto in cui i dati sono trattati. Se riguardano esclusivamente le abitudini di un individuo, senza un chiaro rapporto con i reati commessi, queste informazioni devono essere classificate come dati medici.

Biometria

In Europa, il quadro giuridico per elementi di prova basati sul DNA e altre forme di identificazione biometrica non è uniforme, per cui questi dati possono essere utilizzati dall'Europol nel caso in cui siano stati raccolti e messi a sua disposizione conformemente alla relativa legislazione nazionale.

Vittime e testimoni

I dati riguardanti queste categorie possono essere particolarmente sensibili considerata la posizione di tali persone. Qualora i dati relativi sono trattati in archivi di analisi, l'ACC

ritiene che, laddove possibile, debba essere rispettato l'anonimato.

Responsabilità degli Stati membri

Non è sempre possibile per uno Stato membro, partecipante a un progetto di analisi, valutare i dati prima di trasmetterli all'Europol. Ciononostante, l'articolo 15 della convenzione Europol stabilisce chiaramente che la trasmissione dei dati all'Europol e la loro introduzione spetta agli Stati membri. Ciascuno Stato membro deve pertanto adottare misure per garantire che i dati trasmessi all'Europol riguardino reati coperti dal mandato dell'Ufficio europeo di polizia.

In mancanza di tali misure, nella pratica, gli Stati membri rischiano di trasmettere dati all'Europol senza avere alcuna certezza che tali informazioni rientrino nell'attuale ambito di competenze dell'Ufficio. Si verrebbe a creare così una situazione in cui l'Europol tratterebbe dei dati al di fuori del suo mandato, agendo pertanto in violazione della convenzione Europol (articoli 2 e 10).

Il 2 luglio 2002 il Regno di Danimarca ha proposto un'iniziativa volta a realizzare un protocollo destinato a modificare la convenzione Europol. Una delle proposte riguardava la procedura di costituzione di un archivio di analisi. Il direttore dell'Europol veniva nominato autorità responsabile della costituzione di tale archivio di analisi. In tale proposta il consiglio di amministrazione non aveva più alcun ruolo nell'approvazione della costituzione di questi archivi, ma aveva il diritto di ordinare al direttore la chiusura di un archivio o la modifica della decisione costitutiva. La funzione di controllo per il consiglio di amministrazione cambiava quindi da proattiva a reattiva. La procedura attuale contempla la possibilità che l'ACC formuli osservazioni prima dell'approvazione della costituzione di un archivio di analisi. La proposta invece prevedeva la costituzione dell'archivio prima della possibilità di formulare osservazioni da parte dell'ACC.

Nel parere espresso in merito all'iniziativa danese (parere del 3 ottobre 2002, n. 02-55), l'ACC ha sottolineato che la sua funzione di controllo proattiva è da considerarsi un aspetto fondamentale per quanto riguarda la salvaguardia dei diritti dell'individuo in relazione alla costituzione di archivi di analisi. (Questo particolare ruolo proattivo dell'ACC riveste un'elevata importanza in termini di salvaguardia dei diritti dell'individuo.)

L'attuale procedura di notifica di un progetto di costituzione di un archivio di analisi riconosce all'ACC la facoltà di intervenire prima che i dati personali siano trattati, mentre l'emendamento della convenzione Europol consentirebbe di farlo soltanto a trattamento dei dati avviato. Nel caso in cui l'ACC volesse suggerire la chiusura di un archivio o la modifica di una decisione costitutiva, e il consiglio di amministrazione giungesse alla stessa conclusione, il trattamento dei dati e la loro divulgazione potrebbero essere già iniziati da tempo.

2. Cooperazione con Stati e organismi terzi

Dal momento che la criminalità organizzata non è un fenomeno limitato esclusivamente agli Stati membri dell'Unione europea, l'Europol ha bisogno di cooperare con Stati e organismi terzi. Secondo il Consiglio dell'Unione europea, l'efficacia della lotta contro forme di criminalità organizzata attraverso l'Europol deve essere corroborata da rapporti adeguati tra l'Ufficio e Stati e organismi terzi, con un conseguente scambio reciproco di dati. La convenzione Europol crea i presupposti per una cooperazione di questo tipo e il Consiglio dell'Unione europea ha stabilito delle norme generali per quanto riguarda la ricezione e la trasmissione di dati a Stati e organismi terzi.

Per quanto riguarda i dati di carattere personale, trovano applicazione l'atto del Consiglio, del 3 novembre 1998, (GU C 26 del 30.1.1999) che stabilisce le norme per la ricezione da parte dell'Europol di informazioni provenienti da Stati e organismi terzi e l'atto del Consiglio del, 12 marzo 1999, (GU C 88 del 30.3.1999) che stabilisce le norme per la trasmissione di dati di carattere personale da parte dell'Europol a Stati o organismi terzi.

In aggiunta a tali disposizioni di carattere generale, il Consiglio dell'Unione europea nella sua decisione del 27 marzo 2000 (GU C 106 del 13.4.2000) ha fissato le condizioni

che autorizzano il direttore dell'Europol ad avviare negoziati per la conclusione di accordi con Stati terzi ed organismi non connessi all'Unione europea.

Ricezione dei dati

Talvolta Stati o organismi terzi trasmettono dati all'Europol attraverso contatti dello stesso Ufficio europeo di polizia oppure di Stati membri Tale trasmissione può avvenire direttamente all'Europol oppure tramite uno Stato membro. L'ACC, al momento di formulare un parere su una decisione costitutiva di un archivio di analisi, si è domandata se la ricezione di dati da parte dell'Europol provenienti da Stati o organismi terzi, senza l'esistenza di un accordo, fosse conforme alla convenzione Europol.

Secondo l'Europol, le norme riguardanti la ricezione di dati da Stati ed organismi terzi lasciano aperta la possibilità di ricevere informazioni senza che esista un accordo. Il 24 gennaio 2001 l'Europol ha informato l'ACC della sua politica interna dichiarando che *"se non sussiste alcun accordo di cooperazione l'Europol non deve ricevere dati provenienti da terzi"*.

Ricezione e trasmissione di dati

La regola fondamentale alla base della cooperazione con Stati ed organismi terzi, se la cooperazione prevede anche la trasmissione di dati di carattere personale, è l'esistenza di un accordo. In casi eccezionali il direttore dell'Europol può decidere in merito a una trasmissione di dati.

Negoziati e accordi

Ai sensi della convenzione Europol (articolo 18), degli atti e della decisione del Consiglio, l'ACC è interpellata nelle varie fasi dello sviluppo della cooperazione con Stati o organismi terzi.

La prima fase riguarda l'autorizzazione del Consiglio dell'Unione europea all'Europol di avviare negoziati con Stati terzi e organismi non europei. Tale autorizzazione può essere concessa dopo una valutazione della legislazione e della prassi amministrativa dello Stato terzo o organismo terzo in materia di protezione dei dati, in particolare per quanto riguarda l'autorità responsabile delle questioni di protezione dei dati. L'Europol deve presentare al consiglio di amministrazione una relazione in cui viene illustrata la situazione esistente nello Stato terzo o organismo terzo, in cui si conclude che non esistono ostacoli all'avvio del negoziato. La relazione tratta anche gli aspetti legati alla protezione dei dati. Il consiglio di amministrazione consulta l'ACC su tali relazioni (articolo 1, paragrafo 5, decisione del Consiglio dell'Unione europea del 27 marzo 2000). L'ACC è stata consultata in merito all'avvio di negoziati con trenta Stati terzi e con un organismo terzo (cfr. pareri al punto VII, Allegato-A).

Nella prima fase di questo processo l'ACC ha il compito di accertare se, sulla base della relazione presentata dal consiglio di amministrazione , esistono impedimenti dal punto di vista della protezione dei dati all'avvio delle negoziazioni. Il parere dell'ACC non può essere considerato una attestazione dell'adeguatezza del livello di protezione dei dati. Inoltre, nel suo parere l'ACC esprime i seguenti aspetti specifici della protezione dei dati che devono essere presi in considerazione nelle negoziazioni:

La trasmissione di dati di carattere personale è ammissibile soltanto qualora la finalità e il motivo della trasmissione siano sufficientemente chiari e rientrino (a) nella sfera della convenzione Europol e (b) nell'ambito dell'accordo tra l'Europol e lo Stato o organismo terzo.

I dati trasmessi dall'Europol devono essere utilizzati esclusivamente per gli scopi specificati nell'accordo (gli scopi precisati nella convenzione Europol).

Lo Stato o organismo terzo è giuridicamente vincolato a rettificare o cancellare i dati ricevuti dall'Europol appena decada la pertinenza rispetto alla finalità per la quale sono stati trasmessi.

I termini previsti per l'archiviazione di dati personali indicati nella convenzione Europol e nelle relative norme di applicazione devono essere applicati ai dati trasmessi dall'Europol allo Stato o organismo terzo onde evitare che questi dati siano archiviati per un periodo più lungo di quello concesso all'Europol.

La ritrasmissione a Stati terzi di dati personali ricevuti dall'Europol deve essere vietata.

Un collegamento diretto tra i sistemi informatici dell'Europol e dello Stato terzo costituirebbe una violazione della convenzione Europol.

La trasmissione di dati di carattere personale dall'Europol deve seguire una procedura volta ad assicurare un adeguato livello di sicurezza dei dati nello Stato o organismo terzo.

L'archiviazione e l'uso dei dati devono essere adeguatamente protetti.

La trasmissione di dati dall'Europol è ammissibile soltanto se lo Stato terzo dimostra caso per caso un'esigenza chiara e motivata di trasmissione di tali dati.

L'Europol deve notificare senza indugio allo Stato o organismo terzo le eventuali rettifiche apportate ai dati trasmessi dall'Europol.

Lo Stato o organismo terzo, una volta ricevuta tale notifica, è giuridicamente vincolato a rettificare o cancellare i dati ricevuti dall'Europol conformemente alla suddetta notifica.

L'attuazione dell'accordo deve essere sottoposta ad un'adeguata sorveglianza e deve essere introdotta una disposizione che preveda la responsabilità dello Stato o organismo terzo nei confronti dei singoli individui in caso di mancato rispetto dell'accordo e di trattamento non autorizzato o incorretto dei dati.

Il livello di sicurezza dei dati che lo Stato o organismo terzo è tenuto a garantire, riguardo ai dati di carattere personale trasmessi dall'Europol, deve essere valutato tenendo conto del contesto stabilito nell'articolo 25 della convenzione Europol.

In tre occasioni l'ACC, sulla base della relazione dell'Europol, ha dichiarato che prima di avviare la trasmissione dei dati sensibili, occorre colmare le lacune esistenti nel diritto interno dello Stato terzo e nelle norme dell'Interpol relativamente al trattamento di questi dati.

Dopo i fatti dell'11 settembre 2001, si è avvertita una forte necessità di costruire una cooperazione tra Europol e Stati Uniti. All'ACC è stato richiesto un parere nella procedura di autorizzazione all'avvio dei negoziati con gli Stati Uniti. Contravvenendo alla normale procedura, data le sollecitazioni del momento e la mancanza di informazioni che avrebbero dovuto essere fornite dagli Stati Uniti entro i termini, l'Europol non è stato in grado di sottoporre all'ACC una relazione sulla legislazione e sulla prassi amministrativa vigenti negli Stati Uniti relativamente alla protezione dei dati.

L'ACC ha pertanto riferito al consiglio di amministrazione di non essere in grado di formulare un parere sul livello di protezione dei dati negli Stati Uniti, mancando una relazione da parte dell'Europol. Inoltre l'ACC ha dichiarato che soltanto un accordo ufficiale con gli Stati Uniti costituisce il fondamento legale necessario per la cooperazione tra Europol e Stati Uniti.

L'ACC ha osservato esplicitamente che la legislazione sulla protezione dei dati e la prassi amministrativa in vigore negli Stati Uniti differiscono per molti aspetti dal quadro giuridico dell'Europol. Anche se queste differenze non costituiscono un impedimento a un avvio delle negoziazioni, è necessario risolverle in modo appropriato nel corso dei negoziati. L'ACC ha quindi richiesto con fermezza di essere tenuta al corrente e di partecipare al processo per la risoluzione dei problemi inerenti alla protezione dei dati nel corso delle negoziazioni.

Quando l'Europol vuole avviare delle negoziazioni con un organismo connesso all'Unione europea, il direttore dell'Europol deve chiedere l'autorizzazione del consiglio di amministrazione. In tale procedura l'ACC non viene consultata (atto del Consiglio del 12.03.1999, articolo 3, paragrafo 4). Al momento della conclusione dell'accordo, il consiglio di amministrazione può approvarlo soltanto previo parere dell'ACC.

La seconda fase è il momento in cui il consiglio di amministrazione, nell'ambito delle attività di preparazione per l'approvazione della conclusione dell'accordo da parte del Consiglio,

consulta l'ACC (articolo 3, paragrafo 3 dell'atto del Consiglio del 12 marzo 1999), la quale giudica il progetto di accordo sotto ogni aspetto della protezione dei dati contemplato dalla convenzione Europol, inclusi gli aspetti specifici espressi nel parere riguardante la (non) esistenza di impedimenti all'avvio dei negoziati. L'ACC non ha sollevato obiezioni sulla conclusione di accordi con gli Stati terzi in merito ai quali è stata consultata, ma ha suggerito delle variazioni di alcuni accordi. Per quanto concerne l'accordo con Interpol, il parere positivo dell'ACC è stato subordinato alla rettifica di alcuni punti specifici dell'accordo.

Come già stabilito nella prima fase del processo, la valutazione del progetto di accordo tra Europol e Stati Uniti ha riconfermato i diversi approcci in materia di protezione dei dati sia nella legislazione, sia nella prassi.

Nel suo parere (parere del 3 ottobre 2002, n.02-65), l'ACC ha riconosciuto i considerevoli progressi che sono stati compiuti durante i negoziati tra l'Europol e gli Stati Uniti d'America. Il progetto di accordo è l'espressione di uno sforzo comune per trovare un equilibrio tra la necessità di combattere gravi forme di criminalità e la salvaguardia dei diritti dell'individuo, prendendo in considerazione le diverse strutture giuridiche ed amministrative di entrambe le parti.

Anche se alcuni argomenti hanno dovuto essere ulteriormente chiariti con uno scambio di note, l'ACC ha espresso il parere che il Consiglio era nella posizione di poter autorizzare il direttore dell'Europol a concludere l'accordo.

I casi eccezionali

Conformemente a quanto previsto dall'articolo 4 dell'atto del Consiglio del 12 marzo 1999, in tre occasioni il direttore dell'Europol ha informato l'ACC della sua decisione di trasmettere dati a uno Stato o organismo terzo in via eccezionale.

Due di tali decisioni si riferiscono agli eventi dell'11 settembre 2001. Oltre a decidere specificatamente in merito ad alcuni dati, il direttore dell'Europol ha concesso un'autorizzazione generale di trasmissione di dati agli Stati Uniti, ai fini delle indagini sugli atti terroristici.

Questa autorizzazione si deve interpretare come una misura temporanea per creare un rapporto di collaborazione con gli Stati Uniti, in attesa della conclusione dell'accordo ufficiale. L'ACC ha informato il direttore dell'Europol che una condizione permanente di un'eccezione, anche nel caso dei fatti dell'11 settembre 2001, non può sostituire stabilmente la normale norma per la trasmissione di dati di natura personale. L'ACC ha suggerito di rettificare la decisione del direttore dell'Europol e di applicare un termine all'autorizzazione. Secondo il parere dell'ACC tale autorizzazione non può più essere valida dopo il 1° luglio 2002.

3. Atto del consiglio del 12 marzo 1999

Le norme per la trasmissione di dati di carattere personale escludono qualsiasi ritrasmissione di dati personali che siano stati trasmessi dall'Europol a uno Stato terzo o organismo terzo. stato chiesto il parere dell'ACC su una proposta per autorizzare questa ritrasmissione a uno Stato/organismo terzo, nel caso in cui sia lo Stato membro responsabile dei dati, sia l'Europol fossero d'accordo.

Il divieto di ritrasmissione costituisce una parte integrante del sistema creato dalla convenzione Europol. I dati personali possono essere trasmessi da Stati/organismi terzi soltanto qualora esista un adeguato livello di protezione e sia stato concluso un accordo con lo Stato/organismo terzo in questione, che garantisce i diritti delle persone. Affinché la trasmissione sia legittima, queste due condizioni fondamentali devono essere soddisfatte. L'ACC ha sottolineato che autorizzare le ritrasmissioni senza alcun limite costituirebbe una violazione di questo sistema (pareri n. 00-24, 01-12 e 01-34)

L'ACC, riconoscendo che l'esclusione totale della ritrasmissione di dati di carattere personale può costituire un problema per l'Europol e, in particolare, per i rapporti dell'Europol con Stati ed organismi terzi, ha formulato delle condizioni che devono essere soddisfatte prima che la ritrasmissione possa avere luogo. Tali condizioni devono essere rese attuative in

un atto del Consiglio e prese in considerazione nella conclusione degli accordi con Stati o organismi terzi.

Nel suo parere, l'ACC ha dichiarato che l'emendamento proposto (e rivisto) —che permette la ritrasmissione di dati personali da parte di organismi terzi in caso di accordo con lo Stato o organismo terzo in questione che includa i dati provenienti dalla ritrasmissione nonché, in taluni casi eccezionali di cui all'articolo 2 delle norme di trasmissione di dati personali, sia accettabile alle condizioni delineate nel presente parere.".

Tali condizioni sono le seguenti:

- *deve essere concluso un accordo tra l'Europol e l'organismo terzo in oggetto prima che quest'ultimo possa trasmettere ulteriormente dati a carattere personale;*
- *la ritrasmissione di dati personali deve basarsi su circostanze veramente eccezionali conformemente all'articolo 2, paragrafo 1, lettera b), delle norme, circostanze che devono essere debitamente motivate per ciascun singolo caso;*
- *deve esistere un'esigenza chiara e fondata per la trasmissione di dati personali a Stati o organismi terzi tramite un organismo intermedio invece di trasmetterli direttamente;*
- *il direttore dell'Europol e gli Stati membri che hanno fornito i dati sono tenuti a dare il loro accordo previo alla ritrasmissione in ciascun singolo caso;*
- *il direttore dell'Europol deve garantire e provare che la protezione dei dati nello Stato o organismo terzo ricevente è di grado adeguato, ai sensi dell'articolo 2, paragrafo 2, delle norme;*
- *il direttore dell'Europol è tenuto a registrare ogni caso di ritrasmissione e ad informarne ogni volta l'ACC, in virtù dell'articolo 4 delle norme.*

L'atto del Consiglio del 12 marzo 1999 è stato modificato il 28 febbraio 2002 (GU C 76 del 27.3.2002) secondo il parere dell'ACC.

4. Progetti operativi degli Stati membri con sostegno dell'Europol

Il gruppo d'ispezione dell'ACC che ha condotto un'ispezione presso l'Europol nel novembre 2000 ha segnalato l'esistenza di archivi di analisi in funzione per questo tipo di progetti, meglio conosciuti come MSOPES. Nell'ambito di questi progetti l'Europol fornisce servizi di analisi agli Stati membri. In alcuni casi l'Europol crea degli archivi di analisi sotto la responsabilità dello Stato membro e non applica l'articolo 10 della convenzione.

L'ACC ha quindi contattato l'Europol per avere ulteriori informazioni in merito alla prassi dei MSOPES. Il direttore dell'Europol ha riferito all'ACC che a suo avviso "l'attuale quadro giuridico definito dalla convenzione Europol consente a quest'ultimo di contribuire ai servizi di analisi". L'ACC si è dichiarata d'accordo con il giudizio del direttore dell'Europol, secondo cui un'azione efficace contro gravi forme di criminalità richiede l'adozione di strategie ed iniziative comuni, nonché una stretta collaborazione. In questo campo il ruolo dell'Europol è chiaramente riconosciuto e ben definito nella convenzione Europol. L'ACC ha quindi preso atto dei vari modi per rendere questo tipo di servizio, concentrando la sua attenzione sull'esistenza di archivi di analisi come sostegno al MSOPES da parte dell'Europol.

L'ACC ha concluso affermando che le funzioni dell'Europol illustrate nella convenzione sono definite in linea generale. Tuttavia in alcuni punti la convenzione specifica qual è il compito dell'Europol. L'articolo 7 (istituzione del sistema d'informazione) e l'articolo 10 (archivi di lavoro per fini di analisi) mettono in relazione l'esistenza del sistema di informazione e degli archivi di analisi con lo svolgimento della funzione dell'Europol (articolo 7) o il raggiungimento dell'obiettivo indicato nell'articolo 2, paragrafo 1 della Convenzione.

Considerati i compiti di carattere generale dell'Europol citati nell'articolo 3, paragrafo 1 e la particolare funzione di analisi di cui all'articolo 10 della Convenzione, la creazione di archivi di analisi può avvenire soltanto nel quadro dell'articolo 10. Ciò significa che a giudizio dell'ACC, l'assistenza sotto forma di analisi dell'Europol costituendo archivi di analisi al di fuori dell'ambito dell'articolo 10 della convenzione Europol, è in contrasto con la convenzione stessa.

L'iniziativa danese del 2 luglio 2002 di un protocollo per emendare la convenzione Europol conteneva una disposizione che autorizzava di fornire sostegno analitico a indagini in Stati membri, conformemente alla legislazione interna del paese che richiede tale assistenza, e sotto esclusiva responsabilità dello Stato membro.

Nel suo parere (parere del 3 ottobre 2002, n. 02-55), l'ACC ha obiettato con decisione a questa proposta volta a disciplinare la situazione in cui alcuni Stati membri richiedono assistenza analitica, anche per quelle indagini che rientrano chiaramente nell'obiettivo dell'Europol, senza tuttavia l'intenzione, da parte di tali Stati membri, di voler partecipare a un archivio di analisi nel quadro giuridico e sotto la responsabilità dell'Europol. L'ACC ha dichiarato che per quanto riguarda la protezione dei dati, è cruciale mantenere un solo sistema giuridico, quale è stato sviluppato nell'articolo 10 della convenzione Europol per archivi di analisi. L'ACC ha sottolineato che una situazione in cui si possano applicare svariati sistemi giuridici su archivi di analisi identici, per contenuto, obiettivo e struttura, porterà a mancanza di trasparenza e renderà difficile, se non impossibile, la comprensione del quadro giuridico sia per tutti i partecipanti al processo analitico, sia per l'individuo a cui si riferiscono i dati trattati.

5. Iniziativa danese per emendare la convenzione Europol

Il Regno di Danimarca ha proposto il 2 luglio 2002 una iniziativa per un protocollo per emendare la convenzione Europol. Tale iniziativa prevedeva alcune modifiche fondamentali alla convenzione Europol. Alcune delle proposte formulate e il commento dell'ACC (parere del 3 ottobre 2002, n. 02-55) sono già state illustrate nel capitolo A, punti 1 e 4.

Obiettivo dell'iniziativa era di rafforzare l'efficienza migliorata e la cooperazione tra Stati membri, affermando il ruolo chiave dell'Europol rispetto alla cooperazione tra le autorità degli Stati membri nel campo delle indagini internazionali.

Nella sua risposta l'ACC ha dichiarato che dal punto di vista della protezione dei dati, questo ruolo chiave ed una lotta efficace contro forme gravi di criminalità internazionale devono essere accompagnati da uno sforzo comune dell'Europol e di tutti gli Stati membri ai fini di un corretto trattamento dei dati, della riservatezza, dell'attendibilità e della qualità dei dati.

Sono state avanzate proposte di emendamento relative a vari aspetti della convenzione Europol e al lavoro svolto da quest'ultimo. L'ACC ha commentato tutte le proposte che riguardavano il trattamento dei dati personali. Tali proposte si riferivano a svariati aspetti della convenzione Europol, quali l'obiettivo dell'Europol, le sue funzioni, i contatti con gli Stati membri, gli archivi di lavoro analitici, la conservazione dei dati, il controllo sul richiamo dei dati e sulla loro trasmissione a Stati e organismi terzi.

L'iniziativa prevedeva anche l'introduzione di un sistema per informazioni di base per l'esecuzione delle funzioni dell'Europol. L'ACC ha risposto dicendo che la proposta non era sufficientemente specifica ed erano necessari ulteriori chiarimenti.

Per permettere alle autorità competenti degli Stati membri di consultare il sistema di informazione dell'Europol è stata introdotta la possibilità di interrogare il sistema. Anche se un'ulteriore incentivazione della cooperazione tra gli Stati membri potrebbe renderlo necessario, l'ACC, considerato l'obiettivo dell'Europol e la categoria dei dati trattati, ha sottolineato che la comunicazione deve avvenire limitatamente a quelle autorità competenti che hanno un incarico legalmente riconosciuto nella prevenzione e nella lotta di gravi forme di criminalità internazionale.

In generale l'ACC ha concluso che l'iniziativa volta a modificare la convenzione Europol condurrebbe a una frammentazione della cooperazione tra Stati membri ed Europol e non a un ruolo chiave per l'Europol, con conseguenze negative sulla qualità della protezione delle informazioni di quegli individui i cui dati sono, o saranno, trattati dall'Europol. L'ACC ha invitato caldamente a riconsiderare il progetto di protocollo.

B. Ispezioni

Conformemente all'articolo 24, paragrafo 1 della convenzione Europol, l'ACC ha l'incarico di vigilare sull'attività dell'Europol per accertarsi che la memorizzazione, il trattamento e l'utilizzazione dei dati detenuti dai servizi dell'Europol non ledano i diritti delle persone.

Il 29 giugno 2000 l'ACC ha istituito un gruppo di ispezione incaricato di condurre un'indagine sulla sicurezza e sugli archivi di lavoro per fini di analisi. In previsione dell'ispezione programmata nel mese di novembre 2000 e di altre future, l'Europol e l'ACC hanno adottato un protocollo su particolari accordi presi con l'Europol, riguardanti visite ed ispezioni da parte dell'ACC.

Durante la preparazione e lo svolgimento dei controlli, il gruppo di ispezione ha utilizzato come base i principi e le raccomandazioni pertinenti dell'Information Systems Audit and Control Association (ISACA), adeguati alle caratteristiche specifiche dell'installazione, nonché alle limitazioni legate all'ambiente, agli obiettivi, alle informazioni disponibili e alla durata dell'ispezione. Per condurre l'ispezione sono stati anche presi in considerazione criteri europei, quali elencati nei documenti ITSEC e ITSEM, che sono considerati dagli Stati membri dell'Unione europea come la principale fonte di riferimento ufficiale nel campo, conformemente alla raccomandazione del Consiglio del 7 aprile 1995 (95/144/CEE). Il progetto di relazione è stato presentato all'Europol nel dicembre 2000. Dopo aver ricevuto i commenti dell'Europol nell'aprile 2001, la relazione di ispezione è stata modificata ed adottata in occasione della riunione dell'ACC il 12 ottobre 2001.

Tenuto conto dei risultati ottenuti dal gruppo di ispezione, l'ACC ha concluso che l'Europol soddisfa i requisiti citati nei relativi regolamenti e inoltre opera conformemente ai principi di buona prassi. Tale conclusione si riferisce soltanto agli aspetti oggetto di ispezione. L'ACC ha formulato svariate raccomandazioni e ha sottolineato la necessità di applicare le misure necessarie menzionate nelle raccomandazioni per migliorare la conformità ai regolamenti.

Nel mese di marzo 2002 è stata condotta una seconda ispezione. Alla riunione del 13 dicembre 2001, l'ACC ha istituito un gruppo di ispezione incaricato di condurre un'indagine di verifica da parte dell'Europol delle raccomandazioni dell'ACC formulate nella relazione di ispezione del 12 ottobre 2001.

L'ACC è soddisfatta di come l'Europol abbia considerato seriamente le raccomandazioni contenute nella sua prima relazione di ispezione. L'Europol ha già intrapreso numerose iniziative per attuare le raccomandazioni. Alcuni progetti sono stati avviati per assistere l'applicazione delle raccomandazioni che devono ancora essere attuate. La maggior parte di questi progetti devono ancora giungere a conclusione. deplorevole che il loro completamento abbia subito ritardi, non causati da mancanza di determinazione da parte dell'Europol, bensì dalla complessità che l'attuazione dei progetti comporta, con l'approvazione di tutte le parti coinvolte e dai cambiamenti avvenuti nel dipartimento TS. indispensabile che questi progetti siano portati a termine senza ulteriori ritardi. particolarmente importante che quei progetti che incidono su altre iniziative, segnatamente il progetto di analisi del rischio, procedano verso una rapida conclusione. L'ACC ha comunicato all'Europol il suo desiderio di essere tenuta al corrente dei progressi compiuti e della riuscita attuazione delle raccomandazioni che dipendono dal loro completamento dei progetti.

C. Altre attività

1. Contatti

Il consiglio di amministrazione e il direttore dell'Europol insieme all'ACC hanno riconosciuto la necessità di incontrarsi regolarmente. Nella pratica queste riunioni avvengono in coincidenza con il cambiamento della presidenza dell'Unione europea ogni sei mesi. Gli incontri contribuiscono a una migliore comprensione delle diverse responsabilità dei tre partecipanti.

L'ACC ha organizzato nel giugno 2002 una riunione con i rappresentanti delle autorità per la protezione dei dati in Stati ed organismi terzi con cui l'Europol ha concluso un accordo di cooperazione e di scambio dei dati di carattere personale. Tutti i partecipanti hanno convenuto che la protezione dei dati è meglio promossa condividendo informazioni ed esperienze tra le autorità di protezione dei dati che controllano la trasmissione e il successivo trattamento dei dati. Alla conclusione di questa prima riunione tutti i partecipanti sostenevano la necessità di ripetere l'esperienza a scadenza annuale.

2. Studi

L'ACC ha promosso un questionario sul diritto di accesso. Tale questionario è incentrato sulle disposizioni di legge negli Stati membri che riguardano il diritto di accesso ad archivi di polizia. Questo studio ha consentito di avere una visione generale di un aspetto molto importante: il modo in cui questo diritto di accesso è gestito nella pratica. Una relazione su questo studio è prevista nel 2003.

L'ACC ha intenzione di compiere delle indagini sulla qualità dei dati trattati dall'Europol. I dati che sono trattati dall'Europol possono essere utilizzati in ciascuno Stato membro nell'ambito di attività di prevenzione e lotta dei reati penali che rientrano sotto la competenza dell'Europol, nonché per combattere altre gravi forme di criminalità. Considerato il tipo di dati trattati, essi influiscono pesantemente sul modo in cui un individuo potrebbe essere trattato negli Stati membri. Dopo tutto si tratta di persone sospettate di avere connessioni con la criminalità internazionale in una struttura organizzata. Pertanto un elevato livello qualitativo dei dati è della massima importanza.

Dato che il valore dell'Europol nella lotta alla criminalità internazionale mediante il mantenimento di un sistema di informazione si fonda sulla condivisione di dati (provenienti da Stati membri, Stati ed organismi terzi e archivi di analisi) relativi a un certo individuo, è importante che queste informazioni forniscano una descrizione di quella persona pertinente, corretta e precisa.

III. Il futuro

L'Europol è un'organizzazione con il compito specifico di fornire alla cooperazione delle forze di polizia europee una dimensione supplementare. Agevolare lo scambio di dati, la loro analisi e condivisione mantenendo dei sistemi informatici rappresenta un aspetto importante delle funzioni dell'Europol. Per quanto le responsabilità relative al trattamento dati siano divise tra l'Europol e gli Stati membri, il successo dell'Europol e la riuscita dei suoi compiti specifici costituiscono in realtà una responsabilità comune per gli Stati membri e l'Europol. Il mandato dell'Europol riguarda la criminalità internazionale e pertanto necessita di una risposta comune a livello internazionale.

Un'organizzazione come l'Europol dipende sostanzialmente dalla cooperazione di altri. Dipende dall'inserimento di dati provenienti da diverse fonti e dalla volontà degli Stati membri di condividere le informazioni. Se non sono inseriti dei dati, oppure se la loro qualità non è adeguata, il lavoro aggiunto dell'Europol è a rischio. A questo punto le preoccupazioni relative alla protezione dei dati vanno di pari passo con l'applicazione della legge e l'interesse della sicurezza a livello europeo. Il principio della qualità dei dati è pertanto indispensabile sia per la protezione dei dati, sia per l'applicazione della legge e per il valore aggiunto dell'Europol.

Molte iniziative europee riguardano (l'ulteriore sviluppo) dell'applicazione della legge e la sicurezza in Europa. Alcune delle evoluzioni in questi campi come Eurojust, l'istituzione di un sistema di informazione doganale e lo sviluppo di un nuovo sistema di informazione di Schengen presentano degli elementi di un trattamento dei dati di natura personale a livello europeo. Inoltre sono intraprese iniziative per lo scambio di dati tra Europol, Eurojust e il sistema di informazione di Schengen. Anche le discussioni sulla funzione dell'Europol possono comportare implicazioni per il trattamento dei dati.

L'allargamento dell'Unione europea condurrà alla creazione di una dimensione comune tra l'Europol ed i paesi candidati. La condivisione di conoscenze circa il funzionamento delle forze di polizia e delle procedure correlate, come pure riguardo allo scambio di dati, giocherà un ruolo decisivo sia per i nuovi Stati membri sia per l'Europol medesimo. Su questa linea, si rileva che la maggior parte di tali paesi ha già provveduto a sottoscrivere un accordo di cooperazione con l'Europol.

In un contesto in cui i dati di carattere personale sono condivisi da organizzazioni o sistemi di informazione diversi, è evidente la necessità di investire nella qualità dei dati. La condivisione e l'utilizzo di questi dati da parte di autorità diverse, il processo di analisi per scoprire collegamenti particolari tra i dati oppure crearne dei nuovi, influirà notevolmente sul modo in cui le persone sono trattate nella loro vita privata. Gli Stati membri e l'Europol devono pertanto investire in un sistema di verifica e controllo per mettere a disposizione e mantenere un alto livello di qualità dei dati.

L'ACC controlla costantemente questi sviluppi in collaborazione con le altre autorità di controllo comune e ove necessario interviene. L'ACC verificherà che tali sviluppi tengano conto della tutela dei diritti degli individui e in particolare della protezione dei dati di natura personale. Se questi sviluppi hanno implicazioni a livello nazionale, l'ACC collaborerà con la relativa autorità di controllo nazionale.

L'ACC ispezionerà regolarmente l'Europol, cercando di mantenere il dialogo con l'Ufficio europeo di polizia ed altre istituzioni responsabili, per sostenere un livello adeguato di protezione dei dati. L'ACC investirà in (ulteriori) sviluppi nel campo dei metodi e delle procedure d'ispezione. Tali accertamenti possono riguardare l'attuazione generale dei principi dell'articolo 25 della convenzione Europol o altri obiettivi più specifici. Ciò tuttavia non significa che l'ACC ritiene di essere l'unico controllore. A livello nazionale degli ispettori controllano le unità nazionali dell'Europol e l'ufficiale incaricato della protezione dei dati dell'Europol ha una particolare funzione di controllo all'interno dell'organizzazione.

Data la peculiare posizione dell'Europol, l'autorità di controllo avrà il compito di incentivare e sostenere l'operato di questi vari controllori. La cooperazione tra l'ACC, i controllori nazionali degli Stati membri e degli Stati terzi con cui l'Europol ha un accordo sulla trasmissione di dati personali, sarà (ulteriormente) sviluppata. La protezione dei dati a livello dell'Europol è più efficace monitorando gli aspetti della protezione dei dati legati alla cooperazione nel campo dell'applicazione della legge a livello nazionale e di autorità di controllo comune. L'ACC incentiverà ulteriormente lo sviluppo di strumenti di controllo interno per l'Europol.

V. Comitato per i ricorsi

La convenzione Europol impone all'ACC di istituire un comitato per i ricorsi previsti dalla convenzione stessa. Il comitato per i ricorsi dell'ACC è stato istituito il 23 novembre 1998 e da allora si è riunito 14 volte. La procedura di ricorso e l'operato del comitato sono disciplinati nel Titolo III del Regolamento interno dell'ACC.

Chiunque desideri esercitare il proprio diritto di accesso a dati che lo riguardano oppure voglia che tali dati siano controllati, può inoltrare una richiesta all'autorità nazionale competente in qualsiasi Stato membro. Generalmente sono le autorità incaricate della protezione dei dati a essere preposte al ricevimento delle richieste. Le autorità competenti in questione sono obbligate a inoltrare immediatamente la richiesta all'Europol. L'Europol deve esaminare la richiesta entro tre mesi ed informare il richiedente che se non è soddisfatto della decisione presa può appellarsi alla ACC.

Per quanto l'Europol riceva regolarmente richieste di accesso o di controllo dei dati, sono stati presentati soltanto due ricorsi. Il 16 maggio 2002 il comitato ha pronunciato la sua decisione relativa al primo caso in una riunione pubblica.

VI. Parere del consiglio di amministrazione dell'Europol

Conformemente al disposto ai sensi dell'articolo 24, paragrafo 6, della convenzione Europol, il consiglio di amministrazione ha la possibilità di formulare un parere in merito alla relazione di attività.

Nessun commento in tal senso è pervenuto all'ACC da parte del consiglio di amministrazione.

Allegati

A. Pareri del periodo ottobre 1998 – ottobre 2002

N. 99-01	Parere relativo alle norme per la trasmissione di dati di carattere personale (15-01-99).
N. 99-08	Parere relativo al Regolamento interno (23-04-99).
N. 99-10	Parere relativo alla stesura delle relazioni sul richiamo dei dati di carattere personale dal sistema di informazione (23-04-99).
N. 99-15	Parere relativo al modello di decisione costitutiva e alle quattro decisioni costitutive (09-07-99).
N. 99-20	Parere su tre decisioni costitutive (01-11-99).
N. 00-02	Parere su due decisioni costitutive (15-03-00).
N. 00-07	Parere su una decisione costitutiva (08-05-00).
N. 00-08	Parere sull'istituzione di un segretariato permanente (19-04-00).
N. 00-09	Parere dell'ACC in merito al livello di protezione dei dati presso l'Interpol (07-06-00).
N. 00-10	Parere dell'ACC in merito al livello di protezione dei dati in Norvegia (07-06-00).
N. 00-12	Parere su una decisione costitutiva (19-07-00).
N. 00-18	Parere dell'ACC in merito al livello di protezione dei dati in Ungheria (20-10-00).
N. 00-19	Parere dell'ACC in merito al livello di protezione dei dati in Islanda (20-10-00).
N. 00-20	Parere dell'ACC in merito al livello di protezione dei dati in Polonia (20-10-00).
N. 00-22	Parere dell'ACC in merito al livello di protezione dei dati in Estonia (21-12-00).
N. 00-23	Parere dell'ACC in merito al livello di protezione dei dati in Slovenia (21-12-00).
N. 00-24	Parere sulla modifica delle Norme che regolano la trasmissione di dati personali in relazione alla ritrasmissione di dati personali (21-12-00).
N. 01-04	Parere su una decisione costitutiva (08-02-01).
N. 01-05	Parere su una decisione costitutiva (08-02-01).
N. 01-08	Parere relativo alla stesura delle relazioni sul richiamo dei dati di carattere personale dal sistema di informazione (08-02-01).
N. 01-09	Consiglio dell'ACC in merito al proposto sistema d'informazione dell'Europol (08-02-01).
N. 01-12	Parere sulla modifica delle Norme che regolano la trasmissione di dati personali in relazione alla ritrasmissione di dati personali (18-04-01).
N. 01-13	Parere dell'ACC in merito al livello di protezione dei dati nella Repubblica ceca (18-04-01).
N. 01-14	Parere su una decisione costitutiva modificata (18-04-01).

N. 01-15	Parere relativo al progetto di accordo da firmare tra Europol e Norvegia (02-05-01).
N. 01-16	Parere relativo al progetto di accordo da firmare tra Europol e Islanda (02-05-01).
N. 01-17	Parere relativo al progetto di accordo da firmare tra Europol e Interpol (02-05-01).
N. 01-21	Parere relativo al progetto di accordo da firmare tra Europol e Polonia (02-06-01).
N. 01-22	Parere relativo al progetto di accordo da firmare tra Europol e Ungheria (26-06-01).
N. 01-23	Parere relativo al progetto di accordo da firmare tra Europol e Estonia (02-06-01).
N. 01-24	Parere relativo al progetto di accordo da firmare tra Europol e Slovenia (26-06-01).
N. 01-25	Parere su una decisione costitutiva modificata (26-06-01).
N. 01-	Parere su due decisioni costitutive (16-10-01).
N. 01-31	Parere relativo all'uso delle attrezzature di analisi dell'Europol nei progetti operativi degli Stati membri con il sostegno dell'Europol (08-11-01).
N. 01-34	Parere sulla modifica delle Norme che regolano la trasmissione di dati personali in relazione alla ritrasmissione di dati personali (26-11-01).
N. 01-38	Parere dell'ACC in merito al livello di protezione dei dati negli Stati Uniti (26-11-01).
N. 01-39	Parere relativo al progetto di accordo da firmare tra Europol e Federazione svizzera (26-11-01).
N. 01-40	Parere relativo al progetto di accordo da firmare tra Europol e Repubblica ceca (26-06-01).
N. 02-01	Parere su una decisione costitutiva (06-03-02).
N. 02-08	Parere relativo alla decisione del direttore dell'Europol circa la trasmissione di dati personali alle forze di Polizia degli Stati Uniti d'America (06-03-02).
N. 02-10	Parere relativo al sistema di indice
N. 02-13	Parere su una decisione costitutiva (06-03-02).
N. 02-14	Parere su una decisione costitutiva (06-03-02).
N. 02-27	Parere relativo ai requisiti di verifica del nuovo sistema di analisi (15-05-02).
N. 02-46	Parere su una decisione costitutiva (26-06-02).
N. 02-47	Parere su una decisione costitutiva (26-06-02).
N. 02-48	Parere dell'ACC in merito al livello di protezione dei dati in Canada (26-06-02).
N. 02-49	Parere dell'ACC in merito al livello di protezione dei dati in Bulgaria (26-06-02).
N. 02-51	Parere dell'ACC in merito al livello di protezione dei dati nella Repubblica slovacca (26-06-02).
N. 02-54	Parere dell'ACC in merito al livello di protezione dei dati in Lituania (01-08-02).
N. 02-55	Parere relativo al progetto di atto del Consiglio che stabilisce un protocollo che modifica la convenzione Europol (03-10-02).
N. 02-60	Parere dell'ACC in merito al livello di protezione dei dati nella Repubblica di Lettonia (03-10-02).
N. 02-61	Parere dell'ACC in merito al livello di protezione dei dati a Cipro (03-10-02).
N. 02-62	Parere su una decisione costitutiva 03-10-02).
N. 02-65	Parere in merito al progetto di accordo da firmare tra l'Europol e gli Stati Uniti d'America (03-10-02).
N. 02-66	Parere su una decisione costitutiva 03-10-02).

B. RELAZIONI DEL PERIODO OTTOBRE 1998 – OTTOBRE 2002

-Relazione d'ispezione n. 01/00, adottata il 12-10-01
-Relazione d'ispezione n. 02-16, adottata il 26-06-02

C. NORME DI PROCEDURA

Atto n. 1/99 dell'Autorità di contollo comune dell'Europol del 22 aprile 1999
che stabilisce il proprio regolamento interno

L'AUTORITÀ DI CONTROLLO COMUNE,

vista la convenzione, basata sull'articolo K.3 del trattato sull'Unione europea, che istituisce un ufficio europeo di polizia (convenzione Europol), [1] in particolare l'articolo 24, paragrafo 7,

considerando che spetta all'autorità di controllo comune stabilire, con decisione presa all'unanimità, il proprio regolamento interno,

HA ADOTTATO IL SEGUENTE REGOLAMENTO INTERNO:

TITOLO I - FUNZIONI E COMPETENZE DELL'AUTORITÀ DI CONTROLLO COMUNE

Articolo 1. Funzioni

1. L'autorità di controllo comune è incaricata di vigilare, nel rispetto della convenzione, sull'attività dell'Europol per accertarsi che la memorizzazione, il trattamento e l'utilizzazione dei dati in possesso dei servizi dell'Europol non ledano i diritti della persona. Essa controlla inoltre la legittimità della trasmissione dei dati provenienti dall'Europol (articolo 24, paragrafo 1, prima e seconda frase, della convenzione).

2. A tal fine, l'autorità di controllo comune svolge in particolare le seguenti funzioni:
   a) esame delle decisioni costitutive degli archivi (articolo 12, paragrafo 1, seconda frase, e paragrafo 2, terza frase, della convenzione);
   b) esame delle disposizioni relative alla stesura delle relazioni sul richiamo di dati di carattere personale (articolo 16, prima frase, della convenzione);
   c) esame delle norme generali per la trasmissione di dati di carattere personale da parte dell'Europol agli Stati e ad organismi terzi (articolo 18, paragrafo 2, seconda frase, della convenzione);
   d) esame delle questioni relative a:
      - applicazione e interpretazione della convenzione connesse con l'attività dell'Europol per quanto riguarda il trattamento e l'utilizzazione di dati di carattere personale (articolo 24, paragrafo 3, primo caso, della convenzione),
      - controllo indipendente effettuato dalle autorità di controllo degli Stati membri (articolo 24, paragrafo 3, secondo caso, della convenzione), ?esercizio del diritto all'informazione (articolo 24, paragrafo 3, terzo caso, della convenzione), ?elaborazione di proposte armonizzate in vista di soluzioni comuni ai problemi che si presentano (articolo 24, paragrafo 3, quarto caso, della convenzione);
   e) verifica della legittimità e della correttezza dell'eventuale memorizzazione, rilevamento, trattamento ed utilizzazione di dati di carattere personale da parte dell'Europol su richiesta dell'interessato (articolo 24, paragrafo 4, della convenzione);
   f) stesura periodica di relazioni di attività (articolo 24, paragrafo 6, della convenzione).

Articolo 2. Competenze

1. Nello svolgimento delle sue mansioni, l'autorità di controllo comune è dotata delle competenze conferitele dalla convenzione.

2. In particolare, l'autorità di controllo comune è autorizzata ad ottenere informazioni dall'Europol, ad ottenere l'accesso a tutti i documenti e agli archivi cartacei, nonché a qualsiasi altra informazione memorizzata dall'Europol, nonché ad ottenere libero accesso in qualsiasi momento a tutti i locali dell'Europol (articolo 24, paragrafo 2, della convenzione). Ciò include l'informazione su hardware e software e l'accesso ai medesimi, ogniqualvolta sia

(1) GU C 316 del 27.11.1995, pag. 1

necessario per lo svolgimento delle funzioni dell'autorità di controllo comune. Le modalità possono essere fissate in accordi tra l'autorità di controllo comune e il consiglio di amministrazione dell'Europol.

Articolo 3. Comitati

1. L'autorità di controllo comune istituisce il comitato di cui all'articolo 24, paragrafo 7, della convenzione.

2. Può istituire una o più commissioni interne e determinarne la composizione e le competenze (articolo 24, paragrafo 8, della convenzione).

TITOLO II - REGOLAMENTO INTERNO DELL'AUTORITÀ DI CONTROLLO COMUNE

Articolo 4. Composizione

1. L'autorità di controllo comune è composta da al massimo due membri o rappresentanti di ciascuna delle autorità di controllo nazionali che costituiscono una delegazione. Ciascun membro può avere un supplente. I membri dell'autorità di controllo comune e i loro supplenti sono nominati per cinque anni dai rispettivi Stati membri (articolo 24, paragrafo 1, terza frase, della convenzione); tale mandato è rinnovabile.

2. I membri dell'autorità di controllo comune e i loro supplenti sono indipendenti, non ricevono istruzioni nello svolgimento delle loro mansioni e sono soggetti soltanto alla legge. In particolare, essi non devono essere contemporaneamente membri di un altro organismo istituito secondo la convenzione o far parte del personale dell'Europol.

In casi di conflitto di interessi, la persona interessata notifica tale interesse e non partecipa alle discussioni e alle decisioni sul caso e può, ove necessario, essere esclusa a maggioranza dei voti espressi a scrutinio segreto dalle delegazioni che partecipano alla riunione. La persona interessata viene ascoltata prima che si proceda all'esclusione, ma non partecipa alla decisione. Una persona che si ritiri o venga esclusa può farsi sostituire dal supplente.

3. Possono essere nominati membri dell'autorità di controllo comune o supplenti solo coloro che possiedono le capacità richieste (articolo 24, paragrafo 1, terza frase, della convenzione). Particolare attenzione viene rivolta ai requisiti relativi alla designazione del comitato per i ricorsi.

4. Qualora un membro dell'autorità di controllo comune non possa assistere ad una riunione, può farsi rappresentare dal suo supplente.

5. La carica di membro dell'autorità di controllo comune termina quando la persona in questione si dimette o cessa di essere membro o rappresentante dell'autorità di controllo nazionale, a meno che il suo mandato sia confermato dallo Stato membro interessato. La nomina a membro non può essere revocata se non in base alla legislazione nazionale. La presente disposizione si applica, con gli opportuni adattamenti, anche ai supplenti.

Articolo 5. Presidenza

1. L'autorità di controllo comune elegge al suo interno un presidente e un vicepresidente a maggioranza di due terzi dei voti espressi, a scrutinio segreto, dalle delegazioni presenti. Il vicepresidente non può essere membro della delegazione del presidente. Se nessuno dei candidati ottiene la maggioranza richiesta nel primo turno di votazione, si procede a un secondo turno tra i due candidati che hanno ottenuto il maggior numero di voti. Il presidente e il vicepresidente sono eletti per un periodo di due anni, prorogabile per un secondo mandato di un anno.

2. Il presidente rappresenta l'autorità di controllo comune e ne presiede le riunioni. Egli vigila sul corretto andamento dei lavori; convoca le riunioni dell'autorità di controllo comune e ne fissa il luogo, la data e l'ora. Apre e chiude le sedute, prepara l'ordine del giorno provvisorio e assicura l'esecuzione delle decisioni dell'autorità di controllo comune.

3. In caso di assenza del presidente, il vicepresidente ne fa le veci. In assenza del vicepresidente, il membro più anziano in termini di età fa le veci del vicepresidente. La prima riunione dell'autorità di controllo comune è convocata e presieduta dal membro più anziano in termini di età sino all'elezione del presidente.

4. L'autorità di controllo comune può, al fine di preparare i propri lavori in merito a questioni particolari, nominare tra i propri membri, su proposta del presidente, uno o più relatori. In caso d'urgenza, il presidente può procedere a tale nomina direttamente. In tal caso egli ne informa senza indugio i membri dell'autorità di controllo comune.

5. Il presidente o la maggioranza delle delegazioni possono chiedere la presenza del direttore alle riunioni e invitare ad esse membri del personale dell'Europol, esperti nazionali, ufficiali di collegamento e altre persone.

Articolo 6. Metodi di lavoro

1. L'autorità di controllo comune si riunisce almeno quattro volte all'anno. Si riunisce altresì su iniziativa del presidente e ogniqualvolta almeno tre delegazioni presentino una richiesta scritta motivata ovvero una proposta orale nel corso di una precedente riunione. Il presidente del consiglio di amministrazione e il direttore dell'Europol possono proporre punti da iscrivere all'ordine del giorno e proporre la convocazione dell'autorità di controllo comune.

2. Ad eccezione dei casi ritenuti urgenti dal presidente, la notifica della convenzione della riunione deve giungere almeno due settimane prima della riunione e ad essa vengono acclusi l'ordine del giorno provvisorio e i documenti necessari per la riunione, a meno che la natura dei documenti stessi non lo consenta. L'ordine del giorno definitivo viene adottato all'inizio di ogni riunione.

3. Le riunioni dell'autorità di controllo comune sono valide solo se vi partecipano almeno i due terzi delle delegazioni. Le decisioni vengono adottate a maggioranza semplice delle delegazioni presenti, salvo che il presente regolamento interno disponga diversamente. Ciascuna delegazione ha diritto a un voto. In caso di parità, prevale il voto del presidente.

4. Le riunioni dell'autorità di controllo comune non sono pubbliche. I suoi documenti sono riservati, a meno che l'autorità di controllo comune disponga diversamente. Tuttavia, i documenti trasmessi dall'Europol sono soggetti alle norme sulla segretezza di cui all'articolo 31, paragrafo 1, della convenzione.

5. L'autorità di controllo comune si riunisce sulla base di documenti e progetti redatti in tutte le lingue ufficiali delle istituzioni dell'Unione europea. Sono ammesse deroghe a tale regola solo in casi di urgenza. Tuttavia, ogni delegazione ha il diritto di chiedere una traduzione nella propria lingua.

6. Le decisioni dell'autorità di controllo comune possono essere adottate tramite procedura scritta, sempreché tale procedura sia stata approvata da tutte le delegazioni in riunione. In casi urgenti il presidente è autorizzato a ricorrere alla procedura scritta. In entrambi i casi il presidente trasmette un progetto di decisione ai membri dell'autorità di controllo comune. Se le delegazioni non si oppongono al progetto di decisione, tradotto nelle rispettive lingue ufficiali, entro un termine stabilito dal presidente e non inferiore a 14 giorni dalla notifica, la proposta è considerata adottata. Qualora entro cinque giorni lavorativi dalla notifica del progetto di decisione, una delegazione chieda un dibattito orale in sede di autorità di controllo comune, la procedura scritta viene sospesa.

Articolo 7. Controlli in loco ed esperti

1. Nell'ambito delle competenze conferitele dall'articolo 24 della convenzione, l'autorità di controllo comune può eseguire controlli sulla protezione dei dati presso l'Europol.

2. L'autorità di controllo comune può nominare uno o più membri incaricati di eseguire questi controlli. Tali membri possono essere assistiti da esperti, nel modo ritenuto appropriato dall'autorità di controllo comune. Tali esperti sono selezionati unicamente da un elenco preventivamente stilato dall'autorità di controllo comune e da essa comunicato

all'Europol. Gli esperti figuranti in tale elenco devono provenire dalle autorità di controllo nazionali e da organismi delle amministrazioni pubbliche, tranne nel caso in cui siffatti esperti non siano disponibili. Tutti gli esperti devono soddisfare i requisiti di sicurezza in vigore secondo i rispettivi diritti nazionali.

3. Per motivi di urgenza, il presidente può procedere alla nomina di tali membri ed esperti direttamente. In questo caso ne informa senza indugio i membri dell'autorità di controllo comune.

4. I membri dell'autorità di controllo comune incaricati di effettuare un controllo riferiscono alla medesima in merito ai risultati della loro attività.

Articolo 8. Procedura in caso di violazioni

Qualora l'autorità di controllo comune constati violazioni di disposizioni della convenzione per quanto riguarda la memorizzazione, il trattamento o l'utilizzazione di dati di carattere personale, ne informa il direttore dell'Europol e gli chiede una risposta scritta entro un termine stabilito. L'autorità di controllo comune, se ritiene che la risposta non sia sufficiente o non sia stata trasmessa per tempo, ovvero se sorgono altre difficoltà, interpella per iscritto il consiglio di amministrazione (articolo 24, paragrafo 5, terza frase della convenzione). La mancata esecuzione di una decisione definitiva del comitato per i ricorsi è considerata una violazione della convenzione.

Articolo 9. Processo verbale

Di ogni riunione dell'autorità di controllo comune è redatto un processo verbale. Il progetto di verbale è preparato dal segretariato sotto la direzione del presidente e sottoposto all'autorità di controllo comune per l'adozione nella successiva riunione. Ciascun membro ha il diritto di far modificare il processo verbale affinché rispecchi le osservazioni da esso formulate nel corso della riunione.

Articolo 10. Relazione di attività

1. L'autorità di controllo comune redige una relazione di attività almeno ogni due anni. Almeno un mese prima che tale relazione sia trasmessa al Consiglio, il consiglio di amministrazione ha la possibilità di esprimere un parere, che viene allegato alla relazione (articolo 24, paragrafo 6 della convenzione).

2. L'autorità di controllo comune decide di pubblicare o meno la relazione di attività e, nel primo caso, decide in merito alle modalità della pubblicazione.

TITOLO III - REGOLAMENTO INTERNO DEL COMITATO PER I RICORSI

Articolo 11. Funzioni del comitato per i ricorsi

1. Il comitato per i ricorsi (in prosieguo denominato "il comitato") esamina i ricorsi previsti nell'articolo 19, paragrafi 6, 7 e 8, nell'articolo 20, paragrafo 4, e nell'articolo 22, paragrafo 3, della convenzione.

2. Il comitato adotta le decisioni definitive in merito alle questioni di cui al paragrafo 1.

3. Oltre alle competenze di cui all'articolo 2, paragrafo 2, il comitato è dotato dei poteri previsti dal presente capitolo.

Articolo 12. Composizione

1. Il comitato è composto da un membro di ciascuna delegazione dell'autorità di controllo comune. Ogni membro può avere un supplente. I membri del comitato e i loro supplenti sono nominati per un periodo di cinque anni dall'autorità di controllo comune, su designazione della delegazione interessata. Il loro mandato è rinnovabile.

2. I membri del comitato e i loro supplenti devono possedere le qualifiche necessarie per esaminare e deliberare in merito ai ricorso di cui all'articolo 1, paragrafo 1, che compren-

dono tra l'altro conoscenze specialistiche in campo giuridico ed esperienza in materia di risoluzione delle controversie e di protezione dei dati.

3. Qualora un membro del comitato non possa assistere ad una riunione, egli può farsi rappresentare dal suo supplente.

4. La qualifica di membro del comitato viene meno quando la persona interessata si dimette o cessa di essere membro dell'autorità di controllo comune. Tale disposizione si applica altresì ai supplenti.

Articolo 13. Indipendenza e imparzialità

1. Nello svolgimento delle loro mansioni i membri del comitato sono indipendenti e imparziali, non sono vincolati dalle istruzioni dell'autorità di controllo comune o di chiunque altro e sono soggetti soltanto alla legge. Per tutta la durata del loro mandato essi non possono svolgere attività incompatibili con i requisiti di indipendenza e imparzialità prescritti loro in quanto membri del comitato o con la disponibilità richiesta a tale fine. Le attività che sono o sono state svolte per conto dell'autorità nazionale di controllo non sono considerate incompatibili con l'attività svolta nel comitato. Le disposizioni del presente paragrafo si applicano altresì ai supplenti.

2. Qualora un membro del comitato o un supplente sia stato coinvolto nel caso in modo tale da dare adito a seri dubbi in ordine alla sua imparzialità, o in qualsiasi altra circostanza che possa recare pregiudizio alla corretta deliberazione su un ricorso, egli rende nota la sua posizione e si ritira dal caso.

3. Se una parte ricusa un membro o un supplente per i motivi di cui ai paragrafi 1 e 2, il comitato ascolta la persona interessata nonché le altre parti, quindi decide sulla questione in assenza della persona interessata e a scrutinio segreto.

4. Qualora una persona si dimetta o venga esclusa dal caso a norma del paragrafo 3, essa viene sostituita dal supplente.

Articolo 14. Presidenza

1. Il comitato elegge al suo interno un presidente e un vicepresidente a maggioranza di due terzi dei voti espressi, a scrutinio segreto, dai membri presenti. Qualora nessun candidato ottenga la maggioranza richiesta al primo turno di votazioni, ha luogo un secondo turno tra i due candidati che hanno ricevuto il maggior numero di voti. Il presidente o il vicepresidente dell'autorità di controllo comune non può essere eletto presidente o vicepresidente del comitato né essere membro della stessa delegazione. Il presidente e il vicepresidente vengono eletti per un periodo di due anni. Essi possono essere eletti per un secondo mandato di un anno.

2. Il presidente presiede le riunioni e vigila sul corretto andamento dei lavori. Convoca le riunioni del comitato, ne fissa il luogo, la data e l'ora e prepara l'ordine del giorno provvisorio.

3. In caso di assenza del presidente, il vicepresidente ne fa le veci. In assenza del vicepresidente, il membro più anziano in termini di età fa le veci del vicepresidente. La prima riunione del comitato è convocata e presieduta dal membro più anziano in termini di età fino all'elezione del presidente.

4. Il comitato può, al fine di preparare le sue deliberazioni, nominare tra i propri membri, su proposta del presidente, uno o più relatori. In tali casi, il membro designato quale relatore appartiene in linea di massima allo Stato membro da cui proviene il ricorrente oppure, se il ricorrente proviene da uno Stato terzo, allo Stato membro cui il caso è più strettamente connesso. In caso d'urgenza, il presidente può procedere a tale nomina direttamente. In tal caso egli ne informa senza indugio i membri del comitato. Il relatore esamina il ricorso e presenta al comitato una relazione sulla sua ammissibilità nonché una proposta relativa ad ulteriori procedimenti con particolare riguardo alle misure preparatorie necessarie.

Articolo 15. Rappresentanza

Il ricorrente può essere assistito o rappresentato da un avvocato o da un altro consulente. Il comitato può decidere di escludere dal procedimento un avvocato o un consulente in caso di comportamento gravemente scorretto. In caso di esclusione il presidente fissa un termine per consentire alla parte interessata di designare un altro avvocato o consulente; il procedimento è sospeso fino alla scadenza di tale termine. L'avvocato o il consulente esibisce, su richiesta del comitato, il mandato conferitogli dal ricorrente.

Articolo 16. Lingue

1. I lavori vengono svolti in una delle lingue ufficiali delle istituzioni dell'Unione europea. Il ricorrente sceglie la lingua ufficiale del procedimento. Questa è utilizzata nelle dichiarazioni orali e nei documenti scritti delle parti, nonché nei processi verbali e nelle decisioni del comitato.

2. I documenti redatti in una lingua diversa da quella del procedimento sono corredati di una traduzione in tale lingua. In caso di documenti molto lunghi, la traduzione può limitarsi a estratti o sunti. Il comitato può trasmettere in qualsiasi momento, in virtù delle sue competenze o su richiesta di una delle parti, una traduzione completa.

3. Se necessario, i servizi di interpretazione e traduzione vengono forniti, a titolo gratuito, a ogni membro del comitato e alle parti. Le decisioni del comitato sono tradotte in tutte le lingue ufficiali delle istituzioni dell'Unione europea.

4. Qualora il ricorrente non conosca nessuna delle lingue ufficiali delle istituzioni dell'Unione europea, la denuncia può essere presentata in un'altra lingua. Il ricorrente è tenuto a presentare un sunto in una delle lingue ufficiali. Il presidente o il relatore fa tradurre la denuncia nella lingua scelta.

Articolo 17. Istruzione della procedura

1. Il ricorso viene introdotto mediante denuncia scritta depositata presso il segretariato dell'autorità di controllo comune entro tre mesi dalla data di ricezione della decisione dell'Europol da parte del ricorrente. In mancanza di una decisione, il ricorso è introdotto entro tre mesi dalla data di scadenza dei termini di cui all'articolo 19, paragrafo 6, all'articolo 20, paragrafo 4, e all'articolo 22, paragrafo 3, della convenzione. Qualsiasi dubbio in merito all'osservanza dei termini è risolto a favore del ricorrente.

2. Il ricorrente espone i motivi del ricorso. Nella denuncia devono risultare chiari l'identità del ricorrente, l'oggetto del ricorso e le motivazioni. La denuncia è corredata dell'eventuale documentazione giustificativa disponibile. Il ricorrente può ritirare la denuncia in qualsiasi momento.

3. Il segretariato notifica l'avvenuto ricevimento della denuncia entro quattro settimane e fornisce informazioni generali sullo svolgimento futuro del procedimento.

4. Se la denuncia non soddisfa i requisiti di cui al paragrafo 2, prima e seconda frase, e all'articolo 16, paragrafo 4, seconda frase, il segretariato invita il ricorrente a rettificare eventuali omissioni entro quattro settimane.

5. Il comitato respinge, su proposta del presidente o del relatore, i ricorsi che non soddisfino i requisiti previsti. Un ricorso presentato oltre i termini di cui al paragrafo 1 può essere accolto qualora il ritardo sia dovuto a circostanze particolari.

Articolo 18. Esame preliminare

1. Se la denuncia soddisfa i requisiti stabiliti, essa viene esaminata dal comitato in base alle disposizioni seguenti, che tengono conto della convenzione, in particolare degli articoli 19, 20 e 22.

2. Copia della denuncia viene trasmessa all'Europol affinché comunichi le proprie osservazioni, che vengono presentate entro quattro settimane, prorogabili di altre due settimane.

3. Il comitato può decidere, in singoli casi, di coinvolgere nella procedura di ricorso anche una o più unità nazionali. Il ricorrente e l'Europol sono informati della decisione. Copia delle osservazioni dell'Europol e del ricorrente è in tal caso trasmessa alle pertinenti unità nazionali affinché, entro quattro settimane, prorogabili di altre due settimane, possano presentare le proprie osservazioni.

4. Una volta ricevute le osservazioni o scaduti i termini, il comitato dispone di tre mesi di tempo per esaminare la denuncia.

Articolo 19. Informazioni supplementari

1. Il comitato può chiedere al ricorrente, all'Europol, alle unità nazionali, alle autorità di controllo nazionali o ad altri organi di fornirgli informazioni, elementi di prova o osservazioni. Le parti hanno il diritto di presentare al comitato suggerimenti riguardo all'assunzione delle prove o di chiedere l'ammissione degli elementi di prova. Il comitato esamina attentamente tali suggerimenti e richieste di ammissione nella misura necessaria all'esame del caso.

2. Il comitato può anche decidere di effettuare ispezioni in loco presso l'Europol. Si applica parimenti l'articolo 7. In tal caso il ricorrente o il suo consulente sono informati dell'esito delle ispezioni.

Articolo 20. Accesso agli atti del procedimento

1. Tutte le parti hanno, se lo desiderano, accesso agli atti del procedimento e possono chiedere al segretariato dell'autorità di controllo comune di fornire loro, a proprie spese, estratti o fotocopie. L'accesso è negato qualora ciò sia necessario:

- per il corretto svolgimento delle funzioni dell'Europol;
- per la tutela della sicurezza e dell'ordine pubblico negli Stati membri o per la prevenzione della criminalità;
- per la protezione dei diritti e delle libertà di terzi, tutti casi nei quali non possono essere invocati gli interessi della persona in questione.

2. L'Europol, le unità nazionali e le autorità di controllo nazionali possono indicare in quale misura le informazioni da essi fornite non debbano essere messe a disposizione del ricorrente, specificando le ragioni di tale limitazione. Il comitato può chiedere ulteriori motivazioni. Se il comitato ritiene accettabili tali motivazioni, le informazioni in questione non vengono trasmesse. Il comitato può decidere diversamente, all'unanimità, solo in assenza di motivi accettabili. In tal caso il comitato può decidere di richiedere un sunto da mettere a disposizione del ricorrente o chiedere che talune informazioni vengano fornite a quest'ultimo.

Articolo 21. Audizioni

1. Le parti, qualora ne facciano richiesta, sono sentite dal comitato. Il comitato informa debitamente le parti del loro diritto di essere sentite. Tale diritto si esercita per iscritto. Il comitato decide di ricorrere a una audizione orale su richiesta di una delle parti del procedimento, nella misura ritenuta necessaria per l'esame del caso. Il comitato informa debitamente le parti del loro diritto di essere sentite. Tutte le parti vengono informate a tempo debito dell'audizione orale e hanno il diritto di presenziarvi.

2. L'audizione è pubblica a meno che il comitato decida, d'ufficio o su richiesta di una delle parti, di escludere totalmente o parzialmente il pubblico qualora lo rendano necessario motivi di pubblica sicurezza, in particolare i motivi di cui all'articolo 19, paragrafo 3, della convenzione, o la tutela della vita privata di una persona, oppure nella misura strettamente necessaria, a giudizio del comitato, in particolari circostanze in cui la pubblicità potrebbe recare pregiudizio alla corretta decisione del ricorso. Qualora uno Stato membro coinvolto nella procedura oppure l'Europol richiedano di non ammettere il pubblico, il comitato può decidere diversamente, all'unanimità, solo in assenza dei motivi menzionati alla frase 1.

3. Il comitato può decidere, su richiesta di una parte o di propria iniziativa, di sentire una parte senza la presenza di terzi, qualora sia necessario per assicurare il corretto funzionamento dell'Europol, per tutelare la sicurezza di uno Stato membro o per proteggere gli

interessi del ricorrente o di un terzo. Le parti assenti vengono informate dei lavori svolti in loro assenza.

Articolo 22. Audizione di testimoni ed esperti

1. Il comitato può decidere, su richiesta di una parte o di propria iniziativa, di sentire testimoni. Tutte le parti e i testimoni interessati vengono informati a tempo debito dell'audizione. Si applica altresì l'articolo 21, paragrafi 2 e 3.

2. I testimoni convocati dal comitato hanno diritto al rimborso delle spese di viaggio e di alloggio e ad una compensazione per il mancato guadagno nella misura ritenuta equa dal comitato. Essi possono ricevere i necessari anticipi. Tutti i pagamenti sono a carico del bilancio dell'autorità di controllo comune.

3. I testimoni sono sentiti dal comitato. I membri del comitato possono interrogare i testimoni. Con l'autorizzazione del presidente, le parti possono interrogare i testimoni. Prima dell'inizio dell'udienza, il presidente rammenta ai testimoni che sono tenuti a dire la verità.

4. Il comitato può nominare esperti e definire i loro compiti. Gli esperti hanno diritto ad un compenso per il lavoro svolto. Il comitato può decidere di sentire gli esperti. Si applicano inoltre le regole relative all'audizione dei testimoni.

Articolo 23. Dichiarazioni conclusive

Prima di prendere una decisione definitiva, il comitato invita tutte le parti a fare dichiarazioni conclusive.

Articolo 24. Processo verbale

1. Il comitato redige un processo verbale dei procedimenti che rispecchia l'andamento di ogni audizione e le dichiarazioni rilasciate nel corso della stessa. Le parti possono richiedere che taluni documenti o talune dichiarazioni vengano inclusi, integralmente o in parte, nel processo verbale. Il processo verbale viene firmato dal presidente, trasmesso alle parti e allegato agli atti del procedimento. Nei casi di cui all'articolo 21, paragrafo 2, o all'articolo 2, o all'articolo 22, paragrafo 1, il comitato impone alcune limitazioni.

2. L'articolo 9 si applica altresì a tutte le riunioni del comitato alle quali le parti non partecipano.

Articolo 25. Decisioni e riservatezza

1. Le riunioni del comitato sono valide solo se vi partecipano i quattro quinti dei membri o dei loro supplenti.

2. Le decisioni vengono adottate a maggioranza semplice dei membri o supplenti presenti alla riunione, salvo che il presente regolamento o la convenzione dispongano diversamente. In caso di parità, prevale il voto del presidente. Tutti coloro che prendono parte alla decisione definitiva devono aver partecipato ad una audizione.

3. Le deliberazioni del comitato rimangono riservate.

4. Nella decisione definitiva del comitato figurano i nomi delle parti e dei loro rappresentanti, i nomi dei membri del comitato che hanno partecipato alla decisione, la data nella quale la decisione è pronunciata, la parte dispositiva della decisione, una breve esposizione dei fatti del caso e le motivazioni. La decisione viene pronunciata in una sessione pubblica e notificata alle parti. Copia della decisione è trasmessa all'autorità di controllo comune.

Articolo 26. Notificazioni

Le notificazioni e le altre comunicazioni alle parti, ai testimoni e agli esperti vengono trasmesse con mezzi tali da garantire che i destinatari vengano debitamente informati e che, se necessario, ciò possa essere verificato.

Articolo 27. Spese

1. Il comitato decide in merito alle spese del procedimento nella sua decisione definitiva. Il procedimento dinanzi al comitato è gratuito. In caso di proposizione del ricorso, le spese necessarie sostenute dal ricorrente per la presentazione e il procedimento sono imputate, interamente o in parte, all'Europol, nella misura ritenuta equa dal comitato.

2. Al ricorrente che non sia in grado di sostenere in tutto o in parte le spese del procedimento può essere concesso in qualsiasi momento, su richiesta, un contributo per coprire tali spese. All'atto della presentazione della domanda egli acclude alla stessa i documenti attestanti il suo stato di necessità. Il comitato può revocare in qualsiasi momento il contributo, qualora i requisiti in base ai quali esso è stato concesso mutino nel corso del procedimento. In caso di approvazione del contributo, le spese sono imputate al bilancio dell'autorità di controllo comune. Se ciò è giustificato, la decisione definitiva può prescrivere ad una parte di restituire al bilancio dell'autorità di controllo comune gli anticipi concessi. Nel presentare la domanda il ricorrente dichiara di acconsentire al pagamento delle spese, ove prescritto dalla decisione definitiva.

Articolo 28. Regolarità delle procedure

Nei casi non contemplati dal presente regolamento interno, il comitato provvede a che lo svolgimento del procedimento sia conforme ai principi generali del diritto comunitario di cui all'articolo F, paragrafo 2, del trattato sull'Unione europea.

TITOLO III - DISPOSIZIONI FINALI

Articolo 29. Segretariato

1. Nello svolgimento delle sue mansioni l'autorità di controllo comune è assistita da un segretariato situato presso la sua sede. Il segretariato è un organo permanente, i cui membri sono assunti unicamente in base alla competenza. I membri agiscono esclusivamente nel vero interesse dell'autorità di controllo comune, sono totalmente indipendenti dall'Europol e non accettano istruzioni da nessun'altra autorità. Le assunzioni o i distacchi del personale del segretariato avvengono su proposta dell'autorità di controllo comune. I membri del personale del segretariato non svolgono altre attività lavorative senza l'autorizzazione del presidente dell'autorità di controllo comune.

2. Il segretariato è posto sotto la direzione del presidente dell'autorità di controllo comune in base alle norme stabilite da detta autorità. Il segretariato fornisce inoltre servizi al comitato per i ricorsi. Nell'esercizio di tali funzioni esso è posto sotto la direzione del presidente di detto comitato. Il segretariato tiene un registro dei ricorsi e di ogni altro documento.

3. Il segretariato assicura inoltre che gli obblighi di cui all'articolo 32 della convenzione siano rispettati nei lavori dell'autorità di controllo comune.

Articolo 30. Riservatezza

1. I membri dell'autorità di controllo comune, i supplenti, gli esperti e i membri del segretariato sono tenuti a trattare in maniera riservata le informazioni di cui siano venuti a conoscenza nell'ambito della loro attività, a meno che il corretto svolgimento delle loro mansioni richieda altrimenti. Tale obbligo sussiste anche dopo la cessazione dall'incarico.

2. All'atto della loro nomina, i membri dell'autorità di controllo comune, i supplenti, gli esperti e i membri del segretariato dichiarano di accettare detti obblighi.

3. Nel caso di violazioni dell'obbligo di riservatezza, un membro dell'autorità di controllo comune o il suo supplente può essere sospeso a maggioranza dei due terzi delle votazioni espresse a scrutinio segreto dalle delegazioni che partecipano a una riunione dell'autorità di controllo comune. L'interessato è ascoltato prima che sia presa la decisione, ma non partecipa alla stessa. La presente disposizione si applica allo stesso modo al comitato per i ricorsi, qualora la violazione dell'obbligo di riservatezza interessi i lavori di quel comitato.

In tal caso l'autorità di controllo comune è informata senza indugio.

Se un membro viene sospeso, esso è sostituito dal suo supplente. La decisione di sospensione è comunicata all'autorità di controllo nazionale che ha nominato il membro sospeso.

Articolo 31. Bilancio e spese

1. Il segretariato prepara il progetto di bilancio annuale da sottoporre all'autorità di controllo comune; una volta approvato, il progetto viene trasmesso al consiglio di amministrazione prima delle consultazioni previste dall'articolo 24, paragrafo 9, della convenzione.

2. L'autorità di controllo comune decide circa l'erogazione dei fondi di bilancio ad essa destinati, che vengono amministrati dal segretariato.

3. Le spese dell'autorità di controllo comune e del comitato per i ricorsi, comprese le spese per i membri di detto comitato ed i loro supplenti, necessarie al corretto esercizio delle loro funzioni, sono a carico del bilancio dell'autorità di controllo comune in base alle norme da essa stabilite.

Articolo 32. Modifica del regolamento interno

Le modifiche del presente regolamento interno vengono adottate all'unanimità dall'autorità di controllo comune e sottoposte all'approvazione unanime del Consiglio (articolo 24, paragrafo 7, prima frase, della convenzione).

Articolo 33. Valutazione

Il presente regolamento interno è sottoposto ad una valutazione da parte dell'autorità di controllo comune entro tre anni dopo la sua entrata in vigore.

Articolo 34. Entrata in vigore del regolamento interno

Il presente regolamento interno entra in vigore il giorno successivo a quello dell'approvazione da parte del Consiglio, a norma dell'articolo 24, paragrafo 7, della convenzione.

Fatto a Bruxelles, addì 22 aprile 1999

Per l'Autorità di controllo comune
Il Presidente
Fergus GLAVEY

DICHIARAZIONE DEL CONSIGLIO
sull'articolo 4, paragrafo 5, e sull'articolo 12, paragrafo 4,
adottata all'atto dell'approvazione del regolamento interno
dell'Autorità di controllo comune dell'Europol

Gli Stati membri concordano sul fatto che la cessazione della carica di membro o di supplente dell'autorità di controllo comune prima del termine previsto non possa verificarsi in particolare per motivi riguardanti lo svolgimento della funzione nell'ambito del comitato per i ricorsi.

D. Decisione del Consiglio del 17 ottobre che istituisce un segretariato

Decisione del Consiglio del 17 ottobre 2000 che istituisce un segretariato delle autorità di controllo comuni preposte alla protezione dei dati istituite dalla convenzione che istituisce un ufficio europeo di polizia (convenzione Europol), dalla convenzione sull'uso dell'informatica nel settore doganale e dalla convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni (convenzione di Schengen)

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto l'articolo 30 e l'articolo 34, paragrafo 2, lettera c) del trattato sull'Unione europea,

visto l'articolo 2 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea,

vista l'iniziativa della Repubblica portoghese,

tenuto conto del parere del Parlamento europeo,

considerando quanto segue:

(1) La convenzione che istituisce un ufficio europeo di polizia (convenzione Europol), la convenzione sull'uso dell'informatica nel settore doganale e la convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni (convenzione di Schengen) hanno istituito autorità di controllo comuni al fine di vigilare sulla corretta applicazione delle disposizioni relative alla protezione dei dati contenute in detti strumenti.

(2) Per funzionare efficacemente limitando i costi, le autorità di controllo comuni dovrebbero essere coadiuvate da un unico segretariato indipendente "Protezione dati" che, nell'esercizio delle sue funzioni, è tenuto a seguire unicamente le istruzioni di tali autorità.

(3) Per motivi pratici la gestione amministrativa del segretariato "Protezione dati" dovrebbe essere strettamente collegata al Segretariato generale del Consiglio, pur salvaguardando la propria indipendenza nell'esercizio delle sue funzioni.

(4) Allo scopo di garantire tale indipendenza, le decisioni relative alla nomina e alla sospensione dall'incarico del capo del segretariato "Protezione dati" dovrebbero essere adottate dal Segretario generale aggiunto del Consiglio, in base a una proposta delle autorità di controllo comuni, e gli altri funzionari assegnati al segretariato "Protezione dati" dovrebbero seguire esclusivamente le istruzioni del capo del segretariato "Protezione dati".

(5) Le spese amministrative del segretariato "Protezione dati" dovrebbero essere a carico del bilancio generale dell'Unione europea. L'Europol dovrebbe contribuire al finanziamento di talune spese connesse a riunioni riguardanti questioni relative all'attuazione della convenzione Europol.

(6) Poiché la decisione 1999/438/CE del Consiglio, del 20 maggio 1999, concernente l'autorità di controllo comune istituita dall'articolo 115 della convenzione di applicazione dell'accordo di Schengen, del 14 giugno 1985, relativo all'eliminazione graduale dei controlli alle frontiere comuni, firmata il 19 giugno 1990, è superata dalla presente decisione, essa andrebbe pertanto abrogata e sostituita a decorrere dalla data di applicazione della presente decisione.

(7) Le autorità di controllo comuni esistenti hanno dichiarato di approvare i principi enunciati nella presente decisione,

DECIDE:

Articolo 1. Istituzione e compiti del segretariato "Protezione dati"

1. È istituito un segretariato (in seguito denominato: segretariato "Protezione dati") delle autorità di controllo comuni istituite dalla convenzione che istituisce un ufficio europeo di polizia (convenzione Europol), dalla convenzione sull'uso dell'informatica nel settore doganale e dalla convenzione di applicazione dell'accordo di Schengen relativo all'eliminazione graduale dei controlli alle frontiere comuni (convenzione di Schengen).

2. Il segretariato "Protezione dati" assolve i compiti previsti per i segretariati delle autorità di controllo comuni quali stabiliti nei regolamenti interni di tali autorità.

Articolo 2. Segretario "Protezione dati"

1. Il segretariato "Protezione dati" è posto sotto la direzione di un segretario "Protezione dati" a cui viene garantita l'indipendenza nello svolgimento delle sue funzioni, e che è tenuto a seguire esclusivamente le istruzioni delle autorità di controllo comuni e dei loro presidenti. Il Segretario generale aggiunto del Consiglio nomina per un periodo di tre anni, in base a una proposta delle autorità di controllo comuni, il segretario "Protezione dati". Il suo mandato è rinnovabile.

2. Il segretario "Protezione dati" è scelto tra persone che siano cittadini dell'Unione europea, in pieno possesso dei diritti civili e politici, che abbiano l'esperienza e la capacità necessarie per svolgere le funzioni in questione e che offrano piena garanzia di indipendenza. Egli si astiene da qualsiasi azione incompatibile con le sue funzioni e, durante il periodo del suo mandato, non svolge un'altra attività professionale retribuita o non retribuita. Dopo la cessazione delle sue funzioni, egli rispetta i doveri di onestà e riserbo per quanto riguarda l'accettazione di funzioni e vantaggi.

3. Il segretario "Protezione dati" è sospeso dall'incarico dal Segretario generale aggiunto del Consiglio, in base a una proposta delle autorità di controllo comuni, qualora egli non soddisfi più le condizioni necessarie per l'esercizio delle sue funzioni o abbia commesso una colpa grave.

4. Oltre che per la normale procedura di sostituzione alla scadenza del suo mandato, per decesso o per sospensione dall'incarico a norma del paragrafo 3, le funzioni del segretario "Protezione dati" cessano allorché le sue dimissioni prendono effetto. In caso di cessazione del mandato e di dimissioni, egli mantiene le proprie funzioni, a richiesta delle autorità di controllo comuni, finché non viene sostituito.

5. Sia durante che dopo la cessazione del suo mandato, il segretario "Protezione dati" è tenuto al segreto professionale in merito a informazioni riservate di cui è venuto a conoscenza nell'assolvere le sue funzioni.

6. Durante il periodo del suo mandato, il segretario "Protezione dati" è soggetto, salvo disposizione contraria della presente decisione, alle norme che si applicano alle persone aventi lo status di agente temporaneo ai sensi dell'articolo 2, lettera a) del regime applicabile agli altri agenti delle Comunità europee, compresi gli articoli da 12 a 15 e 18 del protocollo sui privilegi e sulle immunità delle Comunità europee. Il segretario "Protezione dati" è inquadrato nella categoria A e il grado e lo scatto ai quali egli è impiegato sono determinati in base ai criteri applicabili ai funzionari e altri agenti delle Comunità. Se la persona nominata è già un funzionario delle Comunità, essa è comandata per il periodo del suo mandato nell'interesse del servizio ai sensi dell'articolo 37, lettera a), primo trattino dello statuto dei funzionari delle Comunità europee (statuto)(8). La prima frase dell'ultimo paragrafo dell'articolo 37 dello statuto si applica fatto salvo il paragrafo 1 del presente articolo.

Articolo 3. Personale

1. Il segretariato "Protezione dati" è dotato del personale necessario all'espletamento dei suoi compiti. I membri del personale assegnati al segretariato "Protezione dati" occupano posti inclusi nell'elenco dei posti aggiunti alla sezione del bilancio generale dell'Unione europea relativa al Consiglio.

2. Nell'esercizio delle loro funzioni, i membri del personale di cui al paragrafo 1 sono soggetti esclusivamente alle istruzioni del segretario "Protezione dati" e delle autorità di controllo comuni o dei loro presidenti. In tale contesto, essi non possono chiedere né accettare istruzioni da alcun governo, autorità, organizzazione o persona, ma solo dal segretario "Protezione dati" e dalle autorità di controllo comuni o dai loro presidenti.

3. Fatto salvo il paragrafo 2, il personale assegnato al segretariato "Protezione dati" è soggetto ai regolamenti e alle regolamentazioni applicabili ai funzionari e agli altri agenti delle Comunità europee. Per quanto riguarda l'esercizio dei poteri conferiti all'autorità che ha il potere di nomina dallo statuto dei funzionari delle Comunità europee e dal regime applicabile agli altri agenti delle Comunità europee, il personale è soggetto alle stesse norme applicabili ai funzionari e agli altri agenti delle Comunità europee.

Articolo 4. Supporto amministrativo

1. Il Segretariato generale del Consiglio fornisce gli uffici e il materiale necessari all'espletamento dei compiti del segretariato "Protezione dati", nonché le strutture e i servizi necessari allo svolgimento delle riunioni delle autorità di controllo comuni nei locali del Consiglio, incluso un servizio di interpretazione.

2. Per quanto concerne le riunioni che si terranno nei locali del Consiglio le presidenze delle autorità di controllo comuni ne stabiliscono il calendario, previo accordo della presidenza del Consiglio.

Articolo 5. Finanziamento

1. Le spese amministrative generali del segretariato "Protezione dati" (in particolare, spese di materiale, retribuzioni, indennità e altre spese riguardanti il personale) sono imputate alla sezione del bilancio generale dell'Unione europea relativa al Consiglio.

2. I costi direttamente connessi con le riunioni sono a carico:

- del Consiglio, nel caso di riunioni nei locali del Consiglio riguardanti questioni relative all'attuazione delle disposizioni della convenzione di Schengen, spese di viaggio connesse con missioni di controllo presso il C.SIS o riunioni riguardanti questioni relative all'attuazione della convenzione sull'uso dell'informatica nel settore doganale,
- dell'Europol, nel caso di riunioni riguardanti questioni relative all'attuazione della convenzione Europol.

Articolo 6, Disposizioni finali

1. La presente decisione entra in vigore il giorno successivo all'adozione da parte del Consiglio. Essa si applica dal 1° settembre 2001.

2. A decorrere dalla data di entrata in vigore della presente decisione, possono essere adottate le decisioni e gli atti necessari alla sua attuazione. Essi non producono effetti prima della data di applicazione della presente decisione.

3. Alla data di applicazione della presente decisione risulta abrogata la decisione 1999/438/CE, che continua tuttavia ad applicarsi alle spese derivanti da eventi antecedenti alla suddetta data.

Fatto a Lussemburgo, addì 17 ottobre 2000

Per il Consiglio Il Presidente
É. Guigou

E. Decisione del Comitato per i ricorsi

Ricorso del sig. X avverso la decisione dell'Europol, del 22 gennaio 2001, sul diritto di accesso (articolo 19 convenzione Europol).

Il comitato per i ricorsi,
Composto dai signori *L. Jørgensen, R. Bachmeier, F. Aldhouse, G. Busia, M. Varges Gomes, P. Hustinx, M. Kleemola, D. Kambouraki, L. Aguilera Ruiz, P. Thomas, A. Türk, U. Widebäck e G. Wivenes.*

Relatore: sig. F. Aldhouse
Segretario: sig. P. Michael

Parti:
1. Sig. X (ricorrente)
2. Europol, rappresentato dal sig. D. Heimans e dal sig. H. Felgenhauer

3. National Criminal Intelligence Service, ministero degli Affari interni del Regno Unito, rappresentato dal sig. R. Gaspar,

SVOLGIMENTO DEL PROCEDIMENTO

L'8 gennaio 2001, il sig. X presentava all'Europol richiesta di accesso a dati personali che lo riguardavano. La richiesta veniva trasmessa al Commissario per la protezione dei dati del Regno Unito.

In data 10 gennaio 2001, il commissario per la protezione dei dati provvedeva a sua volta ad inoltrare l'istanza all'Europol.

Il 22 gennaio 2001 l'Europol trasmetteva al ricorrente la propria decisione in merito alla sua richiesta.

Il 19 febbraio 2001 il sig. X proponeva ricorso avverso tale decisione dinanzi al comitato per i ricorsi.

Il 18 aprile 2001, il comitato per i ricorsi dichiarava il ricorso ammissibile.

Alla riunione del 26 giugno 2001 il comitato per i ricorsi prendeva in esame una relazione investigativa redatta

dal sig. J. Bamford datata 21 giugno 2001 nonché la relazione del relatore datata 26 giugno 2001, compilata parzialmente sulla base della prima relazione.

Il 26 giugno 2001 il comitato per i ricorsi invitava il National Criminal Intelligence Service (NCIS, servizio nazionale di informazione nel settore della criminalità) ad intervenire nel procedimento di ricorso.

Il comitato per i ricorsi prendeva in esame i documenti in fascicolo e le raccomandazioni del relatore nel corso delle riunioni del 18 aprile, 26 giugno, 11 ottobre e 13 dicembre 2001.

Il comitato per i ricorsi, il 13 dicembre 2001, respingeva la richiesta del ricorrente di un'udienza verbale presentata e, alla luce delle speciali circostanze del caso, riteneva opportuno che all'Europol venisse data l'opportunità di riconsiderare la propria decisione e di rinviare la prosecuzione del caso.

In una lettera al presidente del comitato per i ricorsi, in data 1o febbraio 2002, l'Europol chiariva che l'Ufficio medesimo aveva riesaminato la decisione del 22 gennaio 2001. L'Europol dichiarava inoltre che i loro sforzi erano stati vani stante la mancanza di collaborazione del ricorrente.

Il 4 febbraio 2002, il comitato per i ricorsi invitava tutte le parti a presentare le rispettive dichiarazioni conclusive.

Nel corso della riunione del 6 marzo 2002 il comitato per i ricorsi esaminava una seconda relazione del relatore, datata 7 febbraio 2002.

SVOLGIMENTO DEI FATTI

1. In data 8 gennaio 2001, il sig. X, inviava una lettera all'autorità competente del Regno Unito chiedendo di accertare se fossero detenuti negli archivi dell'Europol dati relativi alla sua persona e, in tal caso, di verificarli.

2. Con fax in data 10 gennaio 2001 l'autorità nazionale competente inoltrava tale lettera all'Europol.

3. Previa consultazione con le autorità del Regno Unito, l'Europol rispondeva al sig. X con lettera datata 22 gennaio 2001 in cui dichiarava, tra l'altro che: —In conformità con la procedura stabilita dalla Convenzione Europol e della legislazione del Regno Unito, desidero comunicarLe che, facendo seguito alla sua richiesta, sono state compiute delle verifiche negli archivi dell'Europol. Ai sensi dell'articolo 19 della Convenzione Europol e della legislazione del Regno Unito, desidero comunicarLe che nei Suoi riguardi non sono trattati dati ai quali la persona abbia il diritto di accedere ai sensi dell'articolo 19 della Convenzione Europol".

4. La relazione investigativa del sig. Bamford del 21 giugno 2001 riportava che le verifiche svolte dall'Europol fornivano una rappresentazione veritiera della situazione.

5. Gli sforzi fatti dall'Europol per discutere con il ricorrente la decisione del 22 gennaio 2001 fallivano in quanto il ricorrente non era d'accordo rispetto all'incontro proposto dall'Europol.

LEGISLAZIONE E PRASSI PERTINENTI

La convezione per la protezione delle persone in relazione al trattamento automatico dei dati di carattere personale (convenzione del 28 gennaio 1981 del Consiglio d'Europa) dispone che:

Articolo 8

"Ogni persona deve poter:

a) ...

b) ottenere ad intervalli di tempo ragionevoli e senza ritardo o spese eccessive la conferma dell'esistenza o meno nel casellario

automatizzato dei dati di carattere personale ad essa relativi, come pure la trasmissione di tali dati in forma intellegibile.

Articolo 9, paragrafo 2

È possibile derogare alle disposizioni degli articoli ... e 8 della presente convenzione qualora una tale deroga, prevista dal diritto della Parte, costituisca una misura necessaria in una società democratica:

... alla protezione della sicurezza dello Stato, alla sicurezza pubblica ... o alla repressione dei reati.

Raccomandazione R(87)15 d'Europa del 17 settembre 1987 del Comitato dei ministri del Consiglio.

Principio 6.2

La persona interessata dovrà poter ottenere l'accesso ad un archivio di polizia ad intervalli ragionevoli e senza ritardi eccessivi, in conformità con quanto previsto dal diritto interno.

Principio 6.4

L'esercizio del diritto di accesso, di rettifica o di cancellazione non sarà oggetto di una restrizione, se non nei limiti in cui tale restrizione sia indispensabile per lo svolgimento di un compito legale della polizia ...

La convezione Europol (convenzione del 26 luglio 1995, GUCE 316, del 27 novembre 1995) dispone che:

Articolo 14, paragrafo 1

Per quanto riguarda il trattamento di dati di carattere personale in archivi e nel quadro dell'applicazione della presente convenzione ciascuno Stato membro adotta, al più tardi al momento dell'entrata in vigore di detta convenzione, le disposizioni di diritto interno necessarie per assicurare un livello di protezione dei dati almeno pari a quello derivante dall'applicazione dei principi della convenzione del Consiglio d'Europa del 28 gennaio 1981, tenendo conto della raccomandazione R(87)15 del 17 settembre 1987 del

Comitato dei ministri del Consiglio d'Europa relativa all'uso dei dati di carattere personale da parte delle autorità di polizia.

Articolo 14, paragrafo 3

Nel rilevamento, trattamento e uso dei dati di carattere personale l'Europol si attiene ai principi della . convenzione del Consiglio d'Europa del 28 gennaio 1981 e della raccomandazione R(87)15 del 17 settembre 1987 del Comitato dei ministri del Consiglio d'Europa.

Articolo 19

Diritto di accesso

1. Chiunque desideri esercitare il suo diritto di accedere ai dati memorizzati presso l'Europol che lo riguardano o di fare verificare tali dati, può a tale scopo presentare a titolo gratuito una domanda, in uno Stato membro di sua scelta, all'autorità nazionale competente che la sottopone quindi senza indugio all'Europol e avvisa il richiedente che quest'ultimo gli risponderà direttamente.

2. ...

3. Il diritto della persona interessata di accedere ai dati che la riguardano o di farli verificare si esercita nel rispetto della legislazione dello Stato membro presso il quale essa l'ha fatto valere, tenendo conto delle disposizioni seguenti:

Qualora la legislazione dello Stato membro interpellato preveda la comunicazione relativa ai dati, quest'ultima è rifiutata se ciò è necessario:

1) per il corretto svolgimento delle funzioni dell'Europol,
2) per la protezione della sicurezza degli Stati membri e dell'ordine pubblico o per la lotta contro i crimini;
3) per la protezione dei diritti e delle libertà di terzi, e pertanto le esigenze delle persone interessate alla comunicazione devono passare in secondo piano.

4. ....

5. Il diritto alla verifica si esercita secondo le procedure seguenti:

Qualora la legislazione nazionale applicabile non preveda la comunicazione relativa ai dati o si tratti di una semplice domanda di verifica, l'Europol, in stretto coordinamento con le autorità nazionali interessate, procede alle verifiche e notifica al richiedente che le verifiche sono state effettuate, senza fornire indicazioni che possano rivelargli se abbia o meno informazioni sul suo conto.

La legge del Regno Unito sulla protezione dei dati, del 16 luglio 1998, contiene le seguenti disposizioni:

Parte II, Diritti dei soggetti titolari dei dati e di terzi

Sezione 7, paragrafo 1 - ..... chiunque ha diritto-

a) di essere informato dal responsabile del trattamento dei dati se i dati di carattere personale che lo riguardano sono oggetto di trattamento da parte o per conto del responsabile del trattamento dei dati; b) in tal caso, di ricevere dal responsabile del trattamento dei dati una descrizione i) dei dati di carattere personale cui egli ha diritto. c) di ricevere la comunicazione in formato intelligibile-i) le informazioni che rappresentano i dati di carattere personale che lo riguardano, ...

Parte III, Esenzioni
Sezione 29, paragrafo 1- I dati di carattere personale trattati per una qualsiasi delle seguenti finalità
a) la prevenzione o l'investigazione di reati,
b) la cattura o il perseguimento giudiziario dei rei,
c) ...

sono esenti da ... e comunque dalla sezione 7, nella misura in cui l'applicazione ai dati di tali disposizioni potrebbe pregiudicare una qualsiasi delle materie menzionate nella presente sottosezione.

Parte V, Applicazione

Sezione 42, paragrafo 1

La persona che sia, o ritenga di essere, direttamente interessata dal trattamento di dati di carattere personale può avanzare una richiesta al garante, in proprio o per interposta persona, per valutare la probabilità o l'improbabilità che il trattamento sia avvenuto o avvenga in conformità con quanto disposto dalla presente Legge.

4) Qualora il garante abbia ricevuto una richiesta ai sensi della presente sezione egli notificherà alla persona che l'ha avanzata:

a) se ha proceduto ad una valutazione a seguito della richiesta e

b) nella misura in cui lo ritenga appropriato, tenuto conto in particolare di ogni eventuale esenzione di cui alla sezione 7 che si applichi in relazione ai dati di carattere personale di cui trattasi, le osservazioni formulate o le azioni intraprese a seguito della richiesta.

ARGOMENTAZIONI INNANZI IL COMITATO PER I RICORSI

Sig. X

Il ricorrente, ha ripetutamente affermato di essere oggetto di fastidi e discriminazioni da parte di vari individui quando si reca in Belgio e nei Paesi Bassi. Soltanto la polizia potrebbe aver orchestrato questi episodi e, se così fosse, sulla base di informazioni costruite e rilevate dall'Europol provenienti dal Regno Unito. La risposta fornita dall'Europol (la decisione del 22 gennaio 2001) alla sua richiesta (dell'8 gennaio 2001) nulla dice sul fatto che egli sia o meno noto all'Europol.

SNIC ed Europol

È desiderio della criminalità organizzata scoprire se le autorità sono al corrente delle loro attività, per cui essa investe risorse in vario modo per dare una risposta a questa domanda. Rivelare che nulla si sa sul conto di un individuo coinvolto nella criminalità organizzata è almeno importante quanto sapere che le organizzazioni preposte all'applicazione della legge sanno qualcosa. Se qualcuno che non ha collegamenti con la criminalità organizzata chiede di accedere a dati laddove non ci sono dati oggetto di trattamento, dicendo a tale persona che non ci sono dati che lo riguardano, si va a creare un precedente. Per precedente si intende il fatto che tale risposta dovrebbe essere fornita in tutte le circostanze simili in cui non si hanno dati a disposizione. Questo farebbe sì che un criminale inserito in un'organizzazione saprebbe che non ci sono dati che lo riguardano e con ciò ne trarrebbe un vantaggio. Fornire un vantaggio alla criminalità organizzata è contrario alle finalità dell'Europol e conseguentemente il precedente deve essere evitato. L'unico modo per evitarlo è dare una risposta alla richiesta di accesso come quella che è stata data.

CONCLUSIONI DEL COMITATO PER I RICORSI

Nella sua decisione del 13 dicembre 2001, in ragione delle speciali circostanze del caso, il comitato per i ricorsi aveva ritenuto appropriato che all'Europol venisse data l'opportunità di riesaminare la decisione. Il comitato per i ricorsi ha preso atto degli sviluppi successivi a tale decisione e pertanto limiterà le sue conclusioni alla decisione dell'Europol del 22 gennaio 2001.

In questo caso, il comitato per i ricorsi distingue due questioni.

La prima questione è la risposta data dall'Europol alla richiesta del sig. X di accedere ai dati che lo riguardano.

La Convenzione Europol, all'articolo 19, paragrafo 1, attribuisce il diritto di accesso a tutti gli individui. L'estensione di tale diritto non è specificatamente definita ma, alla luce

dell'articolo 14, paragrafo 1, della Convenzione Europol, deve essere considerata alla stregua del diritto definito dall'articolo 8 della Convenzione d'Europa del 28 gennaio 1981. Tale diritto consente ad ogni persona di accertare se sono stati archiviati dei dati di carattere personale che lo riguardano e, in caso affermativo, gli attribuisce il diritto di conoscerli. Il ricorso riguarda entrambi gli aspetti del diritto di accesso. Ai sensi dell'articolo 19, paragrafo 3, tale diritto va esercitato in conformità con la legislazione dello Stato membro in cui il diritto è invocato, in questo caso il Regno Unito. Questo articolo utilizza l'espressione — comunicazione relativa ai dati", che copre sia la comunicazione dell'esistenza di dati oggetto di trattamento, sia la comunicazione dei dati stessi oggetto di trattamento. Anche la legge sulla protezione dei dati del 1998 riconosce, alla sezione 7, paragrafo 1, il diritto di essere informati sul fatto che ci sono dati oggetto di trattamento ed insieme il diritto alla comunicazione di tali dati. L'esistenza di questi diritti nella legislazione dello Stato membro comporta l'applicabilità del secondo comma dell'articolo 19, paragrafo 3, il quale prevede strettamente i casi in cui la comunicazione vada rifiutata. Se una delle tre fattispecie di esenzione di cui all'articolo 19, paragrafo 3, è applicabile, la comunicazione deve essere rifiutata. Ciò significa che ogni richiesta di accesso in cui trovi applicazione il seconda comma dell'articolo 19, paragrafo 3, deve essere valutata caso per caso, per accertare la necessità di rifiutare la comunicazione in ragione di una delle fattispecie di esenzione. Per quanto l'esercizio del diritto di accesso debba avvenire in conformità con la legislazione dello Stato membro, è l'Europol che ha la responsabilità ultima di verificare l'applicabilità delle esenzioni di cui all'articolo 19, paragrafo 3.

La sezione 29, paragrafo 1, della legge sulla protezione dei dati del 1998 esclude dalla sezione 7 i dati di carattere personale trattati per la prevenzione o l'investigazione di reati e la cattura o il perseguimento giudiziario dei rei, quando l'applicazione della sezione 7 possa arrecare pregiudizio ad uno qualsiasi di questi elementi. Il contenuto di tali esenzioni è strettamente correlato all'esenzione di cui all'articolo 19, paragrafo 3, della Convenzione Europol.

Dalla seconda relazione presentata dal relatore risulta che la decisione dell'Europol è coerente con il parere, dato dall'Information Commissioner (garante delle informazioni) del Regno Unito ai responsabili del trattamento dei dati, circa la forma della risposta ad una richiesta di accesso dell'interessato quando non ci siano dati a disposizione o non ci si possa basare su un'esenzione.

Le argomentazioni utilizzate dall'Europol e dallo SNIC riguardano lo svolgimento delle mansioni dell'Europol, la protezione della sicurezza e dell'ordine pubblico, nonché la prevenzione del crimine, e sono strettamente correlate alla criminalità organizzata. Alla luce della legge e della prassi vigenti nel Regno Unito in merito al diritto di accesso ai dati riguardanti la criminalità organizzata nonché alla luce dell'articolo 19, paragrafo 3, della Convenzione Europol, la decisione dell'Europol rispetto alla richiesta del sig. X è conforme all'articolo 19, paragrafo 3, della Convenzione Europol.

La seconda questione riguarda la richiesta del sig. X di verificare i dati che lo riguardano. L'articolo 19, paragrafo 5, della Convenzione Europol si applica se la legge nazionale applicabile nulla dispone in merito alla comunicazione, oppure nell'ipotesi di una semplice domanda di verifica. Alla luce della sostanza di questo particolare ricorso, la domanda del ricorrente può essere vista come una semplice domanda di verifica. Questo significa che, ai sensi dell'articolo 19, paragrafo 5, della Convenzione Europol, l'Europol dovrà notificare al richiedente che sono state effettuate delle verifiche, senza però dargli alcuna informazione che gli possa rivelare se egli sia noto o meno.

SULLE SPESE

Poiché nessuna richiesta è stata fatta sulla base dell'articolo 27, paragrafo 1, del regolamento interno, non è necessaria alcuna decisione in merito alle spese.

DECISIONE

La decisione dell'Europol sulla richiesta avanzata dal sig. X di accedere ai dati che lo riguardano e di procedere alla loro verifica è conforme ai paragrafi 3 e 5 dell'articolo 19 della Convenzione Europol.

La presente decisione è resa nota in occasione della pubblica riunione del comitato per i ricorsi del 16 maggio 2002, trasmessa alle parti ed inoltrata all'autorità di controllo comune.

Bruxelles, 16 maggio 2002

Mario Manuel Varges Gomes
Presidente del Comitato per i ricorsi
dell'Autorità di controllo comune dell'Europol

F. MEMBRI

AUTORITÀ DI CONTROLLO COMUNE (ACC) DELL'EUROPOL
Presidente : Sig. Klaus KALK
Vicepresidente : Sig. Emilio ACED FELEZ

AUSTRIA

MEMBRI	*SUPPLENTI*
Sig.ra Waltraut KOTSCHY	Sig.ra. Birgit HROVAT-WESENER
Sig.ra Eva SOUHRADA-KIRCHMAYER	

BELGIO

MEMBRI	*SUPPLENTI*
Sig. Paul THOMAS	Sig. B. HAVELANGE
Sig. Bart DE SCHUTTER	

DANIMARCA

MEMBRI	*SUPPLENTI*
Sig.ra. Lena ANDERSEN	Sig. Peter AHLESON
Sig. Ib Alfred LARSEN	

FINLANDIA

MEMBRI	*SUPPLENTI*
Sig. Reijo AARNIO	Sig. Heikki HUHTINIEMI
Sig.ra Maija KLEEMOLA	

FRANCIA

MEMBRI	*SUPPLENTI*
Sig. Alex TÜRK	Sig.ra Marie GEORGES
Sig.ra Florence FOURETS	

GERMANIA

MEMBRI	*SUPPLENTI*
Sig. Joachim JACOB	Sig. Roland BACHMEIER
Sig. Klaus Rainer KALK	Sig.ra Birgitte SCHERBER-SCHMIDT

GRECIA

MEMBRI	*SUPPLENTI*
Sig. Sotirios LYTRAS	Sig. Georgios DELIGIANNIS
Sig.ra Koustoula KAMBOURAKI	

IRLANDA

MEMBRI	*SUPPLENTI*
Sig. Joseph MEADE	Sig. Tom MAGUIRE

ITALIA

MEMBRI	*SUPPLENTI*
Sig.ra Vanna PALUMBO	
Sig. Giuseppe BUSIA	

LUSSEMBURGO

MEMBRI	*SUPPLENTI*
Sig. Georges WIVENES	Sig. Pierre WEIMERSKIRCH
Sig. Edouard DELOSCH	

PAESI BASSI

MEMBRI	*SUPPLENTI*
Sig. Peter J. HUSTINX	Sig.ra Evelien van BEEK
Sig. Ulco van de POL	

PORTOGALLO

MEMBRI	*SUPPLENTI*
Sig. Mário Manuel VARGES GOMES	Sig.ra Isabel CERQUEIRA DA CRUZ
Sig. Amadeu Francisco RIBEIRO GUERRA	

SPAGNA

MEMBRI	*SUPPLENTI*
Sig. José Luis PIÑAR MAÑAS	Sig.ra Concepción ROMERO CIQUE
Sig. Emilio ACED FELEZ	Sig.ra Mercedes ORTUNO

SVEZIA

MEMBRI	*SUPPLENTI*
Sig. Ulf WIDEBÄCK	Sig.ra Agneta RUNMARKER
Sig. Leif LINDGREN	Sig.ra Britt-Marie WESTER

REGNO UNITO

MEMBRI	*SUPPLENTI*
Sig. Richard THOMAS	Sig. David SMITH
Sig.ra Francis ALDHOUSE	

COMITATO PER I RICORSI DELL'ACC

Presidente:	Sig. Mário Manuel VARGES GOMES
Vicepresidente :	Sig. Ulf WIDEBÄCK

AUSTRIA

MEMBRO	*SUPPLENTE*
Sig.ra Waltraut Kotschy	Sig.ra Birgit Hrovat-Wesener

BELGIO

MEMBRO	*SUPPLENTE*
Sig. Paul Thomas	Sig. Bart de Schutter

DANIMARCA	
MEMBRO	*SUPPLENTE*
Sig.ra Lena Andersenensen	Sig. Peter Ahleson
FINLANDIA	
MEMBRO	*SUPPLENTE*
Sig. Reijo Aarnio	Sig.ra Maija Kleemola
FRANCIA	
MEMBRO	*SUPPLENTE*
Sig. Alex Türk	Sig.ra Florence Fourets
GERMANIA	
MEMBRO	*SUPPLENTE*
Sig. Joachim Jacob	Sig. Roland Bachmeier
GRECIA	
MEMBRO	*SUPPLENTE*
Sig. Sotirios Lytras	Sig.ra Koustoula Kambouraki
IRLANDA	
MEMBRO	*SUPPLENTE*
Sig. Joseph Meade	Sig. Tom Maguire
ITALIA	
MEMBRO	*SUPPLENTE*
Sig. Giuseppe Busia	Sig.ra Vanna Palumbo
LUSSEMBURGO	
MEMBRO	*SUPPLENTE*
Sig. Georges Wivenes	Sig. Edouard Delosch
PAESI BASSI	
MEMBRO	*SUPPLENTE*
Sig. Peter .J. Hustinx	Sig. Ulco. van de Pol
PORTOGALLO	
MEMBRO	*SUPPLENTE*
Sig. Mário Manuel Varges Gomes	Sig.ra Isabel Cerqueira da Cruz
SPAGNA	
MEMBRO	*SUPPLENTE*
Sig. Emilio Aced Felez	Sig.ra Concepcion Romero Cique
SVEZIA	
MEMBRO	*SUPPLENTE*
Sig. Ulf Widebäck	Sig. Leif Lindgren
REGNO UNITO	
MEMBRO	*SUPPLENTE*
Sig. Francis Aldhouse	Sig. David Smith

XII - Autorità comune di controllo Schengen

79 Sixth report january 2002 - december 2003 Activities of the Joint Supervisory Authority

Foreword

Eight years have elapsed since the Schengen Information System (SIS) was set up, and now the Joint Supervisory Authority (JSA) in Brussels is submitting its sixth Report.

This document sums up the activity carried out by the JSA in the past two years. Like other texts of this kind, it contains references to initiatives, information campaigns for citizens, decisions, institutional relationships and results achieved, without dwelling on the details – which can be found in the documents adopted by the JSA as well as on its new web site.

Still, this Report has a special value in that it is published on the eve of an historical event – namely, setting out the activities required to deploy, by 2006, a second-generation Information System, called SIS II, which will bring about major innovations and impact considerably on vital functions for Europe and its citizens' rights and fundamental freedoms.

The JSA intends to play a leading role in this major change process by contributing to its guidance.

The SIS is already the largest European centralised database within the framework of the initiatives concerning visas, immigration, and police and judicial cooperation.

Other short-term proposals to amend the Schengen Convention are at an advanced stage of discussion.

As for the long term, the JHA Council of 5-6 June 2003 decided that several new categories of alert, new research fields, interlinks, new purposes, new sensitive categories of personal data – such as biometric data –, new retention periods, and new, larger categories of system user would have to be taken into account for the SIS II.

The purposes to be achieved in future are also important for our democratic societies, however it is necessary to assess their proportionality and carry out a prior checking exercise with regard to the impact that these will have on the rights and fundamental freedoms of the millions of individuals that will be involved for diverse reasons.

The envisaged high-level security measures are not enough. The SIS II should not merely represent a second-generation system from a technical point of view. A revised set of data protection provisions is also required. These should be easy to understand and better known to individuals and practitioners as well as being equal to the challenges posed by the SIS II, providing adequate safeguards and ensuring that the system is consistent with its own purposes.

Data protection does not entail deciding whether given information is to be disclosed or not. In fact, it consists in a more pervasive exercise aimed at affording safeguards, balancing interests, devising proportionate solutions, and organising information flows.

It is necessary to create the best mix between effective police and judicial cooperation and the fundamental right to personal data protection, which has been enshrined in the Charter of Fundamental Rights of the European Union.

The continuing harmonisation of databases in the so-called First and Third Pillars is expected. We call on the other institutions to develop a clear-cut privacy policy as well as a clear-cut concept of the new forms of cooperation that are to replace the compensatory measures originally laid down in the Schengen Convention.

Schengen, Europol, Eurodac, the Visa Information System (VIS) and other systems were set up in different manners, in different periods and for different purposes. Now is the time to enhance the safeguards against the risks of gaps and overlapping, reduce uncertainties further, and do away with merely formal safeguards, lack of information, and sluggish cooperation.

This is why the JSA is grateful to the other institutions, and in particular to the European Parliament, for their closer collaboration, which was fruitfully enhanced in the past few months – in particular with regard to the Spanish proposals to amend the Schengen Convention, the Recommendation adopted by Parliament on 20 November 2003, and the ad hoc workshop held in Brussels on 6 October.

At the latter workshop, the JSA drew the participants' attention to five main requirements:

1) Ensuring that the initiatives concerning the SIS II are reconciled with all the other institutional activities already in progress, such as the Spanish proposals on SIS I, the amendments to the Schengen Convention with regard to trafficking in stolen vehicles, implementing the European arrest warrant, the VIS, and the Greek initiative on the procedure to amend the SIRENE Manual, also with a view to sensible, cost-effective expenditure,

2) Ensuring that the provision for a timely data protection assessment is included in the initial layout of the contract to be granted in 2004 with regard to the SIS II following the public call for tenders,

3) Ensuring effective, continued cooperation with the JSA as shown by the constructive relationship that was developed of late between the JSA and the European Commission,

4) Setting out the objectives of the SIS II prior to laying down its technical features so as to ensure that the new system can work in a logical fashion from the start, and

5) Encouraging improved quality in data protection aimed at more substantive safeguards, by ensuring that the system and its intelligent functions can really be monitored, that it is highly transparent for citizens, and that no redundant data and/or databases are present.

This is a time of strategic importance for the European Union, and data protection is bound to play a specific role.

The SIS II will only manage to be a success story if it is really data protection-oriented. For its part, the JSA is aware that it is entitled to play the enhanced role called for by the European Parliament as well as be provided with a specific budget and adequate resources. The JSA shall also actively cooperate with the European Data Protection Supervisor, and it will continue its activity to address the important issues coming up in the next two years.

The Schengen Joint Supervisory Authority

SCHENGEN JSA ACTIVITY REPORT

CHAPTER 1

1.1. Schengen: the Background

1.1.1. Introduction

Enshrined in the Treaty of Amsterdam, which came into effect in 1999, is the concept of a European Union in which the free movement of persons is assured.

The first steps towards creating an area of free movement came with the Schengen Agreement, signed by France, Germany and the Benelux countries in 1985. Implementing the Agreement, the Schengen Convention of 1990 abolished the internal borders of the signatory states and created a Schengen area with a single external frontier where immigration checks were to be carried out in accordance with a single set of rules.

In response to fears that the unchecked movement of goods and people would be open to abuse, the Convention contained a number of compensatory measures. These included measures to facilitate closer co-operation between border authorities, and the creation of the Schengen Information System (SIS).

1.1.2. The Schengen Information System (SIS)

The SIS is an information system linking up all the states applying the Schengen Convention and the competent authorities in each of those states. National police, customs and border control authorities in the Schengen States use the SIS to make police and customs checks on persons and objects by means of an automatic search procedure. Checks are also made by immigration officials when processing persons from non-Schengen States.

The Schengen Convention specifies the categories of information that may be held in the SIS. National authorities may enter information on certain objects, such as stolen vehicles, and on the following categories of person:

1. persons wanted for arrest for extradition purposes
2. persons refused entry to the Schengen area
3. missing persons or persons who need to be placed under protection
4. persons sought by judicial authorities in connection with criminal proceedings
5. persons who are to be the subject of discreet surveillance or a specific check

The SIS is made up of national sections (NSIS), which can be checked by the authorities competent for making border, customs and police checks; and a central section (CSIS) located in Strasbourg. The authorities in a particular state can search only their own NSIS data file, and each national authority has access to those categories of data needed to carry out its specific checks. Immigration authorities, for example, may only access information concerning persons refused entry to the Schengen area.

To enter information into the system, national officials must first send the information to the national authority responsible for their national section of the SIS (these authorities are known as the SIRENE bureaus). The national SIRENE bureau has to ensure that the information is relevant to the SIS and that Schengen rules have been applied correctly. If so, the information is forwarded to the central section of the SIS, which then updates each national section with the new entry. This ensures that each national section of the SIS is identical to the central section.

1.1.3. The Joint Supervisory Authority

It is important for a complex Europe-wide information system of this kind to adhere to the principles of data protection. Given that a person may be refused access to the Schengen area on the basis of information held in the SIS, it is obviously essential that such information should be accurate and up-to-date, for example.

As a safeguard, the Convention contains a number of provisions relating to data protection; it also established an independent authority – the Joint Supervisory Authority (JSA) – charged with inspecting the central section of the SIS, examining any difficulties of application or interpretation that may arise during the operation of the SIS, and ensuring that the SIS complies with the various data protection provisions mentioned in the Schengen Convention. The JSA comprises two representatives from the national data protection authority of each Schengen State.

1.1.4. Incorporating Schengen into the European Union

Although Schengen began as an intergovernmental convention, the Schengen Convention and the various decisions adopted under it – known collectively as the Schengen acquis – were integrated into the legal and institutional framework of the European Union by the Treaty of Amsterdam. The JSA views this as a positive move, opening Schengen to transparent parliamentary and judicial scrutiny.

The Schengen Agreement paved the way for the area of freedom, justice and security envisaged in the Treaty of Amsterdam. It has since been declared that this area 'should be based on the principles of transparency and democratic control' [1], and it is in this context that the JSA seeks to carry out its tasks. This activity report provides an overview of these tasks, summarising the activities undertaken and the opinions issued over the past two years.

1.2. The Changing Face of the Schengen Information System: SIS II and Other Developments

1.2.1. SIS II

Now, eight years after the introduction of the SIS, the process of replacing the system is under way. There are various reasons for this. The enlargement of the European Union brings with it the need to develop a new system capable of processing a huge amount of information; in addition, those with practical experience of the SIS have been suggesting ways in which the system might be improved. At the same time, developments in the ongoing fight against crime and terrorism, including the creation of new institutions such as Europol and Eurojust, have led to calls for the information held in the SIS to be used for a wider purpose. A new system, SIS II, is being developed and is scheduled to come into operation in 2006.

1.2.2. Initiatives to Amend the Schengen Convention

There are several initiatives to change the SIS even before this new system comes into being. Foremost among these is a Spanish initiative (2) which, among other things, is intended to allow Europol and Eurojust to access the SIS. Another initiative concerns the proposed introduction of a European arrest warrant, which is likely to result in additional categories of information being held in the the SIS.

There are, essentially, two trends that are of particular concern to the JSA. The first relates to the information held in the SIS, with moves to add new categories of information and introduce new types of information, such as biometric data. The second trend concerns access to and use of data held in the SIS. There are proposals to allow other organisations to access the SIS – Europol and Eurojust have already been mentioned – and this is a trend

(1) Taken from the general conclusions of the European Council convened in Tampere in 1999
(2) Official Journal C160, 04/07/2002

that looks set to continue. As this happens, it becomes increasingly likely that data held in the SIS will be used for a wider range of purposes.

The JSA recognises that the SIS has proved to be an essential instrument for safeguarding security across the Schengen area; while at the same time, the rights of individuals whose information is processed in the SIS have been protected by an adequate system of data protection rules and measures.

1.2.3. The Joint Supervisory Authority's Approach

The JSA has warned that, as they stand, these proposals would result in a fundamental change to the nature of the system: whereas the SIS simply alerts the relevant authorities that a particular person is wanted for one of the reasons laid down in the Schengen Convention, the SIS II looks set to become a multi-purpose investigation tool.

As the EU is faced with the prospect of a new system that would allow authorities to share information on millions of individuals for a variety of purposes – possibly using the latest technologies to process sensitive biometric data – there is a clear need for careful consideration of the impact this may have on the rights of individuals. It is necessary to examine all proposals for the SIS II in order to ensure respect for fundamental human rights, and in particular the right to personal data protection that was recently re-affirmed by Article 8 of the Charter of Fundamental Rights of the EU.

In dealing with these various developments, the JSA has set out to:

- raise awareness of any proposals to change the Schengen Convention or the SIS;
- encourage parliamentary scrutiny of such proposals; and
- forge close working relationships with the institutions involved in developing policy on Schengen – particularly the European Parliament, the Council and the European Commission – in order to ensure that the highest standards of data protection are built into the new system.

During the course of 2002 the JSA issued three opinions on the proposals to introduce new functions to the SIS. In these opinions the JSA expressed concern about the moves to allow organisations such as Europol access to the SIS, and requested a more thorough examination of the implications of storing biometric data in the SIS. These opinions are addressed in more detail in the second Part of this report.

The JSA has made efforts to bring the debate on changing the SIS to the fore. On 6 October 2003, a hearing on SIS II was held at the European Parliament before the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs. The hearing provided an opportunity for the JSA to make its position clear. The JSA's chairman, Mr Buttarelli, made a presentation in which he stressed that the SIS II would not be effective if it failed to adhere to data protection principles. He added, however, that data protection need not be an obstacle to change, and that the JSA would be willing to play a constructive role in the development of a second generation SIS. As well as presentations from a number of experts in the field of data protection, the hearing also heard from those with direct responsibility for developing the SIS II, such as Commissioner Vitorino. The JSA was encouraged to note that there was considerable interest from Members of the European Parliament, particularly with regard to the implications of the resulting system on the rights of individuals.

The JSA has sought to co-operate with all bodies involved in the development of the SIS II, both at European level and at national level, and it has urged these bodies to work together to ensure that the highest standards of data protection are built into the new system.

The chairman of the JSA attended another hearing before the Committee on Citizens' Freedoms on 25 March 2003. Entitled 'Data Protection since 11 September 2001: What

Strategy for Europe?', the hearing examined recent developments and the potential implications for data protection. This hearing, together with the hearing in October, helped to build on the JSA's links with the European Parliament, and the Committee on Citizens' Freedoms in particular.

The JSA has been in close dialogue with the Article 36 Committee (the Committee responsible for preparing the ground for Council deliberations on police and judicial co-operation). In a meeting between the chairman of the JSA and the chairman of the Article 36 Committee in February 2002, it was agreed that the Article 36 Committee would forward all relevant documents to the JSA as quickly as possible.

In addition, the JSA has been developing links with the European Commission. The Commission, which is responsible for funding and developing the SIS II, recently sent the JSA a copy of a feasibility study, covering technical and organisational aspects of the development and installation of the new system. Officials from the Commission's IT unit attended the JSA's meeting in December 2003, and provided an overview of the developments that have taken place so far. The Commission representatives have agreed to attend the next meeting of the JSA in 2004, and this will provide the JSA with the opportunity to pose questions on specific aspects of the development process.

CHAPTER 2

2.1. THE WORK OF THE JOINT SUPERVISORY AUTHORITY

2.1.1. How the JSA Operates

The JSA comprises delegations from the 15 countries with information currently in the SIS: namely, Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain and Sweden. Each of these countries may have two members and two alternate members. Ireland and the UK, together with the ten countries that are soon to join the EU, have been granted observer status.

The JSA usually meets quarterly, though there is the possibility of holding extraordinary meetings to discuss issues requiring immediate attention. On 7 October 2003, for example, the JSA met to discuss the hearing on SIS II that had been held in the European Parliament the previous day. Over the course of the last two years the JSA has convened ten meetings.

The members of the JSA elect a chairman and a vice-chairman to preside over meetings. According to the JSA's rules of procedure each can serve for up to two one-year periods. In December 2003 Mr Buttarelli completed his second term of office. The vice-chairman, Mr van de Pol, was elected chairman at the JSA's meeting of 11 December 2003. At the same meeting Ms Cruz was elected as the new vice-chairman.

Although the JSA strives to reach decisions by consensus, in cases where this is not possible members may decide to hold a vote, with each delegation entitled to a single vote. Those delegations with observer status do not have voting rights.

2.1.2. Working Together: Data Protection and the Europe-Wide Information Systems

Moves to facilitate co-operation between police and judicial authorities of the EU Member States have led to the creation of other Europe-wide information systems. Apart from the SIS, the two main systems operating in this field are the Europol information system and the Customs Information System.

Each system has an independent joint supervisory authority charged with ensuring that

the systems comply with data protection provisions. These two joint supervisory authorities share some similarities with the Schengen JSA: all three authorities are made up of representatives from the national data protection authorities, they are all served by the same joint secretariat based in Brussels, [3] and they deal with many issues of a similar nature. With this in mind there have been recent attempts to co-ordinate the efforts of the different authorities.

- In March 2003 the three joint supervisory authorities set up a working group to review, from a data protection perspective, the existing Europe-wide information systems. This working group was given a mandate to examine the existing systems in order to ascertain whether the purposes of the different systems overlap, and to consider the implications of future developments.

- The three authorities also established a technical group. Consisting of technical experts from the data protection authorities of the various Member States, this group provides technical support to the joint supervisory authorities. The group is currently in the process of developing a standard tool for inspecting the three information systems.

As a footnote, it is worth mentioning the role of the European Data Protection Supervisor. [4] The Supervisor, who has yet to be appointed, will be responsible for monitoring that information in the SIS which relates to immigration (specifically, alerts entered under Article 96). For this reason it will obviously be important to ensure that the Schengen JSA works with the Supervisor to develop a co-ordinated approach to supervising the SIS.

2.2. Activities

2.2.1. Raising Awareness

The JSA aims to ensure that individuals are informed of the rights they have under the Schengen Convention.

Briefly, these rights are:

1. the right of access to information held on you in the SIS
2. the right to correct such information if it is factually incorrect or to have it deleted if it is held unlawfully
3. the right to bring an action to correct, delete or obtain information, or to obtain compensation
4. the right to ask a national data protection authority to check the information held on you in the SIS

The JSA's first information campaign in 1998 resulted in the publication of a rights leaflet. The distribution of this leaflet, which informed individuals of the rights they have in relation to information held on them in the SIS, led to a significant increase in the number of requests for access. The JSA has decided to publish a new edition of the rights leaflet and this will soon be available at airports and other national entry points throughout the Schengen area.

Individuals can exercise their right of access in any of the states in the Schengen area, but the procedure varies depending on the national law of the state in which access is requested. In 2002, the JSA produced a booklet – The Guide – which provides details of the procedure to be followed in each of the Schengen States. This information can now be found on the JSA's web site.

In July 2003 the JSA launched a new web site with the intention of providing easy access to the opinions and recommendations of the JSA. The site, which will be maintained by the secretariat, is currently available in English but work is under way to make it available in all

EU languages. The web site address is www.schengen-jsa.dataprotection.org.

In October 2003 the JSA issued its first newsletter. The newsletter was produced in time for the hearing on SIS II at the European Parliament and it contained information on the ongoing work of the JSA. The JSA intends to publish such a newsletter – or perhaps a news update on the web site – on a regular basis.

As well as ensuring that individuals are informed of their rights, the measures outlined above, and the development of the web site and the newsletter in particular, are also intended to raise the profile of the JSA. It is important that other bodies have the opportunity to see exactly what the JSA does. Moreover, increasing awareness of the JSA among the key decision-making bodies of the EU will enable the JSA to voice its concerns with more effect. In addition, such bodies might feel more inclined to consult the JSA to ensure that data protection considerations are taken into account.

2.2.2. Inspection

The JSA has the task of ensuring that the technical support function of the SIS (the CSIS) complies with the data protection principles set out in the Schengen Convention and the other legal texts on data protection mentioned in that Convention, such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.

In December 2002, the JSA set up an inspection team to inspect the CSIS for the second time. The inspection team visited the CSIS in Strasbourg on 25 and 26 March 2003.

The inspection team developed provisional checklists setting out the checks to be carried out during the in situ inspection. These checks covered documents, systems, the procedures applied and the people involved in the processing of data.

Since the JSA's last inspection report (adopted on 1 November 1999) the support function of the SIS has been modified. The JSA considers the present system, known as CSIS1+, to be an improvement on the previous system in so far as compliance with the relevant data protection principles is concerned.

The general conclusion was a positive one. The JSA did, however, adopt some recommendations – largely technical in nature – in order to further improve compliance with the Convention and other related data protection provisions. The latest inspection report was adopted by the JSA at its meeting on 25 September 2003 and it was agreed that the inspection team should monitor the extent to which its recommendations have been followed in March 2004, six months after the adoption of the report.

It is worth noting that during the course of this inspection the team had the full co-operation of the staff responsible for managing the CSIS.

2.2.3. Third Country Nationals and Access to the Schengen Area – Article 96 Data

Under Article 96 of the Schengen Convention, the authorities in Schengen States may enter alerts on third country nationals refused entry to the Schengen area. Article 96 stipulates that before such an alert can be entered there must first have been a national alert resulting from a decision taken by the competent administrative authorities or courts in accordance with the rules of procedure laid down by national law.

The vast majority of alerts on persons held in the SIS have been entered under Article 96, and the JSA has decided to focus on the issue of Article 96 and on the way in which it is applied in the different Schengen States.

An action plan was drawn up and it was agreed that each national data protection authority should check whether personal data entered by the authorities in their country

had been entered in compliance with the provisions of Article 96. It was also decided that the JSA should look to assess, in the short term, the application and interpretation of Article 96 in the different countries of the Schengen area.

The JSA first set out to produce an overview of the various national laws that lead to a decision resulting in an Article 96 alert. To this end, a questionnaire was drawn up and sent to the national data protection authorities of the Schengen States. Results are now being compiled. The JSA's next step has been to develop a methodology for examining Article 96 alerts and the extent to which they comply with the relevant national regulations.

The results from the investigation into the use of Article 96 will require complex analysis, and the whole process is expected to continue for the next two years.

2.3. OPINIONS

2.3.1. Changes to the SIS

2.3.1.1. Spanish Initiative and Other Proposals to Change the SIS

The JSA has issued three opinions on the proposals to change the Schengen Convention: in June, October and December 2002.

The JSA noted that the proposals to grant Europol and Eurojust access to the SIS amounted to a fundamental departure from the basic principles of Article 102 of the Schengen Convention, which limits the use of Schengen data to the purposes laid down in each category of alert. Furthermore, the JSA stressed that the tasks for which these organisations might access the SIS must be in compliance with those articles of the Schengen Convention that deal with access to and use of SIS data. There is need for clarification of the specific tasks for which Europol and Eurojust will require access to SIS data. In general, the JSA is of the view that more information on these proposals is needed.

Proposals to include biometric data in the SIS are of concern to the JSA. Once again, the JSA stated in its opinions that it needed more information in order to make a proper assessment of the implications. There would appear to be two developments: first is the proposal to introduce fingerprints and photographs and, second, the suggestion that the SIS might process other, more sensitive biometric data in the future. It is argued that it is necessary for the SIS to hold fingerprints and photographs so as to identify a particular individual when there are doubts concerning identity. However, the JSA remains of the view that photographs and fingerprints should only be incorporated where it is essential for the execution of an alert and, to date, the JSA has not been presented with any information to suggest that it is necessary to process such information in the case of all alerts. Moreover, a number of questions remain. Will this information only be accessible after a hit and when needed for identification? What conditions will be in place to safeguard the rights of individuals? In any case, there ought to be a full and open discussion of the implications of creating a Europe-wide information system in which sensitive biometric data – such as DNA data – are processed.

2.3.1.2. The European Arrest Warrant

A Framework Decision has been drawn up with a view to replacing the existing extradition arrangements with a European arrest warrant. The European arrest warrant is defined as any judicial decision issued by a Member State with a view to the arrest or surrender by another Member State of a requested person. This may be done for the purposes of conducting a criminal prosecution, for example. Listed in a specimen form attached to the Framework Decision are certain categories of information which the European arrest warrant must contain: these include information on the identity of the person concerned, the issuing judicial authority and the nature of the offence. If this additional information were

to be communicated via the SIS, the SIS would have to be altered considerably.

Although the JSA has not yet issued an opinion on this topic, it has asked the Article 36 Committee whether the categories of information set out in the specimen form attached to the Framework Decision will be incorporated into the SIS. The Article 36 Committee has since confirmed that this is the intention.

2.3.1.3. Accession of Ireland and the UK

In 1999 the UK asked to take part in some aspects of Schengen: namely, co-operation in criminal matters, the fight against drugs, and the SIS. The UK request was approved by Council Decision in May 2000. Ireland asked to participate in some aspects of Schengen in 2000, and in all the provisions concerning the implementation and operation of the SIS. In February 2002 the Council adopted a Decision approving Ireland's request.

Both countries are required to comply with the data protection provisions set out in the Schengen Convention in those areas where they apply the Schengen acquis. In order to assess the level of data protection in both countries the JSA asked the Irish Data Protection Commissioner and the UK's Information Commissioner – who have both been granted observer status by the JSA – to provide documents detailing their national data protection legislation. They were also asked to indicate whether they would take account of the JSA's opinions. Both Commissioners submitted the requested information and, after evaluating the documents, the JSA concluded that from a data protection perspective there were no objections to the accession.

2.3.1.4. Implementation of Schengen in the UK

The UK opted to participate in the provisions of the Schengen acquis concerning the establishment and operation of the SIS except in respect of those provisions concerning alerts entered, for immigration purposes, on persons to be refused entry to the Schengen area (Article 96 alerts).

In 2001 the UK submitted a proposal for implementing the SIS in the UK. However, the JSA voiced concerns about this proposal, as it would lead to the processing of Article 96 data in the UK. This would be in breach of Article 94 of the Schengen Convention which expressly limits the processing of data in the NSIS to those data required for the purposes laid down in the Schengen Convention. In other words, given that the UK would not be applying Article 96 of the Convention, Article 96 data should not be processed in the UK.

The JSA did accept, however, that the UK would need limited access to Article 96 alerts in order to comply with Article 107 of the Convention which requires the state entering an alert to ascertain whether the person on whom the alert is being entered is already the subject of an alert in the system.

In an attempt to allay these concerns the UK gave assurances that although all SIS data would be sent to the UK, Article 96 data would be filtered out at the UK NSIS. This filtered database would be the only one to which all end users would have access – with access to Article 96 data restricted to a limited number of staff. In an opinion issued in February 2002, the JSA made it clear that any mechanism in which Article 96 data were sent to the UK would be in breach of Article 94 and, as such, unacceptable.

A solution was found with the proposal that a filter should be placed at the CSIS in Strasbourg. This filter will prevent Article 96 data from being transmitted to the UK in the first place. New UK alerts will be checked against the existing Article 96 alerts at the CSIS and an automated message will then be sent to the UK in cases where a double alert is found; if further investigations reveal that the alerts do not concern the same person, the UK alert will be accepted by the CSIS and sent out as any other alert.

2.3.1.5. Vehicle Registration Authorities and the Schengen Information System

There is a proposal to add a new article, Article 102a, to the Schengen Convention. [5] This new article would allow those public authorities charged with issuing vehicle registration certificates in the Member States to access the SIS directly and to search data concerning vehicles and trailers, blank official documents and issued identity papers which have been stolen, misappropriated or lost. It is argued that such access will allow authorities to check the status of vehicles presented to them for registration, and to ensure that a particular person applying to become holder of a registration certificate is not using identity or vehicle registration documents which have been stolen, misappropriated or lost.

Direct access to the SIS is to be limited to public vehicle registration authorities. In those Member States where vehicle registration is carried out by private companies and other non-governmental licensing authorities, access will be indirect – and obtained only through those authorities with direct access to the SIS by virtue of Article 101 of the Schengen Convention.

The JSA noted that Article 9 of a Council Directive of 1999 on registration documents for vehicles [6] has been cited as the legal basis providing for the exchange of information between Member States for the purpose of issuing vehicle registration certificates. Article 9 of the Council Directive states that authorities 'may exchange information at bilateral or multilateral level in particular so as to check, before any registration of a vehicle, the latter's legal status'. This would seem to provide for the exchange of information to ascertain the status of a vehicle.

However, the JSA expressed concerns about whether Article 9 provides sufficient legal basis for vehicle registration authorities to search SIS data concerning identity documents. The vehicle registration certificate (the template of which is contained in an annex to the Council Directive) does indeed require the personal details of the holder, but there remains the question whether the cited Council Directive would allow vehicle registration authorities to search SIS data on identity documents for this purpose.

The JSA also stressed that this proposal is part of a continuing trend, marking another departure from the original purposes of the SIS. Whereas access to the SIS was originally limited to border, police, customs and immigration authorities, this proposal will see access granted to another type of body – vehicle registration authorities. Once such authorities have access to SIS data, there will be a new group of users with access to the SIS, and SIS data will be used for the additional purpose of supporting the EU common transport policy.

2.3.2. Opinion on Articles 112 and 113 of the Schengen Convention

The JSA is responsible for examining any difficulties of application or interpretation that may arise during the operation of the SIS.

The Aliens Directorate of the Greek Police asked the Greek data protection authority for its opinion on the period for which alerts entered under Article 96 of the Schengen Convention could be retained in the SIS.

Articles 112 and 113 of the Schengen Convention deal with the retention of data in the SIS.

Article 112 stipulates that personal data entered into the SIS for the purposes of tracing persons shall be kept only for the time required to meet the purposes for which they were entered, and in any case the state which issued the alert must review the need for continued storage of that alert not later than three years after it was entered.

Article 113, on the other hand, states that data other than those referred to in Article 112 may be retained in the SIS for up to 10 years. This Article makes no mention of any requirement to review retention during that ten-year period.

The Greek data protection authority considered the problem and came to the initial

(5) COM (2003) 510 % contains the proposed amendment and an explanatory memorandum

(6) Council Directive 1999/37/EC of 29 April 1999

conclusion that because Article 112 referred to personal data entered in the SIS 'for the purposes of tracing persons' [emphasis added], this Article and the requirement to review retention within three years did not apply to Article 96 alerts. It was argued that rather than being used to trace persons, Article 96 alerts are used to prevent certain persons from entering the Schengen area. Consequently, the Greek data protection authority ruled that the retention of Article 96 data should be covered by Article 113.

The Greek data protection authority subsequently asked the JSA to consider the matter. In an opinion issued in October 2002 the JSA declared that Article 112 was intended to apply to all personal data held in the SIS including those data entered under Article 96 and that, as a result, the retention of Article 96 alerts should be reviewed no later than three years after being entered.

The main principle behind this opinion was that the Schengen Convention does not distinguish between the actions taken in relation to alerts held in the SIS, and it was intended that Article 112 should apply to all personal data held in the SIS.

2.3.3. Austria's Foreign Missions and Access to the Schengen Information System

Article 101(4) of the Schengen Convention requires all Schengen States to supply a list of the competent authorities allowed to carry out direct searches of data held in the SIS. The latest version of this document [7] revealed that the foreign missions of all Schengen States could access alerts entered under Article 96 of the Schengen Convention. The legal basis for such access is provided by Article 101(2) of the Convention, which stipulates that access to data entered in accordance with Article 96 and the right to search such data directly may be exercised by the authorities responsible for examining visa applications.

In addition, the list showed that, as well as having access to Article 96 alerts, the Austrian Federal Ministry of Foreign Affairs and its missions and posts abroad had access to alerts entered under Articles 95, 97, 98 and 100 of the Schengen Convention. Article 101(1)(b) of the Convention was cited as the legal basis for such access. The JSA was asked to consider whether the provisions of the Schengen Convention would allow these authorities to have access to alerts entered under Articles 95, 97, 98 and 100.

The JSA pointed out that although Article 101(1)(b) had been cited as the legal basis on which the Austrian Federal Ministry of Foreign Affairs and its missions and posts abroad could access these other alerts, this Article states that access to such data is to be reserved exclusively to the authorities responsible for 'police and customs checks carried out within the country, and the co-ordination of such checks'. Consequently, the JSA took the view that a national authority should not have access to alerts entered under Articles 95, 97, 98 and 100 of the Schengen Convention unless it can be shown that the tasks of that authority include carrying out police and customs checks (or the co-ordination of such checks), and that these tasks are laid down in law.

The JSA brought this matter to the attention of the Austrian data protection authority. The Austrian data protection authority subsequently raised the matter with the appropriate national authorities, and it has since been confirmed that the Austrian Federal Ministry of Foreign Affairs and its missions and posts abroad will now only have access to alerts entered in the SIS under Article 96 of the Schengen Convention.

(7) 6265/0/03 SIRIS 19
COMIX 89 REV 1

CHAPTER 3

3.1. EVALUATION OF THE PAST TWO YEARS

The two-year period covered by this report has been an eventful one.

As this report shows, the JSA set out to raise awareness of the proposed changes to the SIS and to influence the development of the second generation SIS, but how successful has it been?

The hearings at the European Parliament have given prominence to the debate, and the Committee on Citizens' Freedoms has shown a real interest in the data protection implications of these developments. Furthermore, the JSA is pleased to note that, increasingly, its opinions are being taken into account by decision-makers. This is something that others have noticed in the past – the following is an extract from a document published by the Commission:

'The JSA has played a crucial role . . . issuing opinions and recommendations for the proper functioning of the SIS in line with the rules and rights relating to data protection laid down in the Schengen Convention. In particular it identified 15 recommendations in April 2000, most of which have already been acted upon.'(8)

3.2. THE WAY FORWARD

There are various challenges facing the JSA over the coming period.

- Ten new countries are to join the EU. In preparation for this the JSA has been inviting representatives of the data protection authorities of the acceding countries to its meetings since June 2003. The JSA will strive to improve its efforts to prepare these data protection authorities for accession to the Schengen acquis.

- The JSA considers the development of the SIS II to be one of the most important challenges it faces. There is the prospect of a new Europe-wide system that would allow authorities to share information on millions of individuals for a variety of purposes – possibly using the latest technologies to process sensitive biometric data.

The JSA is committed to monitoring the progress of the SIS II, and will examine all proposals in order to ensure respect for fundamental rights, and in particular the right to personal data protection that was recently re-affirmed by Article 8 of the Charter of Fundamental Rights of the European Union. It is hoped, too, that this activity report might serve to encourage discussion on the SIS II in national parliaments.

MEMBERS OF THE JOINT SUPERVISORY AUTHORITY (*)

The following list represents the membership of the JSA as at December 2003.

Austria	
Members	Alternates
Waltraut Kotschy	Birgit Hrovat-Wesener
Eva Souhrada-Kirchmayer	Gerhard Kunnert
Belgium	
Members	Alternates
Bart de Schutter	Priscilla de Locht
Benedicte Havelange	
Denmark	
Members	
Ib Larsen	
Helene Grønfeldt	
Finland	
Members	Alternates
Reijo Aarnio	Heikki Huhtiniemi
Maija Kleemola	
France	
Members	
Alex Türk	
Florence Fourets	
Germany	
Members	Alternates
Joachim Jacob	Wolfgang von Pommer Esche
Friedrich von Zezschwitz	Angelika Schriever-Steinberg
Greece	
Members	Alternates
Stylianos Sarivalassis	Philippos Mitletton
Ioannis Tsoukalas	Efrosini Siougle
Iceland	
Members	
Margret Steinarsdottir	
Italy	
Members	
Giovanni Buttarelli Chairman	
Sebastiano Neri	
Luxembourg	
Members	Alternates
Georges Wivenes	Edouard Delosch
Pierre Weimerskirch	
The Netherlands	
Members	Alternates
Peter Hustinx	Evelien van Beek
Ulco van de Pol Deputy Chairman	Niels Groenhart

(*) Annex 1

Norway

Members	Alternates
George Apenes	Hanne Gulbrandsen
Guro Slettemark	

Portugal

Members
Isabel Cruz
Luis Barroso

Spain

Members	Alternates
José Luis Piñar Mañas	Emilio Aced Félez
Miguel Lopez-Herrero	

Sweden

Members	Alternates
Ulf Wideback	Leif Lindgren
Britt-Marie Wester	Birgitta Abjornsson

XIII - Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali

(art. 29 direttiva 95/46/CE)

Nuove sfide

80 Documento di lavoro sulla biometria

GRUPPO PER LA TUTELA DEI DATI PERSONALI
(ARTICOLO 29)

12168/02/IT
WP 80

Documento di lavoro sulla biometria
Adottato il 1° agosto 2003

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995[1],

visti gli articoli 29 e 30, paragrafi 1, lettera a) e 3, della direttiva,

visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente documento di lavoro.

1. Introduzione

Il rapido sviluppo delle tecnologie biometriche e l'estensione della loro applicazione nel corso degli ultimi anni rendono necessaria un'attenta analisi per quanto concerne l'aspetto della tutela dei dati [2].

Il gruppo è stato istituito a norma dell'articolo 29 della direttiva 95/46/CE. Si tratta dell'organo consultivo indipendente dell'UE in tema di tutela dei dati e della vita privata. I compiti del gruppo sono definiti dall'articolo 30 della direttiva 95/46/CE e dall'articolo 14 della direttiva 97/66/CE. Segretariato: Direzione E (Servizi, proprietà intellettuale e industriale, media e protezione dei dati) della Commissione europea, Direzione generale "Mercato interno", B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136. Website: www.europa.eu.int/comm/privacy

(1) Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile in http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

(2) Dopo gli avvenimenti dell'11 settembre 2001 la biometria è stata spesso presentata come un valido strumento per migliorare la sicurezza pubblica. In sede di Unione europea sono in corso discussioni sulla possibilità di integrare elementi biometrici a livello di carte di identità, passaporti, documenti di viaggio e visti. Gli Stati Uniti richiederanno presto identificatori biometrici per gli stranieri in ingresso o in uscita dal paese. La Convenzione n.108 dell'OIL è stata modificata nel 2003 allo scopo di introdurre il ricorso obbligatorio alla biometria per i lavoratori marittimi. Sono in atto discussioni anche in altri forum internazionali quali il G8, l'OCSE ecc.

L'uso generalizzato e incontrollato della biometria solleva preoccupazioni in relazione alla tutela dei diritti e delle libertà fondamentali degli individui. Si tratta di dati di carattere speciale in quanto riguardano le caratteristiche comportamentali e fisiologiche di un individuo e sono tali da consentirne l'identificazione univoca [3].

Attualmente si ricorre spesso al trattamento di dati biometrici nelle procedure automatizzate di autenticazione/verifica e di identificazione, in particolare per il controllo dell'accesso ad aree tanto fisiche quanto virtuali (accesso a determinati sistemi o servizi elettronici).

In precedenza l'impiego della biometria era limitato essenzialmente alle prove del DNA e al controllo delle impronte digitali. La rilevazione delle impronte digitali è stata utilizzata segnatamente a fini giudiziari (ad es. nell'ambito di indagini penali). Se la società incoraggia lo sviluppo di basi di dati contenenti impronte digitali o altri dati biometrici per altre applicazioni correnti le possibilità di un loro reimpiego da parte di terzi a scopo di confronto e ricerca per fini propri potrebbero aumentare, pur non essendo questo l'obiettivo inizialmente perseguito; tra questi terzi potrebbero figurare le autorità incaricate di applicare la legge.

Una preoccupazione specifica in relazione ai dati biometrici deriva dalla possibilità che, con l'uso generalizzato di tali dati, il pubblico diventi insensibile agli effetti che il loro trattamento può avere sulla vita quotidiana. L'uso di elementi biometrici nelle biblioteche scolastiche, ad esempio, può diminuire la consapevolezza dei bambini quanto ai rischi legati alla tutela dei dati e alle possibili ripercussioni sulla loro vita futura.

Il presente documento si prefigge di contribuire ad una applicazione efficace ed omogenea delle disposizioni nazionali in tema di protezione dei dati adottate conformemente alla direttiva 95/46/CE in relazione ai sistemi biometrici. Esso si concentra principalmente sulle applicazioni biometriche a fini di autenticazione e verifica. Il gruppo si propone di fornire linee guida uniformi a livello europeo, destinate in particolare all'industria dei sistemi biometrici ed agli utilizzatori di tali tecnologie.

2. Descrizione dei sistemi biometrici

Per sistemi biometrici si intendono le applicazioni di tecnologie biometriche che permettono l'identificazione e/o l'autenticazione/verifica automatica di un individuo [4]. Le applicazioni a fini di autenticazione/verifica sono spesso utilizzate per vari compiti in settori completamente differenti e sotto la responsabilità di numerose entità diverse.

Ogni tecnica biometrica, che sia utilizzata a scopo di autenticazione/verifica o di identificazione, dipende, in misura maggiore o minore, dall'elemento biometrico considerato:

- **universale**: l'elemento biometrico è presente in tutte le persone [5];
- **unico**: l'elemento biometrico deve essere distintivo per ogni persona;
- e **permanente**: ogni persona conserva il proprio elemento biometrico nel corso del tempo.

Si possono distinguere due categorie principali di tecniche biometriche a seconda che vengano utilizzati dati stabili o dati comportamentali dinamici [6].

Esistono, in primo luogo, tecniche di tipo fisico e fisiologico che misurano le caratteristiche fisiologiche di una persona. Esse comprendono: la verifica delle impronte digitali, l'analisi dell'immagine delle dita, il riconoscimento dell'iride, l'analisi della retina, il riconoscimento del volto, la geometria della mano, il riconoscimento della forma dell'orecchio, il rilevamento dell'odore del corpo, il riconoscimento vocale, l'analisi della struttura del DNA [7], l'analisi dei pori della pelle ecc..

In secondo luogo esistono tecniche di tipo **comportamentale** che misurano il comportamento di una persona. Esse comprendono la verifica della firma manoscritta, l'analisi della battitura su tastiera, l'analisi dell'andatura ecc.

Tenendo conto dei rapidi progressi tecnici e della crescente preoccupazione in tema di

(3) L'identificazione univoca dipende tuttavia da numerosi fattori quali le dimensioni della base di dati e il tipo di elementi biometrici utilizzati.

(4) La distinzione fra autenticazione (verifica) ed identificazione è importante. L'autenticazione risponde alla domanda: sono la persona che dichiaro di essere? Il sistema certifica l'identità della persona grazie all'elaborazione di dati biometrici che si riferiscono all'individuo autore della domanda e prende una decisione sì/no (confronto 1:1). L'identificazione risponde alla domanda: chi sono io? Il sistema riconosce l'individuo autore della domanda distinguendolo da altre persone i cui dati biometrici sono a loro volta registrati. In questo caso il sistema prende una decisione "1 su n" e risponde che la persona che pone la domanda è X.

(5) A questo proposito gli elementi biometrici non sono tutti equivalenti ed il tasso di differenziazione di una persona da un'altra può variare considerevolmente in funzione del tipo di dati biometrici utilizzati. Gli elementi biometrici maggiormente distintivi sembrano essere il DNA, la retina e le impronte digitali.

(6) Alcune tecniche possono fondarsi tanto sulla fisiologia quanto sul comportamento.

(7) Benché l'uso del DNA a fini di identificazione biometrica sollevi questioni specifiche queste non verranno discusse nel presente documento. Va detto comunque che attualmente non sembra possibile generare un profilo di DNA in tempo reale come strumento di autenticazione.

sicurezza molti sistemi biometrici funzionano associando diverse modalità biometriche dell'utilizzatore ad altre tecnologie di identificazione o autenticazione. Alcuni sistemi, ad esempio, associano il riconoscimento del volto alla registrazione della voce. Per l'autenticazione si possono utilizzare contemporaneamente tre metodi, basandosi su qualcosa che l'individuo conosce (*password*, numero personale di identificazione (PIN), ecc.), qualcosa che egli possiede (dispositivo di autenticazione o *token*, CAD key, *smart card*, ecc.) e qualcosa che è proprio della sua persona (una caratteristica biometrica). Nel caso di un computer, ad esempio, una persona potrebbe inserire una *smart card*, digitare una *password* e presentare le proprie impronte digitali.

La raccolta di campioni biometrici, i cosiddetti dati biometrici (ad esempio, l'immagine dell'impronta digitale, l'immagine dell'iride o della retina, la registrazione della voce), viene effettuata nel corso della cosiddetta fase di "iscrizione" utilizzando un sensore specifico per ogni tipo di elemento biometrico. Il sistema biometrico estrae dai dati biometrici i tratti specifici dell'utilizzatore necessari per elaborare un "modello" biometrico. Il modello è una riduzione strutturata di un'immagine biometrica, ossia la misura biometrica registrata di un individuo. È tale modello, presentato in forma digitale, ad essere archiviato e non l'elemento biometrico in se stesso. I dati biometrici possono inoltre essere elaborati come dati grezzi (un'immagine) in funzione del sistema biometrico utilizzato [8].

La fase di iscrizione svolge un ruolo essenziale dato che è l'unica in cui sono presenti contemporaneamente dati grezzi, algoritmi di estrazione e protezione (crittografia, *hashing* ecc.) e modelli. A questo proposito va sottolineato che se i dati grezzi rivelano informazioni che possono essere considerate di natura delicata a termini dell'articolo 8 della direttiva 95/46/CE il processo di iscrizione di tali dati va allora effettuato conformemente a tale disposizione (vedi nel seguito punto 3.7).

Un'altra questione importante in relazione alla tutela dei dati riguarda la forma in cui vengono conservati i modelli relativi agli utilizzatori, che dipende dal tipo di applicazione per cui verrà utilizzato il dispositivo biometrico nonché dalle dimensioni dei modelli stessi. I modelli possono essere archiviati secondo una delle seguenti modalità:

a) nella memoria di un dispositivo biometrico;
b) in una base di dati centrale;
c) in tessere plastificate, schede ottiche o *smart card*. Questo metodo di conservazione consente agli utilizzatori di portare con sé i propri modelli come dispositivi di identificazione.

In teoria, ai fini dell'autenticazione/verifica, non è necessario memorizzare i dati di riferimento in una base di dati; è sufficiente archiviare i dati personali in un sistema decentralizzato. L'identificazione invece è possibile solo memorizzando i dati di riferimento in una base di dati centralizzata dato che, per accertare l'identità della persona interessata, il sistema deve confrontare i suoi modelli o i suoi dati grezzi (immagine) con i modelli o i dati grezzi di tutte le persone i cui dati sono già registrati a livello centrale.

Un altro punto essenziale in relazione alla tutela dei dati è rappresentato dal fatto che taluni sistemi biometrici si basano su informazioni, quali i campioni di DNA o le impronte digitali, che possono essere raccolte all'insaputa della persona interessata, che può inconsapevolmente lasciare tracce. Applicando un algoritmo biometrico alle impronte digitali trovate su un bicchiere può essere possibile [9] determinare se la persona è registrata in una base di dati contenente dati biometrici e, in caso affermativo, scoprire la sua identità confrontando i due modelli. Questo si applica inoltre ad altri sistemi biometrici quali quelli basati sull'analisi della battitura su tastiera o sul riconoscimento a distanza del volto a causa delle caratteristiche specifiche della tecnologia adottata [10]. L'aspetto problematico è rappresentato dal fatto che, da un lato, questa raccolta e questo trattamento di dati possono essere effettuati all'insaputa della persona interessata e, dall'altro, che indipendentemente dalla loro attuale affidabilità tali tecnologie biometriche si prestano ad un uso generalizzato a causa del loro "basso livello di intrusività". È quindi necessario stabilire garanzie specifiche in materia.

(8) Il presente documento si riferisce principalmente ai sistemi biometrici basati sui modelli, ma può essere applicato anche in caso di dati grezzi. La specificità dei dati grezzi tuttavia può rendere necessario l'adattamento delle prescrizioni in tema di tutela dei dati.

(9) Sono tuttavia necessari alcuni elementi quali la capacità di raccogliere l'impronta digitale dal bicchiere senza danneggiarla, l'attrezzatura tecnica necessaria per elaborare i dati a partire dalle impronte digitali, l'accesso all'algoritmo del costruttore e/o alla base di dati contenente le impronte digitali.

(10) Si veda il punto 3 sull'applicazione della direttiva 95/46/CE e in particolare il punto 3.3 sull'obbligo di informare la persona interessata.

3. Applicazione dei principi della direttiva 95/46/CE

3.1. Applicazione della direttiva 95/46/CE

L'articolo 2, lettera a) della direttiva 95/46/CE definisce i "dati personali" come "qualsiasi informazione concernente una persona fisica identificata o identificabile (...); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica (...)". La considerazione preliminare 26 aggiunge che "per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona".

Conformemente a tale definizione le misure di identificazione biometrica o la loro traduzione digitale in un modello sono, nella maggior parte dei casi, dati a carattere personale [11]. I dati biometrici possono sempre essere considerati come "informazione concernente una persona fisica" in quanto sono dati che, per la loro stessa natura, forniscono informazioni su una determinata persona. Nell'ambito dell'identificazione biometrica la persona è generalmente identificabile in quanto i dati biometrici sono utilizzati per l'identificazione o l'autenticazione/verifica almeno nel senso di distinguere la persona interessata da tutte le altre [12].

L'articolo 3, paragrafo 1 della direttiva 95/46/CE stabilisce che il principio della tutela dei dati si applica al trattamento di dati personali interamente o parzialmente automatizzato nonché al trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi. Le disposizioni delle direttiva non si applicano se il trattamento dei dati viene effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico. Molte applicazioni biometriche ad uso domestico rientrano in questa categoria.

Oltre a tali esclusioni specifiche il trattamento dei dati biometrici può essere considerato lecito solo se tutte le procedure utilizzate, a partire dall'iscrizione, vengono effettuate conformemente alle disposizioni della direttiva 95/46/CE.

Il presente documento non si occupa di tutte le questioni sollevate dall'applicazione della direttiva 95/46/CE ai dati biometrici. Esso tratta unicamente delle questioni più importanti e non offre quindi una panoramica esauriente delle conseguenze dell'applicazione della direttiva 95/46/CE.

3.2. Principio della finalità e della proporzionalità

L'articolo 6 della direttiva 95/46/CE stabilisce che i dati personali devono essere rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. I dati personali inoltre devono essere adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e successivamente trattati (principio della finalità).

Il rispetto di tale principio implica in primo luogo che venga determinata con chiarezza la finalità per la quale i dati biometrici sono rilevati e trattati. È necessario altresì valutare il rispetto della proporzionalità e della liceità, considerando i rischi per la tutela dei diritti e delle libertà fondamentali degli individui e in particolare la possibilità o meno di perseguire la medesima finalità in modo meno intrusivo. La proporzionalità è stata il principale criterio alla base di quasi tutte le decisioni in tema di trattamento dei dati biometrici prese fino a questo momento dalle autorità incaricate della protezione dei dati.[13]

Ai fini di controllo dell'accesso (autenticazione/verifica) il gruppo ritiene che i sistemi biometrici fondati sulle caratteristiche fisiche che non lasciano tracce (ad esempio, la forma della mano, ma non le impronte digitali) o i sistemi biometrici fondati sulle caratteristiche fisiche che lasciano tracce, ma i cui dati non vengono registrati in una memoria appartenente ad una persona diversa dalla persona interessata (in altre parole, i dati non vengono memorizzati nel dispositivo di controllo d'accesso o in una base di dati centrale) comportino un numero minore di rischi per la protezione dei diritti e delle libertà fondamentali

(11) Qualora i dati biometrici, quali ad esempio un modello, vengano registrati in modo tale che non esistano mezzi che possono essere ragionevolmente usati dal responsabile del trattamento o da altri per identificare la persona interessata tali dati non possono essere considerati come dati personali.

(12) L'identificabilità della persona dipende anche dalla disponibilità di altri dati i quali, insieme o separatamente, consentono alla persona in questione di essere appunto identificata. La possibilità di un'identificazione diretta mediante "uno o più elementi specifici caratteristici della sua identità fisica" è citata espressamente nella definizione di dati personali di cui all'articolo 2, lettera a) della direttiva 95/46/CE.

(13) Decisioni, ad esempio, delle autorità olandesi, francesi, tedesche, italiane e greche.

degli individui [14]. Numerose autorità di protezione dei dati hanno sottoscritto tale opinione dichiarando che i dati biometrici andrebbero preferibilmente memorizzati non in una base di dati, bensì su un oggetto accessibile unicamente all'utilizzatore, quale una tessera microchip, un telefono mobile o una carta bancaria [15]. In altri termini, le procedure di autenticazione/verifica che possono essere realizzate senza ricorrere ad una memoria centrale dei dati biometrici non dovrebbero applicare tecniche di identificazione eccessive.

Il gruppo ritiene pertanto che prima di introdurre altri tipi di applicazioni (basate sulla memorizzazione di modelli numerici di impronte digitali nei terminali o in una base di dati centrale) il loro impiego andrebbe sottoposto ad un'attenta valutazione. Qualora tuttavia si adotti questo tipo di sistema, ad esempio nel caso di impianti di alta sicurezza [16], esso potrebbe essere considerato come un trattamento di dati che presenta rischi a termini dell'articolo 20 della direttiva 95/46/CE e potrebbe quindi dover subire un controllo preventivo da parte delle autorità di protezione dei dati conformemente alla legislazione nazionale (vedi il punto 3.5).

La direttiva 95/46/CE vieta l'ulteriore trattamento dei dati qualora questo sia incompatibile con la finalità per la quale i dati erano stati raccolti. Quando, ad esempio, i dati biometrici vengono sottoposti a trattamento a fini di controllo dell'accesso l'uso di tali dati per valutare lo stato emotivo della persona interessata o a fini di sorveglianza sul luogo di lavoro non sarebbe compatibile con la finalità originaria della rilevazione. Occorre prendere tutti i provvedimenti necessari per evitare questo tipo di riutilizzo incompatibile [17]. La direttiva 95/46/CE prevede deroghe al divieto di trattare ulteriormente i dati per finalità ritenute incompatibili, ma solo quando si applicano condizioni specifiche.

In linea generale si riconosce che il rischio che dati biometrici ottenuti da tracce fisiche lasciate da un individuo a sua insaputa (impronte digitali) siano riutilizzati per finalità incompatibili è relativamente inferiore se i dati, invece di essere memorizzati in basi di dati centralizzate, restano con la persona stessa senza essere accessibili a terzi. L'archiviazione centralizzata dei dati biometrici aumenta altresì il rischio che tali dati vengano utilizzati come chiave per collegare basi di dati distinte ed ottenere così profili dettagliati delle abitudini della persona interessata tanto nel settore pubblico quanto in quello privato. La questione della finalità compatibile solleva inoltre il problema della interoperabilità di sistemi diversi che utilizzano la biometria. La normalizzazione necessaria per conseguire l'interoperabilità potrebbe favorire una maggiore interconnessione fra le basi di dati.

L'impiego della biometria solleva inoltre la questione della proporzionalità di ogni categoria di dati trattati alla luce della finalità per la quale vengono trattati. I dati biometrici possono essere utilizzati solo se adeguati, pertinenti e non eccessivi. Questo implica una valutazione accurata della necessità e della proporzionalità dei dati trattati [18].

In Francia, ad esempio, il CNIL ha rifiutato l'uso delle impronte digitali per controllare l'accesso dei bambini ad una mensa scolastica,[19] ma ha accettato per la medesima finalità l'uso della geometria della mano. In Portogallo l'autorità di protezione dei dati ha emesso di recente una decisione sfavorevole in merito all'uso da parte di un'università di un sistema biometrico (impronte digitali) per controllare l'assiduità e la puntualità del personale non docente [20]. In Germania l'autorità incaricata della protezione dei dati ha emesso una decisione favorevole all'introduzione delle caratteristiche biometriche nei documenti di identità allo scopo di evitarne la falsificazione a condizione che, per il confronto con le impronte digitali del proprietario, i dati siano memorizzati nel microchip della carta e non in una base di dati.

Una difficoltà specifica può derivare dal fatto che spesso i dati biometrici contengono più informazioni di quante siano necessarie per l'identificazione o l'autenticazione/verifica. Questo è più probabile nel caso dell'immagine originale (dati grezzi) dato che il modello può e dovrebbe essere costruito tecnicamente in modo tale da rendere impossibile il trattamento di dati non necessari. I dati non necessari dovrebbero essere distrutti quanto prima possibile [21]. Taluni dati biometrici inoltre possono rivelare l'origine razziale o riguardare la salute (vedi nel seguito punto 3.7).

(14) Si può distinguere il caso in cui i dati biometrici vengono trattati a livello centrale da quello in cui i dati biometrici di riferimento vengono registrati su un dispositivo mobile e in cui il processo di abbinamento viene effettuato sulla carta, ma non sul sensore o anche in cui il sensore fa parte del dispositivo mobile.

(15) È necessario tenere conto dei sistemi adottati per risolvere i problemi derivanti dalla perdita, dal furto o dal danneggiamento delle carte e promuovere gli strumenti che non comportano la memorizzazione dei dati biometrici. Per quanto possibile i dati andrebbero rilevati ancora una volta direttamente presso la persona interessata.

(16) Lo stato attuale della tecnologia biometrica è tale che non esistono ancora soluzioni affidabili per una identificazione in tempo reale di una popolazione di qualsiasi dimensioni reale ed è altrettanto improbabile che possano essere disponibili in un prossimo futuro.

(17) Come sottolineato sopra, tale finalità deve essere chiaramente definita.

(18) In determinate circostanze deve inoltre essere possibile ricorrere all'anonimato o all'uso di pseudonimi. È necessario tenere conto dei sistemi adottati per risolvere i problemi derivanti dalla perdita, dal furto o dal danneggiamento delle carte e promuovere gli strumenti che non comportano la memorizzazione dei dati biometrici. Per quanto possibile i dati andrebbero rilevati ancora una volta direttamente presso la persona interessata.

Va infine ricordato che i sistemi biometrici possono essere concepiti in modo tale da poter essere considerati, inter alia, come tecnologie a difesa della vita privata in quanto possono diminuire il trattamento di altri dati personali quali il nome, l'indirizzo, la residenza ecc.

3.3. Rilevazione leale ed informazione della persona interessata

I dati biometrici devono essere trattati e soprattutto rilevati in modo leale [22]. Il responsabile del trattamento deve informare la persona interessata conformemente agli articoli 10 e 11 della direttiva 95/46/CE [23]. Questo prevede in particolare la definizione esatta della finalità e l'identità del responsabile dell'archivio (che spesso coinciderà con la persona che gestisce il sistema biometrico o che applica la tecnica biometrica).

Vanno evitati i sistemi che raccolgono dati biometrici all'insaputa dei soggetti interessati. Alcuni sistemi biometrici quali il riconoscimento a distanza del volto, la rilevazione delle impronte digitali, la registrazione della voce presentano maggiori rischi da questo punto di vista.

3.4. Criteri per la legittimazione del trattamento dei dati

Il trattamento dei dati biometrici deve fondarsi su una delle basi di legittimazione di cui all'articolo 7 della direttiva 95/46/CE. Se il responsabile del trattamento dell'archivio utilizza il consenso come base di legittimazione il gruppo sottolinea che vanno rispettate le condizioni stabilite dall'articolo 2 della direttiva 95/46/CE (qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento).

3.5. Controllo preliminare - notifica

Come indicato sopra, il gruppo appoggia l'uso di sistemi biometrici che non memorizzano le tracce in un terminale di accesso né le archiviano in una base di dati centrale (cfr. punto 3.2). Se tuttavia è stato previsto di utilizzare tali sistemi ed alla luce del rischio di riutilizzo per finalità diverse nonché dei pericoli specifici derivanti dall'accesso non autorizzato il gruppo raccomanda agli Stati membri di prendere in considerazione la possibilità di sottoporli ad un controllo preliminare da parte delle autorità di protezione dei dati conformemente all'articolo 20 della direttiva 95/46/CE, poiché tale tipo di trattamento presenta potenzialmente rischi specifici per i diritti e le libertà delle persone interessate. Se gli Stati membri intendono introdurre il controllo preliminare in relazione al trattamento dei dati biometrici le autorità nazionali incaricate della protezione dei dati vanno debitamente consultate prima dell'introduzione di tali misure.

3.6. Misure di sicurezza

Conformemente all'articolo 17 della direttiva 95/46/CE il responsabile del trattamento deve attuare le misure tecniche ed organizzative appropriate in tema di sicurezza al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete. Le misure di sicurezza vanno adottate quando i dati biometrici sono sottoposti a trattamento (archiviazione, trasmissione, estrazione delle caratteristiche e confronto ecc.) ed in particolare se il responsabile del trattamento trasmette tali dati via Internet. Le misure di sicurezza possono prevedere, ad esempio, la cifratura dei modelli e la protezione delle chiavi di cifratura oltre al controllo ed alla protezione dell'accesso, rendendo così virtualmente impossibile la ricostruzione dei dati originali a partire dai modelli.

In tale contesto occorre tenere conto di alcune nuove tecnologie. Uno sviluppo interessante è offerto dalla possibilità di utilizzare i dati biometrici come chiavi di cifratura. A priori questo comporterebbe un minor rischio per la persona interessata in quanto la decodificazione è possibile solo grazie ad una nuova rilevazione dei dati biometrici presso la persona interessata, il che eviterebbe la creazione di basi di dati contenenti modelli di dati biometrici che potrebbero venire riutilizzati a fini totalmente diversi.

(19) Sembra tuttavia che nel Regno Unito l'autorità di protezione dei dati abbia accettato l'uso delle impronte digitali in circostanze analoghe a condizione che vengano adottate adeguate precauzioni.

(20) L'autorità portoghese di protezione dei dati ha ritenuto che l'applicazione di sistemi del genere fosse sproporzionata ed eccessiva rispetto alla finalità del trattamento dei dati. Il sistema avrebbe memorizzato i dati in un dispositivo biometrico e le persone da controllare sarebbero state circa 140.

(21) A sostegno di questa soppressione si veda anche l'articolo 6, paragrafo 1, lettera e) della direttiva 95/46/CE che stabilisce che i dati personali vanno conservati per un arco di tempo non superiore a quello necessario per il conseguimento delle finalità per le quali sono trattati.

(22) Articolo 6, lettera a) della direttiva 95/46/CE.

(23) Le deroghe all'obbligo di informare le persone interessate di cui agli articoli 10 e 11 della direttiva 95/46/CE dovrebbero basarsi su misure legislative e costituire una misura necessaria per limitare il campo d'applicazione dell'obbligo di informazione allo scopo di salvaguardare gli interessi elencati nell'articolo 13 della direttiva 95/46/CE (pubblica sicurezza, prevenzione, ricerca, accertamento e perseguimento di infrazioni penali ecc.).

Le necessarie misure di sicurezza dovrebbero essere adottate fin dall'inizio del trattamento, soprattutto nel corso della fase di "iscrizione", quando i dati biometrici vengono trasformati in modelli o immagini. Deve essere chiaro che qualsiasi perdita delle caratteristiche di integrità, riservatezza e disponibilità a livello di basi di dati danneggerebbe tutte le future applicazioni basate sulle informazioni contenute in tali basi di dati e comporterebbe altresì danni irreparabili per le persone interessate. Se, ad esempio, le impronte digitali di un individuo autorizzato fossero associate all'identità di un individuo non autorizzato, quest'ultimo potrebbe avere accesso, senza averne diritto, ai servizi a disposizione del proprietario delle impronte digitali. Il risultato sarebbe una sottrazione di identità che, indipendentemente dal fatto di essere scoperta o meno, renderebbe le impronte digitali della persona inattendibili per future applicazioni, limitandone così la libertà.

Gli errori dei sistemi biometrici possono avere pesanti conseguenze per le persone interessate: in particolare il rifiuto erroneo di persone autorizzate e l'accettazione indebita di persone non autorizzate possono dar luogo a gravi problemi a diversi livelli. A priori l'uso di dati biometrici dovrebbe ridurre il rischio di errori del genere, ma esso potrebbe anche creare l'illusione che l'identificazione o l'autenticazione/verifica della persona interessata sia sempre corretta. Può essere difficile o addirittura impossibile per la persona interessata provare il contrario. Un sistema, ad esempio, potrebbe erroneamente identificare una persona come un individuo che non deve essere autorizzato a prendere un aereo o ad entrare nel territorio di un determinato paese: la persona disporrebbe allora di scarsi mezzi per risolvere il problema di fronte a tali prove "irrefutabili" a suo sfavore. Va sottolineato ancora una volta che in casi del genere qualsiasi decisione che produca effetti giuridici su un individuo va presa solo dopo aver riconfermato il risultato del trattamento automatizzato, conformemente all'articolo 15 della direttiva 95/46/CE.

Occorre infine ricordare che l'uso della biometria potrebbe migliorare le procedure di controllo nel caso di accesso ai dati personali relativi a terzi, ad esempio in caso di furto e di uso improprio (procedure di autorizzazione).

3.7. Dati di natura delicata

Alcuni dati biometrici possono essere considerati di natura delicata a termini dell'articolo della direttiva 95/46/CE, segnatamente i dati che rivelano l'origine razziale o etnica o i dati relativi alla salute. Nei sistemi biometrici basati sul riconoscimento del volto, ad esempio, possono essere trattati dati che rivelano l'origine razziale o etnica. In tali circostanze si applicano le speciali garanzie di cui all'articolo 8 oltre ai principi generali di protezione previsti dalla direttiva.

Questo non significa che qualsiasi trattamento di dati biometrici debba includere necessariamente dati di natura delicata. Stabilire se un trattamento comprende dati di natura delicata è una questione di valutazione legata alle caratteristiche biometriche specifiche utilizzate nonché all'applicazione biometrica stessa. È maggiormente probabile che sia il caso quando vengono trattati dati biometrici sotto forma di immagini dato che in linea di massima i dati grezzi non possono essere ricostruiti a partire dal modello.

3.8. Identificatore univoco

I dati biometrici sono unici e la maggior parte di loro genera un modello (o immagine) unico. Se utilizzati su vasta scala, in particolare per una parte importante di popolazione, i dati biometrici possono essere considerati come un mezzo identificativo di portata generale a termini della direttiva 95/46/CE. In tal caso si applicherebbe l'articolo 8, paragrafo 7 della direttiva 95/46/CE e gli Stati membri dovrebbero determinare le condizioni che regolano il trattamento dei dati.

Se i dati biometrici sono destinati ad essere utilizzati come chiave per collegare basi di dati contenenti dati personali [24], problemi particolarmente seri possono presentarsi qualora la persona interessata non possa opporsi al trattamento dei dati biometrici. Questa situazione può verificarsi frequentemente nei rapporti fra cittadini ed autorità pubbliche.

(24) Vedi anche il punto 3.2 sopra sul riutilizzo compatibile.

Da questo punto di vista sarebbe auspicabile che i modelli e le loro rappresentazioni digitali venissero trattati tramite manipolazioni matematiche (cifratura, algoritmi o funzioni di *hashing*), usando diversi parametri per ogni prodotto biometrico utilizzato, al fine di evitare la combinazione di dati personali provenienti da diverse basi di dati grazie al confronto di modelli o di rappresentazioni digitali.

3.9. Codice di condotta e uso della tecnologia a difesa della vita privata

Il gruppo incoraggia l'industria a produrre sistemi biometrici che facilitino l'attuazione delle raccomandazioni contenute nel presente documento di lavoro e se dovessero essere elaborate norme europee o internazionali in questo settore tale lavoro andrebbe svolto in collaborazione con le autorità di protezione dei dati onde promuovere sistemi biometrici progettati in modo da rispettare la protezione dei dati, minimizzare i rischi sociali ed evitare l'uso improprio dei dati biometrici. Il gruppo sottolinea l'importanza in tale contesto delle tecnologie a difesa della vita privata (*Privacy Enhancing Technologies* - PETS) allo scopo di ridurre la rilevazione dei dati ed impedirne il trattamento illecito.

Il gruppo pone inoltre l'accento sull'importanza dei codici di condotta destinati a contribuire alla corretta applicazione dei principi di protezione dei dati tenendo conto delle caratteristiche specifiche dei diversi settori, conformemente all'articolo 27 della direttiva 95/46/CE. I codici comunitari possono essere presentati al gruppo, che determinerà, tra l'altro, se i progetti ad esso presentati sono conformi alle disposizioni nazionali in tema di protezione dei dati adottate in applicazione della direttiva 95/46/CE.

CONCLUSIONI

Il gruppo ritiene che la maggior parte dei dati biometrici comporti il trattamento di dati personali. Al momento di sviluppare sistemi biometrici è necessario pertanto rispettare pienamente i principi di protezione dei dati di cui alla direttiva 95/46/CE considerando la natura specifica della biometria, fra cui la possibilità di rilevare dati biometrici all'insaputa della persona interessata e la quasi certezza del legame con detta persona.

Il rispetto del principio di proporzionalità, che costituisce l'elemento centrale della protezione garantita dalla direttiva 95/46/CE, impone, soprattutto nell'ambito dell'autenticazione/verifica, una netta preferenza per le applicazioni biometriche che non trattano dati ottenuti a partire da tracce lasciate inconsapevolmente dagli individui o che non rientrano in un sistema centrale. Questo permette alla persona interessata di esercitare un migliore controllo sul trattamento dei dati personali che la riguardano.

Il gruppo intende rivedere il presente documento di lavoro alla luce dell'esperienza delle autorità incaricate della protezione dei dati nonché degli sviluppi tecnologici legati alle applicazioni biometriche. Poiché attualmente i dati biometrici vengono introdotti per vari usi in una serie di diversi contesti sarà necessario proseguire il lavoro senza indugio, in particolare nel settore dell'occupazione, dei visti, dell'immigrazione e della sicurezza nell'ambito dei viaggi.

Benché spetti all'industria sviluppare sistemi biometrici conformi ai principi di protezione dei dati, un dialogo costruttivo tra tutte le parti interessate, comprese le autorità di tutela dei dati, basato in particolare su un progetto di codice di condotta, si rivelerebbe assai utile da tutti i punti di vista.

Bruxelles, 13 giugno 2003

Per il gruppo
Il Presidente
Stefano RODOTÀ

81 Parere n. 7/2003 sul riutilizzo delle informazioni del settore pubblico e la tutela dei dati personali - Trovare il giusto equilibrio (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10936/03/EN
WP 83

Parere n. 7/2003 sul riutilizzo delle informazioni del settore pubblico e la tutela dei dati personali - Trovare il giusto equilibrio –

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2003/wp83_it.pdf

Adottato il 12 dicembre 2003

82 Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (*)

ARTICLE 29 Data Protection Working Party

11750/02/EN
WP 89

Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance

Adopted on 11th February 2004

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2004/wp89_en.pdf

83 Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC (*)

ARTICLE 29 Data Protection Working Party

11601/EN
WP 90

Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs/ 2004/wp90_en.pdf

Adopted on 27 February 2004

84 Working Document on Genetic Data (*)

ARTICLE 29 Data Protection Working Party

12178/03/EN
WP 91

Working Document on Genetic Data

Adopted on 17 March 2004

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp91_en.pdf

Trasferimento dei dati verso Paesi terzi

85 Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers (*)

ARTICLE 29 - DATA PROTECTION WORKING PARTY

11639/02/EN
WP 74

Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp74_en.pdf

Adopted on 3 June 2003

86 Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data (*)

ARTICLE 29 Data Protection Working Party

11070/03/EN
WP 78

Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data

Adopted on 13 June 2003

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

has adopted the present Opinion:

INTRODUCTION

In the aftermath of the events of 11 September 2001, the United States adopted a number of laws and regulations requiring airlines flying into their territory to transfer to the US administration personal data relating to passengers and crew members flying to or from this country.

In a previous opinion issued in October 2002 [2], the Working Party reached the conclusion that compliance with the US requirements by the Airlines creates problems in respect of Directive 95/46/EC on data protection [3] and called for a common approach at the European Union level to be found. A specific recommendation was made for the European Commission to enter into negotiations with the United States of America to resolve this matter.

The Working Party has been updated by the Commission on the progress of the talks, which were conducted by the Commission in order to establish the conditions that would allow the Commission to adopt a decision recognising the "adequate protection" on the basis of Article 25 (6) of Directive 95/46/EC and has also gained further insight from the opportunity to discuss the US requirements with high-level officials of the Department of Homeland Security at its meeting of 5 May.

In particular, the Working Party has received from the Commission a document dated 22 May 2003 of "undertakings" issued by the United States Bureau of Customs and Border

Protection and the United States Transportation Security Administration [4]. It understands that these undertakings are the result so far of the on-going negotiation between the

(*) This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC. The secretariat is provided by Directorate E (Services, Intellectual and Industrial Property, Media and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136. Website: www.europa.eu.int/comm/privacy

(1) Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

(2) Opinion 6/2002 of the Working Party on "transmission of Passenger Manifest Information and other data from Airlines to the United States", WP 66 of the Working Party, issued 24 October 2002.

(3) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

(4) Referred to as "undertakings" in this document.

US administration and the Commission and that the Commission is still pressing the US side to make further progress on a number of issues.

The present Opinion is issued with reference to the level of protection ensured by the United States of America after the requested transmission by airlines of personal data concerning their passengers and crewmembers on the basis of their law and international commitments, as described in the undertakings and as laid down in relevant law. The Working Party has been guided by the general criteria set forth to assess adequacy of protection in previous documents [5] and by its previous opinion on the subject of PNR/APIS data required by the US [6].

This opinion is given at a time when US are requesting from EU or directly from Member States numerous flows of personal data (e.g. visa, etc.).

In addition, the Working Party is fully aware that similar flows from airlines have already been requested and/or proposed by several other third countries. This raises the issue of non-discrimination between third States and the necessity for a global evaluation, which might be a model solution for other countries that may receive similar requests. The Working Party underlines the necessity to provide a framework for personal information circulating throughout the world for purposes related to security in connection with air travel.

1. Action against terrorism and the protection of fundamental rights and freedoms

The issue at stake regarding the transfer of data by airlines to US authorities raises public concern and has broad and sensitive implications in political and institutional terms, as well as having an international dimension.

The fight against terrorism is both a necessary and valuable element of democratic societies. Whilst combating terrorism, respect for fundamental rights and freedoms of the individuals including the right to privacy and data protection must be ensured [7].

Such rights are protected in particular by Directive 95/46/EC, Article 8 of the European Convention on Human Rights [8] and are enshrined in Article 7 and 8 of the Charter of Fundamental Rights of the European Union [9]. Moreover data protection is further recognised and expanded in the draft European Constitution discussed by the Convention on the future of Europe.

The legitimate requirements of internal security in the United States of America may not interfere with these fundamental principles. Limitations to fundamental rights and freedoms regarding the processing of personal data in the European Union should only take place if necessary in a democratic society and for the protection of public interests exhaustively listed in those instruments [10].

2. General remarks

The scope of the present opinion concerns the protection of fundamental rights and freedoms regarding the processing of personal data.

This opinion is given by the Working Party with a view to assessing the adequacy of protection provided by the US in connection with envisaged Commission decisions or other legal instruments dealing with this issue. The Working Party reserves the right to supplement the present opinion by a further opinion should this opinion not be adequately taken into account or if substantial changes are made in the course of future negotiations, such as to warrant specific consideration.

The Working Party observes that the circumstances referred to in the "undertakings"require accurate analysis with a view to assessing the adequacy of the level of protection they provide for personal data.

(5) Working Document on "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", WP 12 of the Working Party, issued 24 July 1998.
(6) Opinion 6/2002 on "transmission of Passenger Manifest Information and other data from Airlines to the United States".
(7) See Opinion 10/2001 "on the need for a balanced approach in the fight against terrorism", adopted 14 December 2001.
(8) See also the relevant case-law of the European Court on Human Rights.
(9) The European Commission has committed itself to respect the Charter. See Commission Communication on the Charter of Fundamental Rights of the European Union (COM(2000) 559 final).
(10) See the interests listed in Article 13 of Directive 95/46/EC.

The choice between different mechanisms for the transfer of data (direct access by the US authorities into the databases of the airlines versus proactive disclosure of the data by airlines) raises not only technical problems but also, more importantly, questions of proportionality.

It also means that US authorities have requests that exceed the powers currently granted to European judicial and police authorities and/or authorities in charge of immigration matters or even of intelligence and security services when carrying out similar activities in the European Union.

Furthermore, the issues at stake affect judicial and police co-operation and should be assessed in the light of the safeguards laid down in recent EU-US agreements and draft agreements concerning co-operation, mutual assistance and extradition.

The collection of the data included in the databases of airlines as requested by the US covers a large number of passengers (estimated to amount to at least 10-11 million per annum) which underlines the need for a cautious approach bearing in mind the possibilities this opens up for data mining affecting, in particular, European citizens and entailing the risk of generalised surveillance and controls by a third State. Therefore, the requests coming from the US administration should be addressed with the utmost attention.

3. Transitional Nature of an Adequacy finding

The scope of the data flows is related to recent serious circumstances at the international level. The Working Party recommends that periodical short-term re-evaluations of the situation shall be made to assess if the necessity for such flows remains. Should the international circumstances alter, it would be necessary to review the situation. The Working Party recommends the Commission to include clauses in its decision providing for "sunset" limitation and review the situation after 3 years in any event.

Additionally, if the guarantees provided by the US administration are not correctly implemented, re-evaluation of the situation will be necessary. For this reason, it is essential that a regular report on the actual use of the data in the US be submitted by the Commission on the implementation of the protection in the US. This should allow for the verification of the conditions of processing in the US, to ensure that the underlying assumptions, which justified the Commission's decision, still hold good.

4. The US Regulatory Framework

The Working Party considers that any Commission Decision recognising the provided protection as adequate as well as any other instrument(s) providing a legal framework for the data flows should be based on a clear-cut picture of primary and secondary US legislation regulating purposes, mechanisms and rationale of data utilisation in the US and the entities entitled to access such data.

A full picture of the relevant US regulatory framework, to meet openness and transparency requirements in respect of European citizens, should be included as an annex to any Commission Decision. In addition, provision should be made for a mechanism that ensures that any relevant legislative innovation is communicated to the Commission. It is necessary to avoid other legislation, including legislation passed prior to the Commission Decision (the "undertakings" create a very broad mandate for use and disclosure of the data "as otherwise required by law"), or conflicting interpretations or implementing instruments passed in the US with regard to, in particular, CAPPS II and the collection of biometric data [11], resulting in substantial unilateral changes to the conditions in the US which are the agreed basis for an adequacy finding.

Moreover, it is essential that the decision should not rest only on mere "undertakings" of administrative agencies aimed at supporting certain interpretations at national level (see point 11).

(11) The issue related to collection of biometric data as envisaged starting from October 2004 for issuing entry documents should be assessed separately and only at a later stage.

An evaluation of the adequacy of the level of protection cannot be made with respect to areas of the US administration whose regulatory framework concerning processing of PNR data may not be regarded as stable or adequately clarified in terms of data access rules and entitlement to process such data. The Working Party makes particular reference to the points in the "undertakings" concerning the Transportation Security Administration and its CAPPS II programme. Nor should the evaluation of the adequacy of the level of protection apply to those systems capable of performing mass data processing operations, whose actual functioning and features involve wide-ranging issues yet to be clarified in particular, the Terrorism Information Awareness Initiative.

In this context, the Working Party highlights the need to avoid a situation where TSA or other agencies operating mass data processing systems would receive data indirectly. In case data are to be transmitted to such systems, an additional and specific assessment of the level of protection would be required.

5. Method of transfer and legal concerns

As for the legal basis, which was especially stressed in the European Parliament's Resolution of 13 March 2003, the Working Party is of the opinion that, given the complexity of the legal issues surrounding the lawfulness of communicating the data to third parties and transferring such data to third countries, it may be necessary - having regard to Directive 95/46/EC as a whole - that a positive finding by the EC Commission pursuant to Article 25(6) of the Directive should be accompanied by a formal commitment made by the US Administration upon conclusion of the negotiations.

The legal basis is referred to by the Working Party on the assumption that, considering possible technical differences between various systems, the sole data transfer mechanism whose implementation does not raise major problems is the "push" one - whereby the data are selected and transferred by airline companies to US authorities - rather than the "pull" one - whereby US authorities have direct online access to airline and reservation systems databases.

In addition to ensuring a greater measure of compliance with the principle by which personal data should be adequate, relevant and not excessive (Article 6 of the Directive), entailing fewer data security problems and making certain US access filtering mechanisms superfluous, the "push-system" would make it unnecessary to apply the national measures adopted in transposing the Directive to the US authorities - which would otherwise be necessary if a pull-system were implemented. Indeed, in the latter case, the entire Directive including Article 4, 6 and 13 could be considered as being directly and completely applicable to the US authorities. Moreover, a "push" system is the only solution to ensure that liability rules provided for by Directive 95/46/EC can be correctly applied to European controllers of data.

The Working Party is therefore pleased to note that the US sees no objection to the "push" system. This solution should be substituted for the present mechanism as soon as possible.

6. Purposes

The purposes for which the data will be used should be limited to fighting acts of terrorism without expanding their scope to other unspecified "serious criminal offences". A clear and limited list of serious offences directly related to terrorism should be provided by the US side, without prejudice to the possibility of performing additional specific and individual data exchanges within the framework of judicial and police cooperation.

The need for clarification also relates to the other public bodies entitled to receive the data, as they are currently not identified. The precise identification of such public bodies and their missions or alternatively, for the precisely identifiable authorities such as the judi-

cial bodies, a functional description of them should be detailed. It is in any case necessary to make it absolutely clear that the data might only be communicated to other authorities where necessary in specific cases for the fight against serious offences directly related to terrorism and that subsequent use of such data continues to be limited in the same way.

Clarification is also needed as to the public bodies and the procedures of the said bodies operating the "no fly" and "watch" lists, against which the PNR is processed.

The Working Party questions the justification of disclosure on the ground of the protection of the vital interests of the data subject or of other persons, since this would significantly increase the possibility for additional transmission of the data. Other ways of meeting this requirement would appear to be available.

As for authorities from other third countries, without prejudice to the possibility of performing additional specific and individual data exchanges within the framework of judicial and police co-operation, any direct or indirect onward transfers should be made on a case by case basis and made conditional upon acceptance of specific "undertakings" no less favourable than those provided to the Commission by the US authorities in connection with protecting the transferred data.

7. PROPORTIONALITY

Proportionality should be ensured not only with regard to purposes and the type of offence to be monitored, but also in respect of other issues concerning:

Transferable Personal Data

The Working Party considers that the amount of data to be transferred (12) goes well beyond what could be considered adequate, relevant and not excessive (Article 6 (1) (c) of the Directive). Access to the full set of PNR data is excessive. Data should be limited to the following information: PNR record locator code, date of reservation, date(s) of intended travel, passenger name, other names on PNR, all travel itinerary, identifiers for free tickets, one-way tickets, ticketing field information, ATFQ (Automatic Ticket Fare Quote) data, ticket number, date of ticket issuance, no show history, number of bags, bag tag numbers, go show information, number of bags on each segment, voluntary/involuntary upgrades, historical changes to PNR data with regard to the aforementioned items.

The US primary legislation requiring airlines to provide PNR on request does not make it obligatory for the US authorities concerned to request the data, still less to require that it be transmitted on a systematic basis. Moreover, the US authorities concerned could limit the PNR data elements they request airlines to send. The US authorities are thus interpreting their legal mandate very broadly.

The Working Party finds it necessary to take into account the other sources of information which the US authorities have available to them or try to obtain in their efforts to acquire information on foreigners, such as the data provided via immigration formalities, APIS etc. Additional data exchanges within the framework of judicial and police co-operation channels should also be taken into account in this context.

Transfer of what can be regarded, broadly speaking, as sensitive data - protected by Article 8 of the Directive - should be ruled out. Furthermore, transfer of SSR data - which are actually processed on an optional basis by certain reservation systems - would not appear to be proportionate, in particular in the light of the initiatives undertaken by IATA to update the relevant Manual, which has reached its 20th edition. This also applies to OSI (Other Service-Related Information) data, open or free-text fields (such as the "General Remarks" where data of a delicate nature can appear), and to the information concerning frequent-flyers and "behavioural data".

A clear, exhaustive list of the data transferred on the basis of the Commission Decision should be attached as an annex alongside the table referred to under point 4).

(12) See Annex B of the "undertakings".

Time of Data Transfer

The Working Party is of the opinion that US CBP should receive the data concerning a specific flight no earlier than 48 hours prior to departure. Thereafter, the data should only be updated once.

Data Retention Time

The Working Party is doubtful whether an excessively long data retention time with regard to millions of individuals can be effective for investigative purposes. Personal data should be kept for no longer than is necessary for the purposes for which they were collected. Thus, only retention of the transferred data in line with the announced purpose of controlling the entry to the US territory with a view to the detection of terrorist acts may be accepted. Data should only be retained for a short period that should not exceed some weeks or even months following the entry to the US. A period of 7-8 years cannot be considered as justified. A short period would seem better adjusted to discharging the highly difficult tasks in question, as well as being considerably less expensive. This is obviously without prejudice to the possible need for the processing to continue on a transitional basis in individual cases where there are well-established, specific grounds to examine certain persons more closely, in view of taking measures related to their actual and/or potential involvement in terrorist activities.

8. SUBCONTRACTORS

The Working Party underlines the necessity to provide for the same level of liability of subcontractors and their employees as for US officials, to ensure that the provided guarantees are upheld.

9. GUARANTEES - RIGHTS OF THE DATA SUBJECTS

One of the most basic principles of an adequate data protection regime is for the data subject to be provided with information and to be able to exercise his/her rights, in an easy, quick and effective manner.

Information

Data subjects should be clearly and precisely informed about their rights in particular about the right of access and rectification in addition to the available redress effective mechanisms.

Access

The Working Party underlines the necessity of effectively enforceable safeguards, in respect of the general freedom of information rules (FOIA), in order to ensure that the latter are not used by third parties to access PNR data held by the US administration. In this context, it is important to prevent possible discrimination between citizens and to ensure that the data subjects' right of access to their own data is enforced generally and unambiguously.

The "undertakings" provided by the US authorities create some concerns regarding the way exemptions may be opposed to the data subject in order to allow the administration to refuse access to him or her.

The Working Party is of the opinion that the data subjects' right of access should extend to any new data which may be generated as a result of the processing to which the data transmitted from Europe are submitted (risk profile, exclusionary lists ...).

Rectification

Since the scope of the US Privacy Act is limited to US residents, the Working Party underlines the importance to provide the data subject with an efficient mechanism to have his/her data corrected.

10. Enforcement and Dispute Settlement

Timely support and help for the individual and independent redress and supervision

The ensured protection should provide rapid support and help to individual data subjects in exercising their rights and provide in their favour independent and appropriate redress.

The Working Party sees major flaws concerning enforcement and independent third-party supervision of the application of the undertakings. The available mechanisms at this moment are limited to audits and the internal Chief Privacy Officer. Moreover, it is not clear how the "undertakings" may produce binding legal effects and be the source of obligations that can give rise to claims before a court (see below point 11).

Moreover, the Working Party notes the need to be provided with more information on the supervisory independent body that has control on the "no fly", "watch" lists and on the logic of the profile mechanism.

Audits

A guarantee of a good level of compliance with the data protection safeguards should exist. In this context, the Working Party underlines the importance of the public availability of certain audits results. The public reports should contain the number and volume of PNR requests from other US public bodies and the number, volume and the motivating reason for those requests for which authorisation has been granted by the first recipients.

11. Level of commitments

The Working Party underlines the necessity to have commitments from the US side that are officially published at least at the level of the Federal Register and fully binding on the US side. In particular, there should be no ambiguity about the capability to create rights in favour of third parties. This raises the point of which authority precisely will commit the US side. Directive 95/46/EC indeed provides that a decision recognising as adequate the protection ensured by a third country to transferred data must be based on its domestic law and/or the international commitments into which it has entered.

Conclusion

This opinion sets out the concerns of the Working Party from a data protection perspective in assessing the level of protection ensured in the US with a view of a possible Commission Decision. The overall objective is to establish as quickly as possible a clear legal framework for any transfer of airline data to the US in a way which is compatible with data protection principles. While recognising that ultimately political judgements will be needed, the Working Party urges the Commission to take its views fully into account in its negotiations with the US authorities.

The Working Party is aware that a more global approach concerning the conditions of the use of air transport data for security purposes in a multilateral context might be necessary.

Done at Brussels, on 13 June 2003

For the Working Party
The Chairman
Stefano RODOTÀ

87 Parere 5/2003 sul livello di protezione dei dati personali a Guernsey (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10595/03/IT
WP 79

Parere 5/2003 sul livello di protezione dei dati personali a Guernsey

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2003/wp79_it.pdf

Adottato il 13 giugno 2003

88 Parere n. 6/2003 sul livello di protezione dei dati personali nell'Isola di Man (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11580/03/IT
WP 82

Parere n. 6/2003 sul livello di protezione dei dati personali nell'Isola di Man

Adottato il 21.11.2003

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs/2003 /wp82_it.pdf

89 Parere 8/2003 sul progetto di clausole contrattuali tipo presentato da un gruppo di organizzazioni commerciali ("il contratto modello alternativo") (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11754/03/IT
GL 84

Parere 8/2003 sul progetto di clausole contrattuali tipo presentato da un gruppo di organizzazioni commerciali ("il contratto modello alternativo")

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp84_it.pdf

Approvato il 17 dicembre 2003

90 Parere 1/2004 sul livello di protezione garantito in Australia per la trasmissione dei dati delle registrazioni dei nomi dei passeggeri da parte delle compagnie aeree (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10031/03/IT
WP 85

Parere 1/2004 sul livello di protezione garantito in Australia per la trasmissione dei dati delle registrazioni dei nomi dei passeggeri da parte delle compagnie aeree

Adottato il 16 gennaio 2004

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp85_it.pdf

91 Parere 2/2004 sul livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche Passeggeri (PNR - Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (Bureau of Customs and Border Protection - US CBP) (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10019/04/IT
WP 87

(*) Il gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, Diritti d'autore, Proprietà Industriale e Protezione dei Dati) della Commissione europea, Direzione generale mercato interno, B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136. Website: www.europa.eu.int/comm/privacy

(1) GU n. L 281 del 23/11/1995, pag. 31, disponibile al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

IL GRUPPO DI LAVORO SULLA PROTEZIONE DELLE PERSONE PER QUANTO RIGUARDA IL TRATTAMENTO DEI DATI A CARATTERE PERSONALE

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [1],

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, di tale direttiva,

visto il regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente parere:

INTRODUZIONE

Sulla scia degli eventi dell'11 settembre 2001, gli Stati Uniti hanno adottato un insieme di leggi e di regolamenti che impongono alle compagnie aeree che gestiscono voli destinati al loro territorio di trasferire alle autorità americane dati personali sui passeggeri e sui membri dell'equipaggio dei voli destinati a tale paese o da esso provenienti. In particolare, le autorità hanno imposto alle compagnie aeree l'obbligo di fornire all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti (CBP) un accesso elettronico ai dati relativi ai passeggeri che figurano nelle pratiche "PNR" per i voli a destinazione degli Stati Uniti, provenienti da tale Paese o che lo attraversano. Le compagnie aeree che respingono tali domande sono suscettibili di essere sanzionate con pesanti ammende e anche con la perdita dei loro diritti di atterraggio, mentre i loro passeggeri subirebbero ritardi al loro arrivo negli Stati Uniti.

Il gruppo di lavoro ha emesso un primo parere nell'ottobre 2002 e un secondo il 13 giugno 2003. Quest'ultimo prendeva in considerazione la dichiarazione d'intenti degli Stati Uniti del 22 maggio 2003 ("Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration") che riflette l'ultimo stadio del dialogo relativo agli impegni della parte americana sulle condizioni di trattamento dei dati passeggeri PNR.

Nel suo parere del 13 giugno il gruppo di lavoro ha richiamato l'attenzione su numerose questioni di protezione dei dati che risultano dal trasferimento dei dati passeggeri PNR alle autorità americane. I principali punti in sospeso riguardano la finalità dei trasferimenti, il principio di proporzionalità per quanto riguarda i dati personali da trasferire nonché il momento dei trasferimenti e la durata di conservazione dei dati, il trattamento dei dati sensibili, l'importanza di adottare un metodo di trasferimento "push", lo stretto controllo degli ulteriori trasferimenti verso altre amministrazioni o autorità estere, le garanzie e i diritti delle persone interessate, il meccanismo d'applicazione e di risoluzione delle controversie, nonché il livello degli impegni.

Di recente, il gruppo di lavoro ha ricevuto la comunicazione della Commissione al Consiglio e al Parlamento intitolata: "Il trasferimento dei dati delle pratiche passeggeri (Passenger Name Record - PNR): la necessità di un approccio globale" [2] e una versione attualizzata della dichiarazione d'intenti americana datata 12 gennaio 2004 (Allegato I).

Conformemente al suo parere 4/2003, il gruppo di lavoro ritiene che sia opportuno emettere un nuovo parere alla luce degli ultimi sviluppi concernenti il trasferimento dei dati passeggeri PNR, tenendo conto in particolare dei risultati dei negoziati tra la Commissione europea e le autorità americane.

1. Azione contro il terrorismo e protezione delle libertà e dei diritti fondamentali

Come è già stato indicato nei pareri 6/2002 e 4/2003, i trasferimenti di dati ad autorità americane suscitano preoccupazioni nella pubblica opinione, hanno ripercussioni profonde e sensibili a livello politico e istituzionale e rivestono una dimensione internazionale.

La lotta contro il terrorismo è un elemento al tempo stesso valido e necessario nelle società democratiche. In questa lotta contro il terrorismo, è opportuno proteggere le libertà individuali e i diritti fondamentali, compresi il rispetto della vita privata e la protezione dei dati.

Questi diritti sono in particolare protetti dalla direttiva 95/46/CE, nonché dall'articolo 8 della Convenzione europea dei diritti dell'uomo, e costituiscono il nucleo fondamentale dei diritti tutelati dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. La protezione dei dati è inoltre riconosciuta e rafforzata dal progetto di Costituzione europea discusso dalla Convenzione sul futuro dell'Europa.

Pertanto le libertà e i diritti fondamentali relativi ai principi che disciplinano la protezione dei dati a carattere personale dell'Unione europea devono essere limitati solo nei casi in cui ciò risulta necessario all'interno di una società democratica o per le esigenze di tutela degli interessi pubblici così, come sono definiti in modo esaustivo negli strumenti sopra menzionati.

Tenuto conto del volume e della sensibilità dei dati in questione, nonché del numero di individui coinvolti (dai 10 agli 11 milioni di passeggeri l'anno), la richiesta di comunicare a un'autorità pubblica i dati personali raccolti a fini commerciali e che figurano nelle basi di dati delle compagnie aeree che propongono voli a destinazione degli Stati Uniti o che transitano per gli Stati Uniti, nonché nei sistemi di prenotazione correlati, fornendo a tale autorità un accesso a questi sistemi, è senza precedenti nella storia dei rapporti tra gli Stati Uniti e l'Europa e costituisce un'eccezione al principio fondamentale di specificazione della finalità in materia di protezione dei dati. È quindi opportuno dar prova di prudenza, tenendo conto anche delle possibilità di estrapolazione dei dati cui tale evoluzione apre la strada, in particolare per i residenti europei, nonché del rischio che ne deriva di sorveglianza generalizzata e di controllo da parte di un paese terzo.

Inoltre, analoghi flussi di dati delle compagnie aeree sono già stati richiesti e/o proposti da molti altri paesi terzi. Ciò solleva la questione dell'uguaglianza di trattamento dei paesi terzi e pone in evidenza la necessità di adottare un approccio globale per l'utilizzazione dei dati dei trasporti aerei ai fini di sicurezza in un contesto multilaterale.

(2) COM(2003)826 def.

Non è certo che la lotta contro il terrorismo e il mantenimento della sicurezza interna saranno più efficaci mettendo parzialmente tra parentesi i principi di proporzionalità e di minimizzazione dei dati, mentre il rispetto di questi principi costituisce una garanzia essenziale per la protezione dei diritti dei cittadini ed è meglio adeguato ai bisogni dello sviluppo commerciale.

A tale riguardo, il gruppo di lavoro rileva che la questione del trasferimento dei dati passeggeri PNR si pone anche per altri paesi, e ciò richiede un approccio globale uniforme su scala mondiale, vale a dire un'armonizzazione delle soluzioni previste per i vari paesi.

Il gruppo di lavoro osserva inoltre che l'esperienza recente acquisita da taluni paesi, e in particolare dall'Australia, mostra che è possibile dare una risposta proporzionata e ragionevole alle legittime esigenze di sicurezza interna e di lotta contro il terrorismo utilizzando sistemi che sono compatibili con i principi fondamentali di rispetto della vita privata e della protezione dei dati a carattere personale.

2. Atti legislativi da adottare

Il gruppo di lavoro deduce dalla comunicazione che, secondo la Commissione, la definizione di una base giuridica di qualità per il trasferimento di dati PNR alle autorità americane debba passare attraverso una decisione della Commissione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE in combinazione con un accordo internazionale che autorizza le compagnie aeree a trattare le esigenze americane come esigenze giuridiche nell'ambito dell'Unione europea e vincolando gli Stati Uniti alla reciprocità e al rispetto dei diritti dei residenti dell'UE ("due process"). A tal fine, la Commissione prevede di stipulare un "accordo bilaterale leggero" con gli Stati Uniti.

Tenuto conto della mancanza di documenti pertinenti e considerando le competenze degli Stati membri per quanto riguarda l'attuazione degli articoli 6 e 7 della direttiva 95/46/CE, il gruppo di lavoro non è in grado di adottare un parere sul contenuto nonché sulla possibile base giuridica e sul valore di un simile accordo.

Il gruppo di lavoro intende sottolineare tuttavia che le decisioni della Commissione adottate sulla base dell'articolo 25, paragrafo 6 della direttiva, fanno riferimento per loro stessa natura alla protezione adeguata dei dati personali una volta che essi siano stati trasferiti a un paese terzo e che, sino ad oggi, hanno riguardato i trasferimenti a organismi del settore privato situati in paesi terzi. E' la prima volta che un trasferimento viene operato sulla base di un obbligo giuridico posto da un paese terzo che esige dagli operatori dell'UE di trasferire dati ad un'autorità pubblica di tale paese terzo, in modo non conforme alle disposizioni della direttiva.

Al fine di garantire per tali trasferimenti una corretta base giuridica, è prevista una formula composta da una decisione sul carattere adeguato della protezione e da un accordo internazionale; tale formula dovrà avere una serie di effetti giuridici. Il gruppo di lavoro ritiene che, nella misura in cui l'accordo internazionale consente di legittimare una limitazione al diritto della vita privata o una restrizione al principio di limitazione ad una determinata finalità prevista all'articolo 6 della direttiva, tale accordo dovrà in ogni caso rispettare i limiti posti dall'articolo 8 della Convenzione europea dei diritti dell'uomo e dall'articolo 13 della direttiva.

3. Campo di applicazione del principio di protezione adeguata e di un eventuale accordo: il sistema CAPPS II e la TSA(transportation security administration)

Il gruppo di lavoro ha esplicitamente escluso il programma CAPPS II e qualunque altro sistema in grado di realizzare operazioni di trattamento di dati su grande scala dal campo di applicazione del suo parere 4/2003.

Tali sistemi presentano infatti differenze qualitative rispetto al semplice trasferimento di dati passeggeri PNR e sollevano questioni gravi che devono essere chiarite e trattate specifi-

camente dal gruppo di lavoro, tenuto conto degli effetti generalizzati che avrebbero sui diritti fondamentali delle persone interessate.

Il sistema CAPPS II solleva in particolare un certo numero di questioni specifiche che richiedono non solo una particolare attenzione da parte del gruppo di lavoro, ma anche clausole di salvaguardia diverse e più efficaci. Qualunque decisione futura sul sistema CAPSS II dovrà essere analizzata specificamente dal gruppo di lavoro e non dovrà derivare da un'estensione automatica del campo di applicazione della prima decisione della Commissione sul livello di protezione adeguato dei trasferimenti di dati passeggeri PNR verso gli Stati Uniti.

Di conseguenza, considerando che il gruppo di lavoro non è stato informato né consultato a proposito del quadro giuridico definitivo del sistema CAPSS II, qualunque utilizzazione di dati a carattere personale da parte della TSA nel quadro del sistema CAPSS II così come è proposta e qualunque prova relativa dovranno essere esclusi ora e in futuro dal campo di applicazione della decisione della Commissione. In altri termini, le riflessioni contenute nel presente parere si basano sul presupposto secondo il quale la decisione della Commissione non sarà estesa in futuro al sistema CAPPS II, né direttamente, né indirettamente attraverso un riferimento alla legislazione interna degli Stati Uniti. In caso contrario, sarebbe opportuno esprimere sin d'ora osservazioni molto più critiche.

Di conseguenza, il gruppo di lavoro raccomanda alla Commissione di precisare, attraverso una clausola specifica nella decisione, che le autorità americane devono astenersi dall'utilizzare i dati passeggeri PNR trasmessi dall'UE non solo per mettere in opera il sistema CAPPS II, ma anche per effettuare le relative prove.

Il gruppo di lavoro ritiene che una simile clausola dovrà inoltre applicarsi a qualunque altra utilizzazione dei dati sui passeggeri europei trasmessi dalle compagnie aeree nel quadro di altri programmi quali "Terrorism Information Awareness" e "US VISIT" o i programmi di trattamento di dati biometrici.

4. Livello degli impegni

Il gruppo di lavoro ricorda che qualunque decisione della Commissione non dovrà basarsi su semplici "impegni" da parte delle autorità amministrative, ma su impegni che siano ufficialmente pubblicati almeno a livello del Registro federale e abbiano forza esecutiva negli Stati Uniti. Più in particolare, non dovrà esserci dubbio in merito all'effetto creativo di diritti a vantaggio di terzi.

Su tale punto, è chiaro che gli impegni presi dagli Stati Uniti non avranno forza esecutiva dal lato degli Stati Uniti. Inoltre, il nuovo paragrafo 47 aggiunto alla fine della dichiarazione d'intenti chiarisce in modo esplicito la forza esecutiva degli impegni presi dagli Stati Uniti, disponendo che "essi non creano diritti o vantaggi a beneficio di persone o parti, private o pubbliche".

Il gruppo di lavoro sottolinea pertanto che il livello degli impegni da parte degli Stati Uniti non può essere considerato come conforme alle esigenze poste nel suo parere 4/2003 e considera che tale questione sia una condizione essenziale che dovrà essere affrontata prima che possa essere formalizzato un accordo.

5. Aspetti specifici

Tenuto conto del contesto globale sopra descritto, le domande americane, così come esse risultano dalla dichiarazione d'intenti (versione aggiornata del 12 gennaio 2004) devono essere valutate alla luce dei pareri emessi in questo settore dal gruppo di lavoro, in particolare il parere 4/2003 del 13 giugno 2003.

A. NATURA TRANSITORIA DEL LIVELLO DI PROTEZIONE ADEGUATO

Un durata di tre anni e mezzo è stata suggerita per l'insieme delle misure, compresi la dichiarazione d'intenti, la constatazione di protezione adeguata e l'accordo internazionale corrispondente.

Il gruppo di lavoro accoglie con favore l'introduzione di una "clausola di caducità" dell'accordo e spera che il periodo di tre anni e mezzo proposto nel suo parere 4/2003 sarà preso in considerazione.

B. LIMITAZIONE AD UNA FINALITÀ SPECIFICA

Il DHS (Ministero americano della sicurezza interna) utilizzerà i dati passeggeri PNR per le esigenze del CBP, al fine di prevenire e combattere:

1) Il terrorismo e i crimini connessi
2) Altri reati gravi, compreso il crimine organizzato, di natura transnazionale;
3) la fuga dall'arresto o custodia per i crimini sopra descritti.

Il gruppo di lavoro rileva che la descrizione delle finalità dell'uso dei dati PNR è più rigorosa e precisa di quanto non fosse in precedenza. Tuttavia, la categoria 2 rimane vaga, in particolare per quanto riguarda il campo di applicazione degli "altri reati gravi" indicati nella dichiarazione americana. Inoltre, la finalità delle misure rimane molto più ampia della lotta contro gli atti di terrorismo, sulla quale il gruppo di lavoro riteneva che fosse opportuno mantenere l'accento (parere 4/2003).

C. ELENCO DEI DATI DA TRASFERIRE

Il CBP propone ora che i trasferimenti di dati passeggeri PNR comprenda un elenco di 34 elementi informativi, e ciò è stato approvato dalla Commissione. Questo elenco risulta dall'esclusione di 4 ambiti di dati (identificazione dei biglietti gratuiti, numero dei bagagli, numero di bagagli per ciascun segmento, passaggi alla classe superiore volontari/involontari) dalla lista dei 38 elementi PNR che figura all'Allegato B della dichiarazione d'intenti del 22 maggio 2003 [3].

Il gruppo di lavoro osserva che i progressi realizzati per quanto riguarda l'elenco dei dati da trasmettere sono molto limitati. In effetti, l'elenco americano modificato contiene sempre i 20 elementi di cui il gruppo di lavoro riteneva il trasferimento sproporzionato e problematico nel suo parere 4/2003.

È opportuno inoltre rilevare che le autorità americane hanno fatto passare il numero di elementi da trasmettere da 38 a 34 solo sopprimendo quattro elementi che erano stati accettati dal gruppo di lavoro nel suo parere del 13 giugno. Per quanto riguarda i 20 elementi che continuano ad essere richiesti dalle autorità americane anche se non sono stati accettati dal gruppo di lavoro, non è stata fornita alcuna indicazione o spiegazione per giustificare la necessità del loro trattamento o il loro carattere proporzionale e non eccessivo nella lotta contro il terrorismo in una società democratica.

Il gruppo di lavoro ricorda l'elenco dei 19 elementi accettati nel suo parere del 13 giugno 2003, e il fatto che qualunque aggiunta a questo elenco è soggetta ad una rigorosa verifica dei principi di proporzionalità e di minimizzazione dei dati.

D. DATI SENSIBILI

Il dialogo ha in particolare consentito di fare in modo che alcuni dati PNR non saranno utilizzati, ma soppressi dalle autorità americane, tenendo presente che a tale riguardo l'articolo 8, paragrafo 1, della direttiva fa riferimento ai dati a carattere personale che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento dei dati relativi alla salute e alla vita sessuale.

(3) Anche se l'Allegato B della dichiarazione d'intenti del 22 maggio 2003 enumera 39 elementi, solo 38 possono realmente figurare in un PNR, poiché il vecchio settore OSI ("other service information") dovrebbe essere utilizzato solo se un codice SSR ("special service request") non è disponibile, conformemente al servizio di prenotazione IATA-Manuale, 20a edizione, effettivo 1° giugno 2003 - 31 maggio 2003, punto 10.3, pag. 127.

L'elenco dei codici e degli ambiti dei dati da sopprimere non è ancora disponibile. Il gruppo di lavoro tiene tuttavia a sottolineare che se alcuni codici devono chiaramente essere soppressi (ad esempio quelli che riguardano le preferenze alimentari, lo stato di salute o le condizioni religiose, quali "Tariffa pellegrino", "missionario" o "clero", altri codici richiedono un esame approfondito, in particolare gli ambiti "liberi" del tipo "Notazioni generali" che sono suscettibili di contenere dati sensibili. Nella loro dichiarazione d'intenti (versione 12 gennaio) le autorità americane fanno sapere che questi elementi sarebbero soppressi attraverso l'utilizzazione di un elenco di parole che fanno scattare la procedura di soppressione. Un simile approccio non garantisce l'eliminazione dell'insieme dei dati sensibili che figurano in questi ambiti. Pertanto l' unica soluzione sicura consisterebbe nell'escludere questi campi dal trasferimento, conformemente al parere 4/2003.

A tale proposito, il gruppo di lavoro ricorda il suo parere del 13 giugno 2003 secondo il quale il trasferimento di dati sensibili deve essere escluso. Non si può quindi prevedere di procedere a soppressioni solo dopo aver trasmesso i dati sensibili alle autorità americane. Il gruppo di lavoro invita la Commissione a trovare soluzioni tecniche adeguate (come ad esempio filtri) al fine di evitare qualunque trasmissione di dati sensibili alle autorità americane.

E. Utilizzazione dei dati derivati dalla pratiche passeggeri PNR

In una formula aggiunta alla dichiarazione, le autorità americane descrivono le limitazioni che esistono per quanto riguarda il loro accesso ai dati "derivati" da pratiche PNR i quali sono suscettibili di rivelare alcuni aspetti della vita di un passeggero e rischiano di interferire gravemente con il diritto della persona interessata a una vita privata e familiare, conformemente all'articolo 8 della Convenzione europea dei diritti dell'uomo. La nuova formulazione è la seguente:

"Ulteriori informazioni personali ricercate come risultato diretto dei dati del PNR possono essere ottenute da fonti estranee al governo solo mediante canali legali, e solo a fini legittimi di contrasto del terrorismo o di applicazione delle leggi. Ad esempio, se in un PNR figura un numero di carta di credito, possono essere ricercate informazioni sulle transazioni legate a quel conto mediante procedimenti legali come un ordine di comparizione emesso da un gran giurì o da un giudice, o come altrimenti previsto dalla legge. Inoltre, l'accesso ai dati relativi agli indirizzi di posta elettronica ottenuti da un PNR deve rispettare le norme di legge degli USA per gli ordini di comparizione, i provvedimenti dei giudici, i mandati d'arresto e gli altri procedimenti autorizzati dalla legge, a seconda del tipo delle informazioni ricercate."

Questi chiarimenti sono benvenuti. Tuttavia, non dissipano completamente le preoccupazioni del gruppo di lavoro. In particolare, le finalità per le quali i dati passeggeri PNR possono essere utilizzati non devono comprendere altri imperativi di "applicazione delle leggi" non specificati. Inoltre, l'accesso alle messaggerie elettroniche e ad altre informazioni personali derivate da una pratica PNR deve iscriversi unicamente nel quadro delle esigenze procedurali previste negli strumenti internazionali di cooperazione giudiziaria e di polizia. Inoltre, deve essere chiaro che in caso di abuso un individuo può presentare un ricorso dinanzi a un'autorità indipendente.

F. Periodo di conservazione dei dati

Il CBP conserverà i dati passeggeri PNR ai fini convenuti dal CBP per tre anni e mezzo. I dati che sono consultati manualmente durante questo periodo saranno conservati in uno schedario di dati cancellati per altri 8 anni.

Il gruppo di lavoro rileva che si tratta di un miglioramento rispetto ai 7 anni inizialmente proposti nella dichiarazione del 22 maggio. Una durata di tre anni e mezzo rimane tuttavia molto più lunga del periodo di "alcune settimane o alcuni mesi" auspicato dal gruppo di lavoro nel suo parere 4/2003. Il gruppo di lavoro dubita che l'immagazzinamento generalizzato dell'insieme dei dati PNR per periodi così lunghi possa essere giudicato "proporzionale e necessario in una società democratica".

Inoltre, la conservazione dei dati per altri otto anni, prevista per il semplice caso in cui tali dati siano stati consultati, è sproporzionata nella misura in cui non vi è un collegamento con un'inchiesta concreta o un mandato concernenti la persona i cui dati sono consultati; ciò rende quindi possibile superare de facto il limite di tre anni e mezzo.

Da notare al riguardo che è possibile prevedere soluzioni che sono più rispettose dei principi di protezione dei dati, ma che restano efficaci nella lotta contro la criminalità. L'Australia, ad esempio, ha elaborato un sistema nel quadro del quale le dogane di questo paese conservano o immagazzinano dati su un passeggero solo se quest'ultimo ha commesso un atto illegale o se i dati sono necessari per le esigenze di un'inchiesta riguardante un presunto delitto.

G. Metodo di trasferimento

Per quanto riguarda il metodo di trasferimento, il gruppo di lavoro ricorda il suo parere 4/2003 nel quale considera che il solo meccanismo di trasferimento la cui attuazione non crea problemi gravi è quello del "push" (tramite il quale i dati sono selezionati e trasferiti dalle compagnie aeree alle amministrazioni americane) piuttosto che quello del "pull" (tramite il quale le autorità americane hanno un accesso in linea diretto alle basi di dati delle compagnie aeree ed ai sistemi di prenotazione).

Anche se le autorità americane non pongono più obiezioni da alcuni mesi sul sistema "push", il gruppo di lavoro è estremamente preoccupato per il fatto che i meccanismi tecnici che consentono di applicare un tale sistema gestito direttamente dalle compagnie aeree europee non sono ancora in funzione. Il gruppo di lavoro ritiene che debbano essere attuate misure concrete entro l'aprile del 2004 e incoraggia vivamente la Commissione ad adottare immediatamente le misure necessarie per raggiungere questo obiettivo. Inoltre, il gruppo di lavoro sottolinea che il livello di protezione assicurato dagli Stati Uniti non potrà essere considerato come adeguato senza l'instaurazione di un sistema "push".

H. Momento del trasferimento

Nel suo parere 4/2003, il gruppo di lavoro ritiene che i servizi dell'US CBP dovrebbero ricevere i dati relativi a un volo specifico non prima di 48 ore prima del decollo. Dopo di ciò, i dati dovrebbero essere aggiornati una sola volta.

Su questo punto, l'ultima versione della dichiarazione è rigorosamente fedele alla versione precedente, che prevede un trasferimento dei dati 72 ore prima del decollo e un massimo di tre aggiornamenti.

Il gruppo di lavoro deplora che non sia stato ottenuto alcun miglioramento su questo punto durante i negoziati.

I. Trasferimento di dati passeggeri PNR verso altre autorità amministrative o estere

Nel suo parere 4/2003, il gruppo di lavoro chiede che gli altri organismi pubblici abilitati a ricevere i dati siano identificati con precisione, aggiungendo che qualunque ulteriore trasferimento diretto o indiretto dovrà essere subordinato all'accettazione di impegni specifici almeno altrettanto favorevoli di quelli che sono forniti alla Commissione dalle autorità americane per quanto riguarda la protezione dei dati trasferiti. Inoltre, il numero di autorità suscettibili di ricevere i dati dovrà essere ristretto.

Il gruppo di lavoro nota che non è stato ancora redatto alcun elenco globale delle autorità cui i dati sono suscettibili di essere trasferibili. Inoltre, il gruppo di lavoro rimane preoccupato dalle disposizioni che consentono al CBP di divulgare dati conformemente alle "altre esigenze previste dalla legge", in particolare se queste disposizioni sono previste alla luce delle leggi e dei protocolli di accordo che obbligano gli Stati Uniti a condividere i loro dati con altri paesi.

In particolare, il meccanismo di cui ai punti 29 e 35 della dichiarazione differisce sensibilmente dal principio di limitazione ad una specifica finalità così come affermato dal gruppo di lavoro (vale a dire la lotta contro il terrorismo e i reati connessi con il terrorismo) e anche dalle più ampie finalità così come definite ai punti 1 e 3 della dichiarazione.

J. GARANZIE – DIRITTI DELLE PERSONE INTERESSATE

1) INFORMAZIONI CHIARE ALLE PERSONE INTERESSATE

Ai termini del parere 4/2003, e conformemente all'articolo 10 della direttiva, un'informazione chiara e precisa dovrebbe essere fornita alle persone interessate sull'identità del responsabile del trattamento, sulla finalità del trattamento e su qualunque altra informazione, come l'esistenza di un diritto di accesso e di rettifica e le vie di ricorso effettive che sono aperte.

Il gruppo di lavoro rileva che il CBP fornirà informazioni ai viaggiatori. A tal fine, il gruppo di lavoro osserva che sarà possibile redigere rapidamente una nota informativa tipo una volta che il quadro giuridico sarà stato fissato in modo più preciso, tenuto conto anche del progetto sottoposto al gruppo di lavoro. È tuttavia opportuno considerare che una nota informativa globale può servire quale complemento, ma in nessun caso può considerarsi un sostituto ai requisiti giuridici che devono essere rispettati affinché i trasferimenti di dati passeggeri PNR verso gli Stati Uniti siano legittimi.

2) ACCESSO

Nel suo parere del 4/2003, il gruppo di lavoro sottolinea la necessità di garanzie realmente applicabili con riferimento alle regole generali poste dalla Legge sulla libertà d'informazione (FOIA), al fine di garantire che queste ultime non saranno utilizzate da terzi per accedere a dati passeggeri PNR in possesso dell'amministrazione americana e che il diritto di accesso delle persone interessate ai propri dati sarà rispettato in modo generale e non ambiguo.

Per quanto riguarda l'accesso dei terzi, il gruppo di lavoro accoglie favorevolmente i chiarimenti forniti dal CBP nel documento "Exemptions Under the Freedom of Information Act (FOIA) Applicable to Passenger Name Record (PNR) Data".

Tuttavia, per quanto riguarda l'accesso dei passeggeri ai propri dati, il gruppo di lavoro continua ad avere timori sul modo in cui talune esenzioni potrebbero essere utilizzate per opporsi ai diritti di una persona interessata, consentendo in tal modo all'amministrazione di rifiutarle l'accesso ai suoi dati.

Inoltre, il gruppo di lavoro sottolinea che il diritto di accesso delle persone interessate non è stato esplicitamente esteso, come era auspicato nel parere 4/2003, ai nuovi dati suscettibili di essere generati dal trattamento dei dati trasmessi dall'Europa (profilo di rischio, elenchi d'esclusione, ecc.).

3) RETTIFICA

Nel suo parere 4/2003, il gruppo di lavoro insiste sull'importanza di fornire alle persone interessate un meccanismo efficace per ottenere la rettifica dei loro dati. Il gruppo di lavoro rileva che il campo d'applicazione della legge americana sulla vita privata ("US Privacy Act") è limitato ai residenti americani. Pertanto la questione della non discriminazione dei residenti europei rispetto ai cittadini americani non è sempre risolta ed è opportuno determinare se il meccanismo di rettifica esposto nella dichiarazione possa essere considerato uno strumento efficace e giuridicamente vincolante per quanto riguarda il diritto di rettifica che il FOIA concede ai cittadini americani e ai residenti esteri.

4) RICORSI

Il "DHS Privacy Office" (Ufficio responsabile per la protezione della vita privata del Ministero della sicurezza interna) ha concordato di esaminare rapidamente i ricorsi che gli saranno presentati dalle autorità incaricate della protezione dei dati degli Stati membri per conto di un residente dell'Unione europea il quale ritenga che il DHS, compreso il suo "Privacy Office", non ha trattato il suo ricorso in modo soddisfacente.

Il gruppo di lavoro accoglie con favore questa evoluzione. È importante che una persona possa ottenere un aiuto qualificato in alcuni casi; tuttavia, la questione relativa all'indipendenza reale del "Chief Privacy Officer" (direttore responsabile per la privacy del DHS) così come è stata sollevata nel parere 4/2003 del gruppo, non è stata ancora risolta. I membri del gruppo di lavoro ritengono che le disposizioni interne che sono state adottate per quanto riguarda le funzioni del "panel" cui si fa riferimento nell'FAQ 5 dell'Accordo sulla sfera di sicurezza possano essere utili in questo contesto. Essi studieranno le correzioni che sarà eventualmente opportuno effettuare al fine di un'applicazione nel contesto dei PNR.

Il gruppo di lavoro deplora d'altro canto che i passeggeri non abbiano la garanzia di poter ricorrere in tutti casi a un meccanismo di ricorso veramente indipendente in caso di controversie con il DHS. Inoltre, sembra ora che la dichiarazione non avrà effetti giuridici vincolanti né genererà obblighi il cui rispetto possa essere preteso dinanzi a un tribunale (cfr. il precedente punto 9). Ciò costituisce un'importante differenza rispetto ai diritti di cui gode qualunque individuo i cui dati sono trattati nell'UE, indipendentemente dalla sua nazionalità.

K. Audit

La nuova formulazione seguente è stata inserita nella dichiarazione d'intenti (paragrafo 43) "Il CBP, in collaborazione col DHS, s'impegna a partecipare, una volta all'anno o anche più spesso se così deciso dalle parti, a un'analisi congiunta con la Commissione, assistita come del caso da esperti degli Stati membri dell'Unione europea (4), sull'attuazione della presente dichiarazione d'intenti, al fine di contribuire da entrambe le parti all'effettivo funzionamento dei procedimenti descritti nella dichiarazione stessa. Detta analisi congiunta può riguardare i risultati della relazione annuale presentata al Congresso dal direttore per la privacy del DHS (come previsto al paragrafo 42 della presente dichiarazione d'intenti) e, nella misura in cui ciò è autorizzato dal direttore per la privacy, tutti gli audit effettuati nel periodo cui si riferisce la relazione, o altri risultati riguardanti in particolare la sicurezza dei dati, la condivisione del PNR con le autorità designate e l'accesso personale al PNR nelle banche dati rilevanti, nonché il trattamento dei reclami. Nella misura in cui ciò è autorizzato dal direttore per la privacy del DHS, l'analisi congiunta può comprendere un esame dell'applicazione della dichiarazione d'intenti e può anche riguardare questioni che possono aiutare a migliorare i risultati dell'uso dei dati del PNR ai fini di cui al paragrafo 3 della presente dichiarazione d'intenti."

Si tratta di un'altra evoluzione favorevole e il gruppo di lavoro si aspetta che tali revisioni siano realizzate con l'apertura e la trasparenza necessarie a garantirne l'efficacia. In ogni caso, i membri del gruppo di lavoro s'impegnano a partecipare eventualmente a qualunque revisione di questo tipo e ad osservare le regole di confidenzialità concordate tra le due parti. Il gruppo di lavoro si riserva evidentemente il diritto di rianalizzare la questione, se lo ritiene necessario, qualunque sia il calendario di tali revisioni.

L. Analisi incrociata di schede

I recenti avvenimenti dimostrano che un nuovo elemento deve essere preso in considerazione oltre a quelli che sono stati ricordati sino ad ora. I dati passeggeri PNR raccolti dal CBP sono confrontati negli Stati Uniti con elenchi di persone ricercate.

Queste operazioni di analisi incrociata di schede sono all'origine dell'annullamento all'ultimo minuto di molti voli provenienti dall'UE. Le informazioni fornite successivamente al pubblico mostrano che tali annullamenti erano dovuti ad errori o a casi di confusione d'identità o di omonimia con persone sospettate di terrorismo.

Queste circostanze si iscrivono nel quadro della qualità dei dati e del principio di protezione dei dati. Il gruppo di lavoro ritiene che altre iniziative debbano essere adottate per evitare di esporre i passeggeri, i membri dell'equipaggio e le compagnie aeree a questo tipo di problemi.

(4) La composizione delle équipe delle due parti sarà comunicata in anticipo e può comprendere le autorità competenti per la privacy/la protezione dei dati, i controlli doganali e altre forme di applicazione delle norme, sicurezza dei confini e/o dell'aviazione. Le autorità partecipanti dovranno rispettare la riservatezza delle discussioni e saranno sottoposte ai nulla osta di sicurezza eventualmente necessari. La riservatezza però non sarà un ostacolo a che entrambe le parti possano riferire in modo appropriato dei risultati dell'analisi congiunta alle rispettive autorità competenti, compresi il Congresso degli USA e il Parlamento europeo. Le due parti determinano insieme le modalità dettagliate per l'analisi congiunta.

CONCLUSIONI

Il gruppo di lavoro ricorda che l'obiettivo globale, conformemente a quanto indicato nel suo parere 4/2003, è la messa a punto di un quadro giuridico chiaro affinché qualunque trasferimento di dati delle compagnie aeree verso gli Stati Uniti sia compatibile con i principi di protezione dei dati personali. Il gruppo di lavoro ha preso nota dei progressi realizzati nel dialogo USA-UE per quanto riguarda i dati passeggeri PNR, in particolare l'ultima dichiarazione del 12 gennaio 2004 recentemente presentata dall'amministrazione americana, ed esprime soddisfazione per i miglioramenti rispetto alla versione precedente.

Secondo il gruppo di lavoro, tuttavia, i limitati progressi che sono stati registrati non consentono di giudicare che sia stato raggiunto un livello adeguato di protezione dei dati. Il gruppo di lavoro ritiene che qualunque soluzione dovrà rispettare almeno i seguenti principi di protezione dei dati:

Qualità dei dati:
- il trasferimento di dati deve unicamente avere come finalità la lotta contro gli atti di terrorismo e taluni reati collegati al terrorismo (da definire);
- l'elenco dei dati da trasferire deve essere proporzionale e non deve essere eccessivo;
- le analisi incrociate di dati relativi a individui sospetti devono rispettare norme di qualità elevate in grado di garantire la certezza dei risultati;
- i periodi di conservazione dei dati devono essere brevi e proporzionali;
- i dati dei passeggeri non devono essere utilizzati per realizzare e/o sperimentare il sistema CAPPS II o sistemi analoghi.

I dati sensibili non devono essere trasmessi.

Diritti delle persone interessate:
- È opportuno trasmettere informazioni chiare, attuali e comprensibili ai passeggeri;
- Un diritto d'accesso e di rettifica deve essere concesso senza discriminazioni;
- È opportuno prevedere disposizioni sufficienti in grado di garantire ai passeggeri il diritto di rivolgersi a un organo di ricorso veramente indipendente.

Livello d'impegno delle autorità americane:
- Gli impegni presi dalla parte americana devono avere un carattere giuridico chiaramente vincolante per gli USA;
- È opportuno chiarire il campo di applicazione, la base giuridica e il valore di un eventuale "accordo internazionale leggero".

Gli ulteriori trasferimenti di dati passeggeri PNR ad altri governi o organismi esteri devono essere strettamente limitati.

Metodo di trasferimento: è opportuno utilizzare un metodo di trasferimento "push", attraverso il quale i dati sono selezionati e trasferiti dalle compagnie aeree alle amministrazioni americane.

Fatto a Bruxelles, il 29 gennaio 2004

Dal gruppo di lavoro
Il Presidente
Stefano RODOTÀ

92 Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines (*)

ARTICLE 29 Data Protection Working Party

10037/04/EN
WP 88

Opinion 3/2004 on the level of protection ensured in Canada for the transmission of Passenger Name Records and Advanced Passenger Information from airlines

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2004/wp88_en.pdf

Adopted on 11th February 2004

Nuove Tecnologie

93 Documento di lavoro sull'amministrazione elettronica

ARTICOLO 29 – Gruppo di lavoro per la tutela dei dati personali

10593/02/IT
WP 73

Documento di lavoro sull'amministrazione elettronica

Adottato l'8.5.2003

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2003/e-government_it.pdf

94 Parere 2/2003 sull'applicazione dei principi di tutela dei dati agli elenchi Whois (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10972/03/IT
def. WP 76

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito a seguito della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 [1],

visti gli articoli 29 e 30, paragrafi 1, lettera a), e 3, di tale direttiva, e l'articolo 14, paragrafo 3, della direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997,

visto il regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il presente parere:

1. INTRODUZIONE:

Gli elenchi Whois pongono vari problemi dal punto di vista della tutela dei dati. I *dati Whois* si riferiscono alle persone che hanno registrato un nome di dominio e contengono in particolare informazioni sul nome del punto di contatto del nome del dominio, inclusi numero di telefono, indirizzo e E-mail e altri dati personali. Inizialmente tali dati sono stati pubblicati per consentire alle persone che effettuano attività in rete di contattare la persona tecnicamente responsabile di un'altra rete o di un altro dominio, in caso di problema. Di per se stesso, tale obiettivo è legittimo.

Il gruppo è consapevole dell'importanza crescente assunta dal dibattito su Whois a mano che un numero sempre maggiore di individui (privati) registrano i loro nomi di dominio e che sono state sporte denunce per l'uso improprio dei dati Whois in vari paesi. La registrazione di nomi di dominio da parte di singoli pone considerazioni giuridiche diverse da quelle di società o di altre persone giuridiche che registrano nomi di dominio, come verrà chiarito nel presente parere.

Il gruppo ha quindi seguito con interesse i lavori della Task Force ICANN Whois riguardanti tali elenchi Whois nonché i lavori svolti in questo campo dal gruppo internazionale per la protezione dei dati nelle telecomunicazioni [2].

Il gruppo è consapevole del fatto che gli elenchi Whois saranno discussi nel quadro della conferenza ICANN/GAC che si terrà a Montreal alla fine del mese di giugno. Il gruppo gradirebbe contribuire alla discussione presentando il suo parere, mirante a sottolineare un certo numero di questioni fondamentali che sorgono con l'applicazione dei principi di protezione dei dati agli elenchi Whois. Il parere riguarda gli elenchi Whois ma, nella misura in cui le stesse circostanze o circostanze simili vi si riferiscano, le stesse considerazioni si applicano anche ad altri registri di nomi di dominio e di indirizzi IP a livello regionale, ad esempio RIPE in Europa, AP-NIC in Asia, ecc.

2. L'APPLICAZIONE DEI PRINCIPI DELLA PROTEZIONE DEI DATI AGLI ELENCHI WHOIS:

- Dal punto di vista della tutela dei dati, è indispensabile determinare in termini esr mamente chiari quale sia l'obiettivo degli elenchi Whois e quali obiettivi possano

(*) Il gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, Proprietà intellettuale e industriale, Media e Protezione dei dati) della Commissione europea, Direzione generale mercato interno, B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136.
Website: www.europa.eu.int/comm/privacy

(1) Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile su: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

(2) Posizione comune sugli aspetti della vita privata e della tutela dei dati della registrazione dei nomi di dominio su Internet, adottata in occasione della 27ª riunione del gruppo di lavoro il 4/5 maggio 2000 a Rethymnon/Creta, disponibile su: www.datenschutz-berlin.de/doc/int/iwgdpt/dns_en.htm

considerarsi legittimi e compatibili con l'obiettivo originale. Le relazioni della Task Force Whois non hanno trattato questi aspetti. Si tratta di una questione estremamente delicata, dato che l'obiettivo degli elenchi Whois non può essere esteso ad altri obiettivi per il semplice fatto che possano essere ritenuti convenienti da certi potenziali utilizzatori degli elenchi. Alcuni obiettivi che potrebbero sollevare problemi connessi con la tutela di dati (compatibilità) sono ad esempio l'utilizzazione di dati da parte di operatori del settore privato nell'ambito di attività di polizia private connesse con presunte violazioni dei loro diritti, ad esempio nel campo della gestione dei diritti digitali.

- L'articolo 6, lettera c) della direttiva impone chiari limiti quanto alla raccolta e all'elaborazione di dati personali nel senso che essi debbono essere pertinenti e non eccessivi per i fini cui sono destinati. In questa prospettiva è indispensabile limitare la quantità di dati personali da raccogliere e elaborare. Di ciò si dovrebbe tener particolarmente conto al momento di discutere il desiderio di alcune parti interessate di aumentare l'uniformità dei vari elenchi Whois.
  La registrazione di nomi di dominio da parte di singoli pone considerazioni giuridiche diverse da quelle di società o di altre persone giuridiche che registrano nomi di dominio.
  - Nel primo caso, la pubblicazione di determinate informazioni circa la società o l'organizzazione (ad esempio, identificazione e indirizzo fisico) è frequentemente un requisito legale nell'ambito delle attività commerciali o professionali svolte. Occorre peraltro osservare che, anche nel caso di società o di organizzazioni che registrano nomi di dominio, i singoli non possono essere obbligati a fornire il loro nome da pubblicare come punto di contatto, dato che possono esercitare il loro diritto di opposizione.
  - Nel secondo caso, ove un singolo registri un nome di dominio, la situazione è diversa e, quantunque sia chiaro che l'identità e il contatto debbano essere conosciuti dal fornitore del servizio, non esiste giustificazione giuridica alla pubblicazione obbligatoria dei dati personali di tale persona. Una tale pubblicazione di dati personali di persone, ad esempio i loro indirizzi e numeri di telefono, verrebbe a scontrarsi con il diritto di tali persone di decidere se i dati di carattere personale loro relativi, e quali di tali dati, debbano figurare in un elenco pubblico [3]. Peraltro l'obiettivo originale di tali elenchi Whois può essere ugualmente raggiunto, in quanto i particolari della persona sono noti al fornitore di servizi Internet che può, in caso di problemi connessi con il sito, contattare la persona [4].

• Alla luce del principio della proporzionalità, è necessario cercare metodi meno invasivi in grado di raggiungere gli obiettivi degli elenchi Whois senza rendere tutti i dati direttamente disponibili on-line per chiunque. Come già menzionato nell'introduzione, i fornitori di servizi Internet possono svolgere, e di fatto lo fanno in alcuni paesi, un ruolo importante in questo campo. In ogni caso dovrebbero essere elaborati meccanismi di filtraggio per garantire una limitazione degli obiettivi nelle interfacce per accedere agli elenchi.

• Il fatto che dati personali sono resi pubblici non significa che i requisiti della direttiva sulla tutela dei dati non si applicano a tali dati. Al contrario, come si è già affermato nei precedenti pareri del gruppo [5], è perfettamente chiaro, dalla formulazione della legislazione in merito alla tutela dei dati, che le disposizioni si applicano anche ai dati resi pubblici: anche dopo essere stati resi pubblici, i dati restano tuttora personali e, di conseguenza, le persone interessate non possono essere private della protezione cui hanno diritto per quanto riguarda il trattamento dei loro dati.

• Il gruppo è particolarmente preoccupato delle proposte relative a dispositivi Whois dotati di maggiori possibilità di ricerca. In questo contesto esso gradirebbe menzionare le conclusioni del suo parere 5/2000 sull'utilizzazione degli elenchi telefonici pubblici per servizi di ricerca inversa o multicriterio (elenchi invertiti) [6]: l'elaborazione di dati personali in elenchi invertiti e in servizi di ricerca multicriterio senza il consenso chiaro e informato della persona interessata è sleale e illecita.

(3) Articolo 12, paragrafo 2, della direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).
(4) Un sistema del genere è stato istituito in vari paesi europei, ad esempio in Francia (attraverso l'AFNIC) e nel Regno Unito. Nel Regno Unito, ad esempio, le persone singole che registrano nomi di dominio ('tag-holders') possono registrarsi negli elenchi Whois a cura del loro FSI, il che significa che, in caso di problema con un sito web, si può contattare il proprietario attraverso l'FSI senza che l'indirizzo della persona in questione figuri in una base dati aperta.
(5) Parere n. 3/99 relativo alle informazioni del settore pubblico e alla protezione di dati personali, WP 20.
(6) http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_2k.htm

• Il gruppo desidera esprimere il suo sostegno alle proposte relative alla precisione dei dati (che è altresì uno dei principi della direttiva europea sulla tutela dei dati [7]) e alla limitazione dell'accesso massiccio a fini di marketing diretto.

L'utilizzazione intensiva dei dati Whois per il marketing diretto è totalmente in contraddizione con i fini per i quali sono stati allestiti e vengono gestiti gli elenchi. Alla luce delle disposizioni della direttiva sulle comunicazioni elettroniche [8] qualsiasi utilizzazione di indirizzi E-mail per il marketing diretto deve basarsi unicamente sul consenso della persona interessata.

Il gruppo invita l'ICANN e la comunità Whois ad esaminare modalità per aumentare la protezione della vita privata nella gestione degli elenchi Whois, in modo sia da raggiungere l'obiettivo originale sia da proteggere i diritti delle persone. Dovrebbe essere comunque possibile, per persone singole, registrare nomi di dominio senza che sia necessario che i loro dati personali figurino in un registro pubblico.

Per il gruppo
Il presidente
Stefano RODOTA

(7) Cfr. articolo 6, lettera d) della direttiva.
(8) Direttive 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

95 Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG) (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

11816/03/FR
WP 86

Documento di lavoro sulle piattaforme informatiche fidate, in particolare per quanto riguarda il lavoro effettuato da Trusted Computing Group (Gruppo TCG)

Adottato il 23 gennaio 2004

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2004/wp86_it.pdf

Codici di Condotta comunitari

96 Parere 3/2003 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

10066/03/EN def
GL 77

Parere 3/2003 sul codice di condotta europeo della FEDMA per l'utilizzazione dei dati personali nel marketing diretto

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs /2003/wp77_it.pdf

Adottato in data 13 giugno 2003

97 Sixth annual report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the year 2001 (*)

ARTICOLO 29 - Gruppo di lavoro per la tutela dei dati personali

Sixth annual report
on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries
covering the year 2001

adopted on 16th December 2003

(*) Prima pagina del documento, rinvenibile in www.europa.eu.int /comm/internal_market /privacy/docs/wpdocs/2003 /2003-6th-annualreport_en.pdf

25ª Conferenza internazionale delle Autorità di protezione dei dati. Sydney 10-12 settembre 2003

98 Risoluzione relativa al miglioramento della comunicazione di informazioni sulle politiche seguite in materia di protezione dei dati e privacy (*)

Proponente: Autorità per la privacy, Australia; co-sponsors:
- Autorità per la protezione dei dati e l'accesso agli atti, Brandeburgo, Germania
- Commissione nazionale informatica e libertà, Francia
- Autorità per la protezione dei dati, Repubblica Ceca
- Autorità ellenica per la protezione dei dati
- Centro indipendente per la tutela della privacy, Schleswig-Holstein, Germania
- Ispettorato statale per la protezione dei dati, Repubblica di Lituania
- Autorità olandese per la protezione dei dati

Risoluzione

La 25ma Conferenza internazionale delle Autorità di protezione dati e della privacy adotta la seguente risoluzione:

1. La Conferenza richiama l'attenzione di soggetti pubblici e privati sull'importanza
   - di migliorare significativamente la comunicazione delle informazioni da essi fornite sulle modalità di gestione e trattamento di dati personali,
   - di raggiungere una coerenza complessiva nelle modalità di comunicazione di tali informazioni,

e, così facendo,

   - di migliorare la comprensione e la sensibilizzazione dei singoli rispetto ai diritti ed alle opzioni disponibili e la rispettiva capacità di incidere su tali diritti e opzioni, e
   - di incentivare i vari soggetti, in seguito a tale sensibilizzazione, a migliorare le politiche seguite nella gestione e nel trattamento dei dati e ad accrescerne la lealtà e correttezza.

2. La Conferenza si fa promotrice dei seguenti strumenti ai fini del raggiungimento degli obiettivi prima citati:
   - messa a punto e utilizzazione di un formato sintetico per la presentazione di un quadro complessivo delle informazioni in materia di privacy che sia standardizzato a livello mondiale per tutti i soggetti e stabilisca
     - le informazioni più importanti da rendere note ai singoli, le informazioni che con maggiore probabilità i singoli desiderano conoscere, e l'impiego di un linguaggio semplice, inequivocabile e diretto;
     - l'impiego della lingua del sito web o del modulo utilizzati per la raccolta delle informazioni;
   - previsione della limitazione del formato ad un numero ristretto di elementi che, coe-

rentemente con quanto sopra indicato, si riferiscano a principi importanti in materia di protezione dati, come ad esempio
  - il soggetto che raccoglie i dati personali e le modalità per contattarlo (almeno la denominazione ufficiale del soggetto e il suo indirizzo fisico);
  - quali dati personali sono raccolti dal soggetto in questione e con quali strumenti; le finalità per cui il soggetto raccoglie i dati personali;
  - se i dati personali saranno resi noti ad altri soggetti e, in tal caso, le tipologie o i nominativi di tali soggetti e le relative finalità,
  - le opzioni in materia di privacy di cui dispongono i singoli ed i meccanismi per esercitarle con facilità, in particolare le opzioni relative all'eventualità che dati personali siano rivelati a terzi per finalità non correlate, ancorché legittime, ed ai dati personali che i singoli sono tenuti a fornire per ricevere un servizio,
  - una sintesi dei diritti di accesso, rettifica, blocco o cancellazione riconosciuti ai singoli,
  - l'ente di controllo indipendente al quale i singoli possono sottoporre reclami qualora ritengano di avere subito una violazione dei propri diritti;
- impiego di strumenti opportuni al fine di consentire ai singoli di reperire con facilità informazioni ulteriori, come ad esempio
  - informazioni che un soggetto sia tenuto a fornire in base alla normativa vigente, per esempio in materia di diritto di accesso, rettifica, blocco o cancellazione, ed il periodo di conservazione dei dati personali da parte dei singoli soggetti, e
  - una spiegazione esauriente delle informazioni presentate in forma sintetica nel formato condensato, e
  - la descrizione completa delle politiche seguite dal soggetto nella gestione e nel trattamento delle informazioni.

3. La Conferenza concorda sul fatto che il formato standardizzato e condensato di cui sopra dovrebbe essere conforme a tutte le norme nazionali applicabili, e che esso debba integrare, se necessario, ed essere compatibile con le informazioni che un soggetto sia tenuto per legge a fornire ai singoli.

4. La Conferenza è consapevole dell'importanza del momento in cui l'interessato prende visione dell'informativa in materia di protezione dati e privacy. Ad esempio, è particolarmente auspicabile che tale informativa sia fornita in modo automatico nel momento in cui ai singoli è data la possibilità di scegliere quali informazioni fornire e se consentire la comunicazione di tali informazioni a terzi. In altri casi può essere opportuno lasciare che siano i singoli a reperire le informazioni in materia di privacy e protezione dati attraverso legami ipertestuali evidenti. La Conferenza è consapevole delle importanti attività svolte dal Gruppo di lavoro UE in materia di protezione dei dati ex Articolo 29, per quanto riguarda la presentazione automatica di informazioni relative a privacy e protezione dati, attraverso la Raccomandazione 2/2001 su alcuni requisiti minimi per la raccolta online di dati personali nell'Unione Europea.

5. La Conferenza ritiene che l'attività delle Autorità di protezione dati e privacy potrebbe proseguire in modo fruttuoso valutando il momento in cui presentare l'informativa nel formato condensato, che tiene conto delle caratteristiche dell'ambiente sia offline sia online.

6. La Conferenza è al corrente, inoltre, di attività correlate quali la definizione di linguaggi informatici in grado di descrivere le politiche adottate in materia di privacy. La Conferenza invita a proseguire nella messa a punto di meccanismi utili a tradurre tali politiche nel formato standardizzato e condensato prima descritto.

7. La Conferenza considera quanto sopra un primo passo volto a promuovere migliori prassi nei meccanismi con cui i vari soggetti comunicano le informazioni relative alle modalità di gestione o trattamento di dati personali. La Conferenza è al corrente delle iniziative intraprese in questo settore, e invita tali iniziative a migliorare la comunicazione fra le parti in causa (soggetti che trattano i dati e singoli individui i cui dati sono oggetto di trattamento). La Conferenza intende collaborare con i soggetti ed i gruppi di interesse impegnati in tali iniziative, e prevede di compiere passi ulteriori al fine di migliorare le comunicazioni fra singoli e soggetti che trattano i dati nell'ambito di future conferenze.

99 Risoluzione relativa alla protezione dei dati ed agli organismi internazionali

Proponente: Autorità per la privacy, Nuova Zelanda.

Co-sponsors:
- Autorità per la protezione dei dati, Irlanda
- Commissione nazionale informatica e libertà, Francia
- Autorità per la privacy e i dati personali, Hong Kong SAR
- Autorità federale per la protezione dei dati, Germania

RISOLUZIONE

La 25ma Conferenza internazionale delle Autorità di protezione dati e della privacy adotta la seguente risoluzione:

La Conferenza invita

a. gli enti internazionali e sopranazionali ad impegnarsi formalmente al rispetto di principi compatibili con i più importanti strumenti internazionali relativi a protezione dei dati e privacy;
b. gli enti internazionali e sopranazionali che detengono o trattano dati personali a definire meccanismi opportuni onde garantire il rispetto dei principi applicabili in materia di protezione dei dati, come la creazione di autorità di controllo interne ma indipendenti sul piano operativo e dotate di poteri di controllo;
c. gli enti internazionali e sopranazionali che partecipino alla promulgazione di norme, regole o prassi comuni tali da produrre effetti sulla gestione di dati personali nel territorio soggetto alla giurisdizione dei rispettivi componenti, ad elaborare e adottare meccanismi atti a garantire che si tenga effettivamente conto degli aspetti legati alla protezione dei dati, come il ricorso a valutazioni dell'impatto in termini di privacy e la consultazione di autorità riconosciute in materia di protezione dei dati; inoltre, chiede all'autorità che ha ospitato la 25ma Conferenza Internazionale di richiamare l'attenzione degli enti pertinenti sulla presente risoluzione.

100 Risoluzione sul trasferimento di dati relativi a passeggeri

L'Autorità federale svizzera per la protezione dei dati, l'Ufficio per la protezione dei dati personali della Repubblica Ceca, l'Ombudsman per la protezione dei dati della Finlandia e l'Autorità federale tedesca per la protezione dei dati propongono che la Conferenza Internazionale adotti la seguente risoluzione:

A. La Conferenza rileva che

1. Nel quadro della lotta legittima contro il terrorismo e la criminalità organizzata, in alcuni Paesi sono allo studio misure che potrebbero minacciare diritti e libertà fondamentali, in particolare il diritto alla privacy.
2. C'è il rischio di minare la democrazia e la libertà attraverso misure finalizzate a difenderle.
3. Disposizioni di legge che impongano ai fornitori di trasporto di consentire l'accesso a, o trasferire dati da, insiemi di dati relativi ai passeggeri, memorizzati nei sistemi di prenotazione aerea, potrebbero confliggere con i principi internazionali della protezione dei dati o con gli obblighi imposti alle compagnie aeree dalle normative nazionali in materia di protezione dei dati.

B. La Conferenza, pertanto, afferma che

1. Nella lotta contro il terrorismo e la criminalità organizzata, gli Stati dovrebbero definire la propria risposta tenendo pienamente conto di principi fondamentali della protezione dei dati, i quali costituiscono parte integrante dei valori da tutelare.
2. Qualora siano necessari trasferimenti internazionali di dati personali su base regolare, ciò dovrebbe avvenire in un contesto che tenga conto della protezione dei dati, ad esempio sulla base di un accordo internazionale che preveda norme adeguate in materia di protezione dei dati, fra cui una chiara limitazione delle relative finalità, la raccolta di dati adeguati e non eccedenti, un periodo limitato di conservazione dei dati, l'informativa per gli interessati, la garanzia dell'esercizio dei diritti riconosciuti agli interessati ed un controllo indipendente.

101 Risoluzione relativa agli aggiornamenti automatici di software

RISOLUZIONE

Le Autorità per la protezione dei dati della Germania, della Repubblica Ceca, dell'Italia, l'Ispettorato per la protezione dei dati della Repubblica di Lituania, l'Autorità per l'informazione e la privacy dello stato di Ontario e l'Autorità federale svizzera per la protezione dei dati propongono che la Conferenza Internazionale adotti la seguente risoluzione:

1. La Conferenza rileva con preoccupazione che le case produttrici di software in tutto il mondo fanno sempre più ricorso a meccanismi non trasparenti per trasferire aggiornamenti di software nel computer degli utenti.

Così facendo, esse

- sono in grado di leggere e raccogliere dati personali memorizzati nel computer dei singoli utenti (ad esempio, le impostazioni dei programmi di navigazione, e informazioni sulle abitudini di navigazione del singolo utente) senza che questi abbiano la possibilità di accorgersene, intervenire o impedirlo,
- possono assumere il controllo, almeno parziale, del computer terminale e, quindi, limitare la capacità dell'utente di far fronte agli obblighi ed alle responsabilità previsti dalla legge nei suoi riguardi, in quanto titolare del trattamento, al fine di garantire la sicurezza dei dati personali eventualmente oggetto di trattamento,
- modificano il software installato sul computer, che sarà quindi utilizzato senza essere collaudato o approvato nei modi previsti, e
- possono provocare malfunzionamenti del computer senza che sia possibile individuarne la causa nell'aggiornamento.

Tutto ciò può comportare particolari problemi per la pubblica amministrazione e le aziende private, nella misura in cui sussistano specifici obblighi di legge a loro carico relativamente alle modalità di trattamento dei dati personali.

2. La Conferenza, pertanto, invita le società produttrici di software

a. ad offrire procedure per l'aggiornamento online del software soltanto su richiesta o iniziativa dell'utente, secondo modalità trasparenti e senza consentire accessi non controllati al computer dell'utente;
b. a chiedere la comunicazione di dati personali soltanto con il consenso informato dell'utente e nella misura in cui ciò risulti necessario per effettuare l'aggiornamento online. Gli utenti non dovrebbero essere obbligati a fornire le proprie credenziali di identificazione – anziché di autenticazione – per dare inizio alla procedura di caricamento remoto;
c. a prevedere meccanismi di libera scelta, offrendo l'aggiornamento online esclusivamente in alternativa ad altre forme (offline) di distribuzione del software, ad esempio via CD-ROM.

3. La Conferenza promuove la definizione e l'applicazione di tecnologie per l'aggiornamento del software che siano rispettose della privacy e dell'autonomia degli utenti.

102 Risoluzione sull'identificazione attraverso radiofrequenze (RFID)

Sulla base di una proposta formulata dall'Autorità per la protezione dei dati e l'accesso alle informazioni del Brandeburgo, dal Centro indipendente per la tutela della privacy dello Schleswig-Holstein, dall'Autorità spagnola per la protezione dei dati e dall'Autorità per la protezione dei dati del Cantone Zug, Svizzera, la Conferenza internazionale delibera quanto segue:

I dispositivi basati sull'identificazione attraverso radiofrequenze (RFID) trovano impiego crescente per numerosi scopi. Pur esistendo situazioni in cui tale tecnologia può avere effetti positivi e benefici, vi sono anche implicazioni potenziali in termini di privacy. Sinora le etichette RFID vengono utilizzate soprattutto per l'identificazione e la gestione di oggetti (prodotti), per il controllo della catena distributiva, o per tutelare l'autenticità di singoli marchi; tuttavia, esse potrebbero essere messe in relazione con dati personali come quelli ricavabili dalle carte di credito, e potrebbero essere utilizzate persino per raccogliere tali dati, oppure per localizzare o profilare individui in possesso di oggetti che rechino tali etichette. La tecnologia in questione potrebbe consentire di ricostruire le attività di singoli individui e istituire collegamenti fra le informazioni raccolte e banche dati preesistenti.

La Conferenza sottolinea la necessità di tenere conto dei principi di protezione dati qualora si preveda di introdurre etichette RFID connesse a dati personali. Occorre rispettare tutti i principi fondamentali della normativa in materia di protezione dei dati e privacy nella progettazione, nella realizzazione e nell'utilizzazione di dispositivi basati sulla tecnologia RFID. In particolare,

a) prima di ricorrere a etichette RFID connesse a dati personali, o tali da consentire la profilazione della clientela, ciascun titolare di trattamento dovrebbe valutare approcci alternativi che consentano di raggiungere lo stesso obiettivo senza raccogliere dati personali o profilare la clientela;
b) qualora il titolare del trattamento dimostri che è indispensabile ricorrere a dati personali, questi ultimi devono essere raccolti in modo chiaro e trasparente;
c) i dati personali possono essere utilizzati esclusivamente per lo scopo specifico per cui sono stati inizialmente raccolti, e possono essere conservati soltanto finché risultino necessari al raggiungimento (o al soddisfacimento) di tale scopo, e
d) i singoli interessati dovrebbero avere la possibilità di cancellare i dati e di disattivare o distruggere le etichette RFID una volta che ne siano entrati in possesso.

Si dovrebbe tenere conto dei principi sopra indicati nella progettazione e nell'utilizzazione di prodotti con tecnologie RFID.

La lettura e l'attivazione remote di etichette RFID, senza che la persona in possesso dell'oggetto recante un'etichetta del genere abbia alcuna ragionevole possibilità di intervenire in tale procedimento, sarebbero fonte di ulteriori preoccupazioni in termini di privacy.

La Conferenza e l'International Working Group on Data Protection in Telecommunications intendono seguire con attenzione e in modo approfondito gli sviluppi tecnologici in questo campo, al fine di garantire il rispetto dei principi di protezione dati e privacy nell'ambito della cosiddetta "informatizzazione pervasiva" (ubiquitous computing).

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il Codice

Codice in materia di protezione dei dati personali Decreto legislativo 30 giugno 2003, n. 196 (*)

IL PRESIDENTE DELLA REPUBBLICA

VISTI gli articoli 76 e 87 della Costituzione;

VISTO l'articolo 1 della legge 24 marzo 2001, n. 127, recante delega al Governo per l'emanazione di un testo unico in materia di trattamento dei dati personali;

VISTO l'articolo 26 della legge 3 febbraio 2003, n. 14, recante disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee (legge comunitaria 2002);

VISTA la legge 31 dicembre 1996, n. 675, e successive modificazioni;

VISTA la legge 31 dicembre 1996, n. 676, recante delega al Governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

VISTA la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati;

VISTA la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche;

VISTA la preliminare deliberazione del Consiglio dei ministri, adottata nella riunione del 9 maggio 2003;

SENTITO il Garante per la protezione dei dati personali;

ACQUISITO il parere delle competenti Commissioni parlamentari della Camera dei deputati e del Senato della Repubblica;

VISTA la deliberazione del Consiglio dei ministri, adottata nella riunione del 27 giugno 2003;

SULLA PROPOSTA del Presidente del Consiglio dei ministri, del Ministro per la funzione pubblica e del Ministro per le politiche comunitarie, di concerto con i Ministri della giustizia, dell'economia e delle finanze, degli affari esteri e delle comunicazioni;

EMANA

il seguente decreto legislativo:

(*) Testo consolidato con la legge 26 febbraio 2004, n. 45, di conversione con modificazioni del d.l. 24 dicembre 2003, n. 354

PARTE I - DISPOSIZIONI GENERALI

TITOLO I - PRINCIPI GENERALI

Art. 1. Diritto alla protezione dei dati personali

1. Chiunque ha diritto alla protezione dei dati personali che lo riguardano.

Art. 2. Finalità

1. Il presente testo unico, di seguito denominato "codice", garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il trattamento dei dati personali è disciplinato assicurando un elevato livello di tutela dei diritti e delle libertà di cui al comma 1 nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

Art. 3. Principio di necessità nel trattamento dei dati

1. I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità.

Art. 4. Definizioni

1. Ai fini del presente codice si intende per:
   a) "trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;
   b) "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;
   c) "dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;
   d) "dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
   e) "dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;
   f) "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
   g) "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione

e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) "incaricati", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

i) "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

l) "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

m) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

o) "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

p) "banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

q) "Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

2. Ai fini del presente codice si intende, inoltre, per:

a) "comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

b) "chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

c) "reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) "rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

e) "servizio di comunicazione elettronica", i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera c), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;

f) "abbonato", qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;

g) "utente", qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;

h) "dati relativi al traffico", qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;

i) "dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

l) "servizio a valore aggiunto", il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione;

m) "posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

3. Ai fini del presente codice si intende, altresì, per:

a) "misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

b) "strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

c) "autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

d) "credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica;

e) "parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

f) "profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

g) "sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

4. Ai fini del presente codice si intende per:

a) "scopi storici", le finalità di studio, indagine, ricerca e documentazione di figure, fatti e circostanze del passato;

b) "scopi statistici", le finalità di indagine statistica o di produzione di risultati statistici, anche a mezzo di sistemi informativi statistici;

c) "scopi scientifici", le finalità di studio e di indagine sistematica finalizzata allo sviluppo delle conoscenze scientifiche in uno specifico settore.

Art. 5. Oggetto ed ambito di applicazione

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

Art. 6. Disciplina del trattamento

1. Le disposizioni contenute nella presente Parte si applicano a tutti i trattamenti di dati, salvo quanto previsto, in relazione ad alcuni trattamenti, dalle disposizioni integrative o modificative della Parte II.

TITOLO II - DIRITTI DELL'INTERESSATO

Art. 7. Diritto di accesso ai dati personali ed altri diritti

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:
   a) dell'origine dei dati personali;
   b) delle finalità e modalità del trattamento;
   c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
   d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
   e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:
   a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
   b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
   c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:
   a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
   b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

Art. 8. Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:
   a) in base alle disposizioni del decreto legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
   b) in base alle disposizioni del decreto legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
   c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della

Costituzione;

d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;

e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;

f) da fornitori di servizi di comunicazione elettronica accessibili al pubblico relativamente a comunicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;

g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;

h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

Art. 9. Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

Art. 10. Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere comunicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la comunicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La comunicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di comunicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

TITOLO III - REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

CAPO I - REGOLE PER TUTTI I TRATTAMENTI

Art. 11. Modalità del trattamento e requisiti dei dati

1. I dati personali oggetto di trattamento sono:
a) trattati in modo lecito e secondo correttezza;
b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi;
c) esatti e, se necessario, aggiornati;

d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati;
e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

Art. 12. Codici di deontologia e di buona condotta

1. Il Garante promuove nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. I codici sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice.

3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

Art. 13. Informativa

1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registra-

zione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:
   a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
   b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
   c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

Art. 14. Definizione di profili e della personalità dell'interessato

1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato.

2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17.

Art. 15. Danni cagionati per effetto del trattamento

1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.

2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11.

Art. 16. Cessazione del trattamento

1. In caso di cessazione, per qualsiasi causa, di un trattamento i dati sono:
   a) distrutti;
   b) ceduti ad altro titolare, purché destinati ad un trattamento in termini compatibili agli scopi per i quali i dati sono raccolti;
   c) conservati per fini esclusivamente personali e non destinati ad una comunicazione sistematica o alla diffusione;
   d) conservati o ceduti ad altro titolare, per scopi storici, statistici o scientifici, in conformità alla legge, ai regolamenti, alla normativa comunitaria e ai codici di deontologia e di buona condotta sottoscritti ai sensi dell'articolo 12.

2. La cessione dei dati in violazione di quanto previsto dal comma 1, lettera b), o di altre disposizioni rilevanti in materia di trattamento dei dati personali è priva di effetti.

Art. 17. Trattamento che presenta rischi specifici

1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti.

2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.

CAPO II - REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici

1. Le disposizioni del presente capo riguardano tutti i soggetti pubblici, esclusi gli enti pubblici economici.

2. Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali.

3. Nel trattare i dati il soggetto pubblico osserva i presupposti e i limiti stabiliti dal presente codice, anche in relazione alla diversa natura dei dati, nonché dalla legge e dai regolamenti.

4. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell'interessato.

5. Si osservano le disposizioni di cui all'articolo 25 in tema di comunicazione e diffusione.

Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari

1. Il trattamento da parte di un soggetto pubblico riguardante dati diversi da quelli sensibili e giudiziari è consentito, fermo restando quanto previsto dall'articolo 18, comma 2, anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente.

2. La comunicazione da parte di un soggetto pubblico ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali e può essere iniziata se è decorso il termine di cui all'articolo 39, comma 2, e non è stata adottata la diversa determinazione ivi indicata.

3. La comunicazione da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione da parte di un soggetto pubblico sono ammesse unicamente quando sono previste da una norma di legge o di regolamento.

Art. 20. Principi applicabili al trattamento di dati sensibili

1. Il trattamento dei dati sensibili da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge nella quale sono specificati i tipi di dati che possono essere trattati e di operazioni eseguibili e le finalità di rilevante interesse pubblico perseguite.

2. Nei casi in cui una disposizione di legge specifica la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e di operazioni eseguibili, il trattamento è consentito solo in riferimento ai tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi e nel rispetto dei principi di cui all'articolo 22, con atto di natura regolamentare adottato in conformità al parere espresso dal Garante ai sensi dell'articolo 154, comma 1, lettera g), anche su schemi tipo.

3. Se il trattamento non è previsto espressamente da una disposizione di legge i soggetti pubblici possono richiedere al Garante l'individuazione delle attività, tra quelle demandate ai medesimi soggetti dalla legge, che perseguono finalità di rilevante interesse pubblico e per le quali è conseguentemente autorizzato, ai sensi dell'articolo 26, comma 2, il trattamento dei dati sensibili. Il trattamento è consentito solo se il soggetto pubblico provvede altresì a identificare e rendere pubblici i tipi di dati e di operazioni nei modi di cui al comma 2.

4. L'identificazione dei tipi di dati e di operazioni di cui ai commi 2 e 3 è aggiornata e integrata periodicamente.

Art. 21. Principi applicabili al trattamento di dati giudiziari

1. Il trattamento di dati giudiziari da parte di soggetti pubblici è consentito solo se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

2. Le disposizioni di cui all'articolo 20, commi 2 e 4, si applicano anche al trattamento dei dati giudiziari.

Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari

1. I soggetti pubblici conformano il trattamento dei dati sensibili e giudiziari secondo modalità volte a prevenire violazioni dei diritti, delle libertà fondamentali e della dignità dell'interessato.

2. Nel fornire l'informativa di cui all'articolo 13 i soggetti pubblici fanno espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento dei dati sensibili e giudiziari.

3. I soggetti pubblici possono trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

4. I dati sensibili e giudiziari sono raccolti, di regola, presso l'interessato.

5. In applicazione dell'articolo 11, comma 1, lettere c), d) ed e), i soggetti pubblici verificano periodicamente l'esattezza e l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza e indispensabilità rispetto alle finalità perseguite nei singoli casi, anche con riferimento ai dati che l'interessato fornisce di propria iniziativa. Al fine di assicurare che i dati sensibili e giudiziari siano indispensabili rispetto agli obblighi e ai compiti loro attribuiti, i soggetti pubblici valutano specificamente il rapporto tra i dati e gli adempimenti. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non possono essere utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene. Specifica attenzione è prestata per la verifica dell'indispensabilità dei dati sensibili e giudiziari riferiti a soggetti diversi da quelli cui si riferiscono direttamente le prestazioni o gli adempimenti.

6. I dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, sono trattati con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che, considerato il numero e la natura dei dati trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità.

7. I dati idonei a rivelare lo stato di salute e la vita sessuale sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo. I medesimi dati sono trattati con le modalità di cui al comma 6 anche quando sono tenuti in elenchi, registri o banche di dati senza l'ausilio di strumenti elettronici.

8. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

9. Rispetto ai dati sensibili e giudiziari indispensabili ai sensi del comma 3, i soggetti pubblici sono autorizzati ad effettuare unicamente le operazioni di trattamento indispensabili per il perseguimento delle finalità per le quali il trattamento è consentito, anche quando i dati sono raccolti nello svolgimento di compiti di vigilanza, di controllo o ispettivi.

10. I dati sensibili e giudiziari non possono essere trattati nell'ambito di test psico-attitudinali volti a definire il profilo o la personalità dell'interessato. Le operazioni di raffronto tra dati sensibili e giudiziari, nonché i trattamenti di dati sensibili e giudiziari ai sensi dell'articolo 14, sono effettuati solo previa annotazione scritta dei motivi.

11. In ogni caso, le operazioni e i trattamenti di cui al comma 10, se effettuati utilizzando banche di dati di diversi titolari, nonché la diffusione dei dati sensibili e giudiziari, sono ammessi solo se previsti da espressa disposizione di legge.

12. Le disposizioni di cui al presente articolo recano principi applicabili, in conformità ai rispettivi ordinamenti, ai trattamenti disciplinati dalla Presidenza della Repubblica, dalla Camera dei deputati, dal Senato della Repubblica e dalla Corte costituzionale.

CAPO III - REGOLE ULTERIORI PER I PRIVATI ED ENTI PUBBLICI ECONOMICI

Art. 23. Consenso

1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.

Art. 24. Casi nei quali può essere effettuato il trattamento senza consenso

1. Il consenso non è richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento:

a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato;

c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati;

d) riguarda dati relativi allo svolgimento di attività economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato;

h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati.

Art. 25. Divieti di comunicazione e diffusione

1. La comunicazione e la diffusione sono vietate, oltre che in caso di divieto disposto dal Garante o dall'autorità giudiziaria:

a) in riferimento a dati personali dei quali è stata ordinata la cancellazione, ovvero quando è decorso il periodo di tempo indicato nell'articolo 11, comma 1, lettera e);

b) per finalità diverse da quelle indicate nella notificazione del trattamento, ove prescritta.

2. È fatta salva la comunicazione o diffusione di dati richieste, in conformità alla legge, da forze di polizia, dall'autorità giudiziaria, da organismi di informazione e sicurezza o da altri soggetti pubblici ai sensi dell'articolo 58, comma 2, per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione di reati.

Art. 26. Garanzie per i dati sensibili

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

3. Il comma 1 non si applica al trattamento:

a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei principi indicati al riguardo con autorizzazione del Garante;

b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non

può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

Art. 27. Garanzie per i dati giudiziari

1. Il trattamento di dati giudiziari da parte di privati o di enti pubblici economici è consentito soltanto se autorizzato da espressa disposizione di legge o provvedimento del Garante che specifichino le rilevanti finalità di interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili.

TITOLO IV - SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art. 28. Titolare del trattamento

1. Quando il trattamento è effettuato da una persona giuridica, da una pubblica amministrazione o da un qualsiasi altro ente, associazione od organismo, titolare del trattamento è l'entità nel suo complesso o l'unità od organismo periferico che esercita un potere decisionale del tutto autonomo sulle finalità e sulle modalità del trattamento, ivi compreso il profilo della sicurezza.

Art. 29. Responsabile del trattamento

1. Il responsabile è designato dal titolare facoltativamente.

2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.

4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.

5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni.

Art. 30. Incaricati del trattamento

1. Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite.

2. La designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima.

TITOLO V - SICUREZZA DEI DATI E DEI SISTEMI

CAPO I - MISURE DI SICUREZZA

Art. 31. Obblighi di sicurezza

1. I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Art. 32. Particolari titolari

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta ai sensi dell'articolo 31 idonee misure tecniche e organizzative adeguate al rischio esistente, per salvaguardare la sicurezza dei suoi servizi, l'integrità dei dati relativi al traffico, dei dati relativi all'ubicazione e delle comunicazioni elettroniche rispetto ad ogni forma di utilizzazione o cognizione non consentita.

2. Quando la sicurezza del servizio o dei dati personali richiede anche l'adozione di misure che riguardano la rete, il fornitore del servizio di comunicazione elettronica accessibile al pubblico adotta tali misure congiuntamente con il fornitore della rete pubblica di comunicazioni. In caso di mancato accordo, su richiesta di uno dei fornitori, la controversia è definita dall'Autorità per le garanzie nelle comunicazioni secondo le modalità previste dalla normativa vigente.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e, ove possibile, gli utenti, se sussiste un particolare rischio di violazione della sicurezza della rete, indicando, quando il rischio è al di fuori dell'ambito di applicazione delle misure che il fornitore stesso è tenuto ad adottare ai sensi dei commi 1 e 2, tutti i possibili rimedi e i relativi costi presumibili. Analoga informativa è resa al Garante e all'Autorità per le garanzie nelle comunicazioni.

CAPO II - MISURE MINIME DI SICUREZZA

Art. 33. Misure minime

1. Nel quadro dei più generali obblighi di sicurezza di cui all'articolo 31, o previsti da speciali disposizioni, i titolari del trattamento sono comunque tenuti ad adottare le misure minime individuate nel presente capo o ai sensi dell'articolo 58, comma 3, volte ad assicurare un livello minimo di protezione dei dati personali.

Art. 34. Trattamenti con strumenti elettronici

1. Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

a) autenticazione informatica;

b) adozione di procedure di gestione delle credenziali di autenticazione;

c) utilizzazione di un sistema di autorizzazione;
d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
g) tenuta di un aggiornato documento programmatico sulla sicurezza;
h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Art. 35. Trattamenti senza l'ausilio di strumenti elettronici

1. Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:
a) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
b) previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
c) previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

Art. 36. Adeguamento

1. Il disciplinare tecnico di cui all'allegato B), relativo alle misure minime di cui al presente capo, è aggiornato periodicamente con decreto del Ministro della giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore.

TITOLO VI - ADEMPIMENTI

Art. 37. Notificazione del trattamento

1. Il titolare notifica al Garante il trattamento di dati personali cui intende procedere, solo se il trattamento riguarda:
a) dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;
b) dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria;
c) dati idonei a rivelare la vita sessuale o la sfera psichica trattati da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale;
d) dati trattati con l'ausilio di strumenti elettronici volti a definire il profilo o la personalità dell'interessato, o ad analizzare abitudini o scelte di consumo, ovvero a monitorare l'utilizzo di servizi di comunicazione elettronica con esclusione dei trattamenti tecnicamente indispensabili per fornire i servizi medesimi agli utenti;
e) dati sensibili registrati in banche di dati a fini di selezione del personale per conto terzi, nonché dati sensibili utilizzati per sondaggi di opinione, ricerche di mercato e altre ricerche campionarie;
f) dati registrati in apposite banche di dati gestite con strumenti elettronici e relative al rischio sulla solvibilità economica, alla situazione patrimoniale, al corretto adempimento di obbligazioni, a comportamenti illeciti o fraudolenti.

2. Il Garante può individuare altri trattamenti suscettibili di recare pregiudizio ai diritti e alle libertà dell'interessato, in ragione delle relative modalità o della natura dei dati personali, con proprio provvedimento adottato anche ai sensi dell'articolo 17. Con analogo provvedimento pubblicato sulla *Gazzetta Ufficiale* della Repubblica italiana il Garante può anche individuare, nell'ambito dei trattamenti di cui al comma 1, eventuali trattamenti non suscettibili di recare detto pregiudizio e pertanto sottratti all'obbligo di notificazione.

3. La notificazione è effettuata con unico atto anche quando il trattamento comporta il trasferimento all'estero dei dati.

4. Il Garante inserisce le notificazioni ricevute in un registro dei trattamenti accessibile a chiunque e determina le modalità per la sua consultazione gratuita per via telematica, anche mediante convenzioni con soggetti pubblici o presso il proprio Ufficio. Le notizie accessibili tramite la consultazione del registro possono essere trattate per esclusive finalità di applicazione della disciplina in materia di protezione dei dati personali.

Art. 38. Modalità di notificazione

1. La notificazione del trattamento è presentata al Garante prima dell'inizio del trattamento ed una sola volta, a prescindere dal numero delle operazioni e della durata del trattamento da effettuare, e può anche riguardare uno o più trattamenti con finalità correlate.

2. La notificazione è validamente effettuata solo se è trasmessa per via telematica utilizzando il modello predisposto dal Garante e osservando le prescrizioni da questi impartite, anche per quanto riguarda le modalità di sottoscrizione con firma digitale e di conferma del ricevimento della notificazione.

3. Il Garante favorisce la disponibilità del modello per via telematica e la notificazione anche attraverso convenzioni stipulate con soggetti autorizzati in base alla normativa vigente, anche presso associazioni di categoria e ordini professionali.

4. Una nuova notificazione è richiesta solo anteriormente alla cessazione del trattamento o al mutamento di taluno degli elementi da indicare nella notificazione medesima.

5. Il Garante può individuare altro idoneo sistema per la notificazione in riferimento a nuove soluzioni tecnologiche previste dalla normativa vigente.

6. Il titolare del trattamento che non è tenuto alla notificazione al Garante ai sensi dell'articolo 37 fornisce le notizie contenute nel modello di cui al comma 2 a chi ne fa richiesta, salvo che il trattamento riguardi pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

Art. 39. Obblighi di comunicazione

1. Il titolare del trattamento è tenuto a comunicare previamente al Garante le seguenti circostanze:

a) comunicazione di dati personali da parte di un soggetto pubblico ad altro soggetto pubblico non prevista da una norma di legge o di regolamento, effettuata in qualunque forma anche mediante convenzione;

b) trattamento di dati idonei a rivelare lo stato di salute previsto dal programma di ricerca biomedica o sanitaria di cui all'articolo 110, comma 1, primo periodo.

2. I trattamenti oggetto di comunicazione ai sensi del comma 1 possono essere iniziati decorsi quarantacinque giorni dal ricevimento della comunicazione salvo diversa determinazione anche successiva del Garante.

3. La comunicazione di cui al comma 1 è inviata utilizzando il modello predisposto e reso disponibile dal Garante, e trasmessa a quest'ultimo per via telematica osservando le modalità di sottoscrizione con firma digitale e conferma del ricevimento di cui all'articolo 38, comma 2, oppure mediante telefax o lettera raccomandata.

Art. 40. Autorizzazioni generali

1. Le disposizioni del presente codice che prevedono un'autorizzazione del Garante sono applicate anche mediante il rilascio di autorizzazioni relative a determinate categorie di titolari o di trattamenti, pubblicate nella *Gazzetta Ufficiale* della Repubblica italiana.

Art. 41. Richieste di autorizzazione

1. Il titolare del trattamento che rientra nell'ambito di applicazione di un'autorizzazione rilasciata ai sensi dell'articolo 40 non è tenuto a presentare al Garante una richiesta di autorizzazione se il trattamento che intende effettuare è conforme alle relative prescrizioni.

2. Se una richiesta di autorizzazione riguarda un trattamento autorizzato ai sensi dell'articolo 40 il Garante può provvedere comunque sulla richiesta se le specifiche modalità del trattamento lo giustificano.

3. L'eventuale richiesta di autorizzazione è formulata utilizzando esclusivamente il modello predisposto e reso disponibile dal Garante e trasmessa a quest'ultimo per via telematica, osservando le modalità di sottoscrizione e conferma del ricevimento di cui all'articolo 38, comma 2. La medesima richiesta e l'autorizzazione possono essere trasmesse anche mediante telefax o lettera raccomandata.

4. Se il richiedente è invitato dal Garante a fornire informazioni o ad esibire documenti, il termine di quarantacinque giorni di cui all'articolo 26, comma 2, decorre dalla data di scadenza del termine fissato per l'adempimento richiesto.

5. In presenza di particolari circostanze, il Garante può rilasciare un'autorizzazione provvisoria a tempo determinato.

TITOLO VII - TRASFERIMENTO DEI DATI ALL'ESTERO

Art. 42. Trasferimenti all'interno dell'Unione europea

1. Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.

Art. 43. Trasferimenti consentiti in Paesi terzi

1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando:

a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta;

b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato;

c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21;

d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale;

f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia;

g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati;

h) il trattamento concerne dati riguardanti persone giuridiche, enti o associazioni.

Art. 44. Altri trasferimenti consentiti

1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato:

a) individuate dal Garante anche in relazione a garanzie prestate con un contratto;

b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.

Art. 45. Trasferimenti vietati

1. Fuori dei casi di cui agli articoli 43 e 44, il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è vietato quando l'ordinamento del Paese di destinazione o di transito dei dati non assicura un livello di tutela delle persone adeguato. Sono valutate anche le modalità del trasferimento e dei trattamenti previsti, le relative finalità, la natura dei dati e le misure di sicurezza.

PARTE II - DISPOSIZIONI RELATIVE A SPECIFICI SETTORI

TITOLO I - TRATTAMENTI IN AMBITO GIUDIZIARIO

CAPO I - PROFILI GENERALI

Art. 46. Titolari dei trattamenti

1. Gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento.

2. Con decreto del Ministro della giustizia sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, relativamente a banche di dati centrali od oggetto di interconnessione tra più uffici o titolari. I provvedimenti con cui il Consiglio superiore della magistratura e gli altri organi di autogoverno di cui al comma 1 individuano i medesimi trattamenti da essi effettuati sono riportati nell'allegato C) con decreto del Ministro della giustizia.

Art. 47. Trattamenti per ragioni di giustizia

1. In caso di trattamento di dati personali effettuato presso uffici giudiziari di ogni ordine e grado, presso il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia, non si applicano, se il trattamento è effettuato per ragioni di giustizia, le seguenti disposizioni del codice:

a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;

b) articoli da 145 a 151.

2. Agli effetti del presente codice si intendono effettuati per ragioni di giustizia i trattamenti di dati personali direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché le attività ispettive su uffici giudiziari. Le medesime ragioni di giustizia non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla predetta trattazione.

Art. 48. Banche di dati di uffici giudiziari

1. Nei casi in cui l'autorità giudiziaria di ogni ordine e grado può acquisire in conformità alle vigenti disposizioni processuali dati, informazioni, atti e documenti da soggetti pubblici, l'acquisizione può essere effettuata anche per via telematica. A tale fine gli uffici giudiziari possono avvalersi delle convenzioni-tipo stipulate dal Ministero della giustizia con soggetti pubblici, volte ad agevolare la consultazione da parte dei medesimi uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11 del presente codice.

Art. 49. Disposizioni di attuazione

1. Con decreto del Ministro della giustizia sono adottate, anche ad integrazione del decreto del Ministro di grazia e giustizia 30 settembre 1989, n. 334, le disposizioni regolamentari necessarie per l'attuazione dei principi del presente codice nella materia penale e civile.

CAPO II - MINORI

Art. 50. Notizie o immagini relative a minori

1. Il divieto di cui all'articolo 13 del decreto del Presidente della Repubblica 22 settembre 1988, n. 448, di pubblicazione e divulgazione con qualsiasi mezzo di notizie o immagini idonee a consentire l'identificazione di un minore si osserva anche in caso di coinvolgimento a qualunque titolo del minore in procedimenti giudiziari in materie diverse da quella penale.

CAPO III - INFORMATICA GIURIDICA

Art. 51. Principi generali

1. Fermo restando quanto previsto dalle disposizioni processuali concernenti la visione e il rilascio di estratti e di copie di atti e documenti, i dati identificativi delle questioni pendenti dinanzi all'autorità giudiziaria di ogni ordine e grado sono resi accessibili a chi vi abbia interesse anche mediante reti di comunicazione elettronica, ivi compreso il sito istituzionale della medesima autorità nella rete Internet.

2. Le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale della medesima autorità nella rete Internet, osservando le cautele previste dal presente capo.

Art. 52. Dati identificativi degli interessati

1. Fermo restando quanto previsto dalle disposizioni concernenti la redazione e il contenuto di sentenze e di altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado, l'interessato può chiedere per motivi legittimi, con richiesta depositata nella

cancelleria o segreteria dell'ufficio che procede prima che sia definito il relativo grado di giudizio, che sia apposta a cura della medesima cancelleria o segreteria, sull'originale della sentenza o del provvedimento, un'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste giuridiche, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento.

2. Sulla richiesta di cui al comma 1 provvede in calce con decreto, senza ulteriori formalità, l'autorità che pronuncia la sentenza o adotta il provvedimento. La medesima autorità può disporre d'ufficio che sia apposta l'annotazione di cui al comma 1, a tutela dei diritti o della dignità degli interessati.

3. Nei casi di cui ai commi 1 e 2, all'atto del deposito della sentenza o provvedimento, la cancelleria o segreteria vi appone e sottoscrive anche con timbro la seguente annotazione, recante l'indicazione degli estremi del presente articolo: *"In caso di diffusione omettere le generalità e gli altri dati identificativi di ..."*.

4. In caso di diffusione anche da parte di terzi di sentenze o di altri provvedimenti recanti l'annotazione di cui al comma 2, o delle relative massime giuridiche, è omessa l'indicazione delle generalità e degli altri dati identificativi dell'interessato.

5. Fermo restando quanto previsto dall'articolo 734-bis del codice penale relativamente alle persone offese da atti di violenza sessuale, chiunque diffonde sentenze o altri provvedimenti giurisdizionali dell'autorità giudiziaria di ogni ordine e grado è tenuto ad omettere in ogni caso, anche in mancanza dell'annotazione di cui al comma 2, le generalità, altri dati identificativi o altri dati anche relativi a terzi dai quali può desumersi anche indirettamente l'identità di minori, oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone.

6. Le disposizioni di cui al presente articolo si applicano anche in caso di deposito di lodo ai sensi dell'articolo 825 del codice di procedura civile. La parte può formulare agli arbitri la richiesta di cui al comma 1 prima della pronuncia del lodo e gli arbitri appongono sul lodo l'annotazione di cui al comma 3, anche ai sensi del comma 2. Il collegio arbitrale costituito presso la camera arbitrale per i lavori pubblici ai sensi dell'articolo 32 della legge 11 febbraio 1994, n. 109, provvede in modo analogo in caso di richiesta di una parte.

7. Fuori dei casi indicati nel presente articolo è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

TITOLO II - TRATTAMENTI DA PARTE DI FORZE DI POLIZIA

CAPO I - PROFILI GENERALI

Art. 53. Ambito applicativo e titolari dei trattamenti

1. Al trattamento di dati personali effettuato dal Centro elaborazione dati del Dipartimento di pubblica sicurezza o da forze di polizia sui dati destinati a confluirvi in base alla legge, ovvero da organi di pubblica sicurezza o altri soggetti pubblici per finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati, effettuati in base ad espressa disposizione di legge che preveda specificamente il trattamento, non si applicano le seguenti disposizioni del codice:

a) articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5, e da 39 a 45;

b) articoli da 145 a 151.

2. Con decreto del Ministro dell'interno sono individuati, nell'allegato C) al presente codice, i trattamenti non occasionali di cui al comma 1 effettuati con strumenti elettronici, e i relativi titolari.

Art. 54. Modalità di trattamento e flussi di dati

1. Nei casi in cui le autorità di pubblica sicurezza o le forze di polizia possono acquisire in conformità alle vigenti disposizioni di legge o di regolamento dati, informazioni, atti e documenti da altri soggetti, l'acquisizione può essere effettuata anche per via telematica. A tal fine gli organi o uffici interessati possono avvalersi di convenzioni volte ad agevolare la consultazione da parte dei medesimi organi o uffici, mediante reti di comunicazione elettronica, di pubblici registri, elenchi, schedari e banche di dati, nel rispetto delle pertinenti disposizioni e dei principi di cui agli articoli 3 e 11. Le convenzioni-tipo sono adottate dal Ministero dell'interno, su conforme parere del Garante, e stabiliscono le modalità dei collegamenti e degli accessi anche al fine di assicurare l'accesso selettivo ai soli dati necessari al perseguimento delle finalità di cui all'articolo 53.

2. I dati trattati per le finalità di cui al medesimo articolo 53 sono conservati separatamente da quelli registrati per finalità amministrative che non richiedono il loro utilizzo.

3. Fermo restando quanto previsto dall'articolo 11, il Centro elaborazioni dati di cui all'articolo 53 assicura l'aggiornamento periodico e la pertinenza e non eccedenza dei dati personali trattati anche attraverso interrogazioni autorizzate del casellario giudiziale e del casellario dei carichi pendenti del Ministero della giustizia di cui al decreto del Presidente della Repubblica 14 novembre 2002, n. 313, o di altre banche di dati di forze di polizia, necessarie per le finalità di cui all'articolo 53.

4. Gli organi, uffici e comandi di polizia verificano periodicamente i requisiti di cui all'articolo 11 in riferimento ai dati trattati anche senza l'ausilio di strumenti elettronici, e provvedono al loro aggiornamento anche sulla base delle procedure adottate dal Centro elaborazioni dati ai sensi del comma 3, o, per i trattamenti effettuati senza l'ausilio di strumenti elettronici, mediante annotazioni o integrazioni dei documenti che li contengono.

Art. 55. Particolari tecnologie

1. Il trattamento di dati personali che implica maggiori rischi di un danno all'interessato, con particolare riguardo a banche di dati genetici o biometrici, a tecniche basate su dati relativi all'ubicazione, a banche di dati basate su particolari tecniche di elaborazione delle informazioni e all'introduzione di particolari tecnologie, è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17 sulla base di preventiva comunicazione ai sensi dell'articolo 39.

Art. 56. Tutela dell'interessato

1. Le disposizioni di cui all'articolo 10, commi 3, 4 e 5, della legge 1° aprile 1981, n. 121, e successive modificazioni, si applicano anche, oltre che ai dati destinati a confluire nel Centro elaborazione dati di cui all'articolo 53, a dati trattati con l'ausilio di strumenti elettronici da organi, uffici o comandi di polizia.

Art. 57. Disposizioni di attuazione

1. Con decreto del Presidente della Repubblica, previa deliberazione del Consiglio dei ministri, su proposta del Ministro dell'interno, di concerto con il Ministro della giustizia, sono individuate le modalità di attuazione dei principi del presente codice relativamente al trattamento dei dati effettuato per le finalità di cui all'articolo 53 dal Centro elaborazioni dati e da organi, uffici o comandi di polizia, anche ad integrazione e modifica del decreto del Presidente della Repubblica 3 maggio 1982, n. 378, e in attuazione della Raccomandazione R (87) 15 del Consiglio d'Europa del 17 settembre 1987, e successive modificazioni. Le modalità sono individuate con particolare riguardo:

a) al principio secondo cui la raccolta dei dati è correlata alla specifica finalità perseguita, in relazione alla prevenzione di un pericolo concreto o alla repressione di reati, in particolare per quanto riguarda i trattamenti effettuati per finalità di analisi;

b) all'aggiornamento periodico dei dati, anche relativi a valutazioni effettuate in base alla legge, alle diverse modalità relative ai dati trattati senza l'ausilio di strumenti elettronici e alle modalità per rendere conoscibili gli aggiornamenti da parte di altri

organi e uffici cui i dati sono stati in precedenza comunicati;

c) ai presupposti per effettuare trattamenti per esigenze temporanee o collegati a situazioni particolari, anche ai fini della verifica dei requisiti dei dati ai sensi dell'articolo 11, dell'individuazione delle categorie di interessati e della conservazione separata da altri dati che non richiedono il loro utilizzo;

d) all'individuazione di specifici termini di conservazione dei dati in relazione alla natura dei dati o agli strumenti utilizzati per il loro trattamento, nonché alla tipologia dei procedimenti nell'ambito dei quali essi sono trattati o i provvedimenti sono adottati;

e) alla comunicazione ad altri soggetti, anche all'estero o per l'esercizio di un diritto o di un interesse legittimo, e alla loro diffusione, ove necessaria in conformità alla legge;

f) all'uso di particolari tecniche di elaborazione e di ricerca delle informazioni, anche mediante il ricorso a sistemi di indice.

TITOLO III - DIFESA E SICUREZZA DELLO STATO

CAPO I - PROFILI GENERALI

Art. 58. Disposizioni applicabili

1. Ai trattamenti effettuati dagli organismi di cui agli articoli 3, 4 e 6 della legge 24 ottobre 1977, n. 801, ovvero sui dati coperti da segreto di Stato ai sensi dell'articolo 12 della medesima legge, le disposizioni del presente codice si applicano limitatamente a quelle previste negli articoli da 1 a 6, 11, 14, 15, 31, 33, 58, 154, 160 e 169.

2. Ai trattamenti effettuati da soggetti pubblici per finalità di difesa o di sicurezza dello Stato, in base ad espresse disposizioni di legge che prevedano specificamente il trattamento, le disposizioni del presente codice si applicano limitatamente a quelle indicate nel comma 1, nonché alle disposizioni di cui agli articoli 37, 38 e 163.

3. Le misure di sicurezza relative ai dati trattati dagli organismi di cui al comma 1 sono stabilite e periodicamente aggiornate con decreto del Presidente del Consiglio dei ministri, con l'osservanza delle norme che regolano la materia.

4. Con decreto del Presidente del Consiglio dei ministri sono individuate le modalità di applicazione delle disposizioni applicabili del presente codice in riferimento alle tipologie di dati, di interessati, di operazioni di trattamento eseguibili e di incaricati, anche in relazione all'aggiornamento e alla conservazione.

TITOLO IV - TRATTAMENTI IN AMBITO PUBBLICO

CAPO I - ACCESSO A DOCUMENTI AMMINISTRATIVI

Art. 59. Accesso a documenti amministrativi

1. Fatto salvo quanto previsto dall'articolo 60, i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali, e la relativa tutela giurisdizionale, restano disciplinati dalla legge 7 agosto 1990, n. 241, e successive modificazioni e dalle altre disposizioni di legge in materia, nonché dai relativi regolamenti di attuazione, anche per ciò che concerne i tipi di dati sensibili e giudiziari e le operazioni di trattamento eseguibili in esecuzione di una richiesta di accesso. Le attività finalizzate all'applicazione di tale disciplina si considerano di rilevante interesse pubblico.

Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale

1. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai

diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

CAPO II - REGISTRI PUBBLICI ED ALBI PROFESSIONALI

Art. 61. Utilizzazione di dati pubblici

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali provenienti da archivi, registri, elenchi, atti o documenti tenuti da soggetti pubblici, anche individuando i casi in cui deve essere indicata la fonte di acquisizione dei dati e prevedendo garanzie appropriate per l'associazione di dati provenienti da più archivi, tenendo presente quanto previsto dalla Raccomandazione n. R (91)10 del Consiglio d'Europa in relazione all'articolo 11.

2. Agli effetti dell'applicazione del presente codice i dati personali diversi da quelli sensibili o giudiziari, che devono essere inseriti in un albo professionale in conformità alla legge o ad un regolamento, possono essere comunicati a soggetti pubblici e privati o diffusi, ai sensi dell'articolo 19, commi 2 e 3, anche mediante reti di comunicazione elettronica. Può essere altresì menzionata l'esistenza di provvedimenti che dispongono la sospensione o che incidono sull'esercizio della professione.

3. L'ordine o collegio professionale può, a richiesta della persona iscritta nell'albo che vi ha interesse, integrare i dati di cui al comma 2 con ulteriori dati pertinenti e non eccedenti in relazione all'attività professionale.

4. A richiesta dell'interessato l'ordine o collegio professionale può altresì fornire a terzi notizie o informazioni relative, in particolare, a speciali qualificazioni professionali non menzionate nell'albo, ovvero alla disponibilità ad assumere incarichi o a ricevere materiale informativo a carattere scientifico inerente anche a convegni o seminari.

CAPO III - STATO CIVILE, ANAGRAFI E LISTE ELETTORALI

Art. 62. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative alla tenuta degli atti e dei registri dello stato civile, delle anagrafi della popolazione residente in Italia e dei cittadini italiani residenti all'estero, e delle liste elettorali, nonché al rilascio di documenti di riconoscimento o al cambiamento delle generalità.

Art. 63. Consultazione di atti

1. Gli atti dello stato civile conservati negli Archivi di Stato sono consultabili nei limiti previsti dall'articolo 107 del decreto legislativo 29 ottobre 1999, n. 490.

CAPO IV - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 64. Cittadinanza, immigrazione e condizione dello straniero

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di cittadinanza, di immigrazione, di asilo, di condizione dello straniero e del profugo e sullo stato di rifugiato.

2. Nell'ambito delle finalità di cui al comma 1 è ammesso, in particolare, il trattamento dei dati sensibili e giudiziari indispensabili:

a) al rilascio e al rinnovo di visti, permessi, attestazioni, autorizzazioni e documenti anche sanitari;
b) al riconoscimento del diritto di asilo o dello stato di rifugiato, o all'applicazione della protezione temporanea e di altri istituti o misure di carattere umanitario, ovvero all'attuazione di obblighi di legge in materia di politiche migratorie;
c) in relazione agli obblighi dei datori di lavoro e dei lavoratori, ai ricongiungimenti, all'applicazione delle norme vigenti in materia di istruzione e di alloggio, alla partecipazione alla vita pubblica e all'integrazione sociale.

3. Il presente articolo non si applica ai trattamenti di dati sensibili e giudiziari effettuati in esecuzione degli accordi e convenzioni di cui all'articolo 154, comma 2, lettere a) e b), o comunque effettuati per finalità di difesa o di sicurezza dello Stato o di prevenzione, accertamento o repressione dei reati, in base ad espressa disposizione di legge che prevede specificamente il trattamento.

Art. 65. Diritti politici e pubblicità dell'attività di organi

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di:

a) elettorato attivo e passivo e di esercizio di altri diritti politici, nel rispetto della segretezza del voto, nonché di esercizio del mandato degli organi rappresentativi o di tenuta degli elenchi dei giudici popolari;
b) documentazione dell'attività istituzionale di organi pubblici.

2. I trattamenti dei dati sensibili e giudiziari per le finalità di cui al comma 1 sono consentiti per eseguire specifici compiti previsti da leggi o da regolamenti fra i quali, in particolare, quelli concernenti:

a) lo svolgimento di consultazioni elettorali e la verifica della relativa regolarità;
b) le richieste di *referendum*, le relative consultazioni e la verifica delle relative regolarità;
c) l'accertamento delle cause di ineleggibilità, incompatibilità o di decadenza, o di rimozione o sospensione da cariche pubbliche, ovvero di sospensione o di scioglimento degli organi;
d) l'esame di segnalazioni, petizioni, appelli e di proposte di legge di iniziativa popolare, l'attività di commissioni di inchiesta, il rapporto con gruppi politici;
e) la designazione e la nomina di rappresentanti in commissioni, enti e uffici.

3. Ai fini del presente articolo, è consentita la diffusione dei dati sensibili e giudiziari per le finalità di cui al comma 1, lettera a), in particolare con riguardo alle sottoscrizioni di liste, alla presentazione delle candidature, agli incarichi in organizzazioni o associazioni politiche, alle cariche istituzionali e agli organi eletti.

4. Ai fini del presente articolo, in particolare, è consentito il trattamento di dati sensibili e giudiziari indispensabili:

a) per la redazione di verbali e resoconti dell'attività di assemblee rappresentative, commissioni e di altri organi collegiali o assembleari;
b) per l'esclusivo svolgimento di una funzione di controllo, di indirizzo politico o di sindacato ispettivo e per l'accesso a documenti riconosciuto dalla legge e dai regolamenti degli organi interessati per esclusive finalità direttamente connesse all'espletamento di un mandato elettivo.

5. I dati sensibili e giudiziari trattati per le finalità di cui al comma 1 possono essere comunicati e diffusi nelle forme previste dai rispettivi ordinamenti. Non è comunque consentita la divulgazione dei dati sensibili e giudiziari che non risultano indispensabili per assicurare il rispetto del principio di pubblicità dell'attività istituzionale, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 66. Materia tributaria e doganale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dei soggetti pubblici dirette all' applicazione, anche tramite i loro concessionari, delle disposizioni in materia di tributi, in relazione ai contribuenti, ai sostituti e ai responsabili di imposta, nonché in materia di deduzioni e detrazioni e per l'applicazione delle disposizioni la cui esecuzione è affidata alle dogane.

2. Si considerano inoltre di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le attività dirette, in materia di imposte, alla prevenzione e repressione delle violazioni degli obblighi e alla adozione dei provvedimenti previsti da leggi, regolamenti o dalla normativa comunitaria, nonché al controllo e alla esecuzione forzata dell'esatto adempimento di tali

obblighi, alla effettuazione dei rimborsi, alla destinazione di quote d'imposta, e quelle dirette alla gestione ed alienazione di immobili statali, all'inventario e alla qualificazione degli immobili e alla conservazione dei registri immobiliari.

Art. 67. Attività di controllo e ispettive

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di:
   a) verifica della legittimità, del buon andamento, dell'imparzialità dell'attività amministrativa, nonché della rispondenza di detta attività a requisiti di razionalità, economicità, efficienza ed efficacia per le quali sono, comunque, attribuite dalla legge a soggetti pubblici funzioni di controllo, di riscontro ed ispettive nei confronti di altri soggetti;
   b) accertamento, nei limiti delle finalità istituzionali, con riferimento a dati sensibili e giudiziari relativi ad esposti e petizioni, ovvero ad atti di controllo o di sindacato ispettivo di cui all'articolo 65, comma 4.

Art. 68. Benefici economici ed abilitazioni

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni.

2. Si intendono ricompresi fra i trattamenti regolati dal presente articolo anche quelli indispensabili in relazione:
   a) alle comunicazioni, certificazioni ed informazioni previste dalla normativa antimafia;
   b) alle elargizioni di contributi previsti dalla normativa in materia di usura e di vittime di richieste estorsive;
   c) alla corresponsione delle pensioni di guerra o al riconoscimento di benefici in favore di perseguitati politici e di internati in campo di sterminio e di loro congiunti;
   d) al riconoscimento di benefici connessi all'invalidità civile;
   e) alla concessione di contributi in materia di formazione professionale;
   f) alla concessione di contributi, finanziamenti, elargizioni ed altri benefici previsti dalla legge, dai regolamenti o dalla normativa comunitaria, anche in favore di associazioni, fondazioni ed enti;
   g) al riconoscimento di esoneri, agevolazioni o riduzioni tariffarie o economiche, franchigie, o al rilascio di concessioni anche radiotelevisive, licenze, autorizzazioni, iscrizioni ed altri titoli abilitativi previsti dalla legge, da un regolamento o dalla normativa comunitaria.

3. Il trattamento può comprendere la diffusione nei soli casi in cui ciò è indispensabile per la trasparenza delle attività indicate nel presente articolo, in conformità alle leggi, e per finalità di vigilanza e di controllo conseguenti alle attività medesime, fermo restando il divieto di diffusione dei dati idonei a rivelare lo stato di salute.

Art. 69. Onorificenze, ricompense e riconoscimenti

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di applicazione della disciplina in materia di conferimento di onorificenze e ricompense, di riconoscimento della personalità giuridica di associazioni, fondazioni ed enti, anche di culto, di accertamento dei requisiti di onorabilità e di professionalità per le nomine, per i profili di competenza del soggetto pubblico, ad uffici anche di culto e a cariche direttive di persone giuridiche, imprese e di istituzioni scolastiche non statali, nonché di rilascio e revoca di autorizzazioni o abilitazioni, di concessione di patrocini, patronati e premi di rappresentanza, di adesione a comitati d'onore e di ammissione a cerimonie ed incontri istituzionali.

Art. 70. Volontariato e obiezione di coscienza

1. Si considerano di rilevante interesse pubblico, ai sensi dell'articolo 20 e 21, le finalità

di applicazione della disciplina in materia di rapporti tra i soggetti pubblici e le organizzazioni di volontariato, in particolare per quanto riguarda l'elargizione di contributi finalizzati al loro sostegno, la tenuta di registri generali delle medesime organizzazioni e la cooperazione internazionale.

2. Si considerano, altresì, di rilevante interesse pubblico le finalità di applicazione della legge 8 luglio 1998, n. 230, e delle altre disposizioni di legge in materia di obiezione di coscienza.

Art. 71. Attività sanzionatorie e di tutela

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità:
   a) di applicazione delle norme in materia di sanzioni amministrative e ricorsi;
   b) volte a far valere il diritto di difesa in sede amministrativa o giudiziaria, anche da parte di un terzo, anche ai sensi dell'articolo 391-*quater* del codice di procedura penale, o direttamente connesse alla riparazione di un errore giudiziario o in caso di violazione del termine ragionevole del processo o di un'ingiusta restrizione della libertà personale.

2. Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se il diritto da far valere o difendere, di cui alla lettera b) del comma 1, è di rango almeno pari a quello dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 72. Rapporti con enti di culto

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative allo svolgimento dei rapporti istituzionali con enti di culto, confessioni religiose e comunità religiose.

Art. 73. Altre finalità in ambito amministrativo e sociale

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità socio-assistenziali, con particolare riferimento a:
   a) interventi di sostegno psico-sociale e di formazione in favore di giovani o di altri soggetti che versano in condizioni di disagio sociale, economico o familiare;
   b) interventi anche di rilievo sanitario in favore di soggetti bisognosi o non autosufficienti o incapaci, ivi compresi i servizi di assistenza economica o domiciliare, di telesoccorso, accompagnamento e trasporto;
   c) assistenza nei confronti di minori, anche in relazione a vicende giudiziarie;
   d) indagini psico-sociali relative a provvedimenti di adozione anche internazionale;
   e) compiti di vigilanza per affidamenti temporanei;
   f) iniziative di vigilanza e di sostegno in riferimento al soggiorno di nomadi;
   g) interventi in tema di barriere architettoniche.

2. Si considerano, altresì, di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, nell'ambito delle attività che la legge demanda ad un soggetto pubblico, le finalità:
   a) di gestione di asili nido;
   b) concernenti la gestione di mense scolastiche o la fornitura di sussidi, contributi e materiale didattico;
   c) ricreative o di promozione della cultura e dello sport, con particolare riferimento all'organizzazione di soggiorni, mostre, conferenze e manifestazioni sportive o all'uso di beni immobili o all'occupazione di suolo pubblico;
   d) di assegnazione di alloggi di edilizia residenziale pubblica;
   e) relative alla leva militare;
   f) di polizia amministrativa anche locale, salvo quanto previsto dall'articolo 53, con particolare riferimento ai servizi di igiene, di polizia mortuaria e ai controlli in materia di ambiente, tutela delle risorse idriche e difesa del suolo;
   g) degli uffici per le relazioni con il pubblico;

h) in materia di protezione civile;
i) di supporto al collocamento e all'avviamento al lavoro, in particolare a cura di centri di iniziativa locale per l'occupazione e di sportelli-lavoro;
l) dei difensori civici regionali e locali.

CAPO V - PARTICOLARI CONTRASSEGNI

Art. 74. Contrassegni su veicoli e accessi a centri storici

1. I contrassegni rilasciati a qualunque titolo per la circolazione e la sosta di veicoli a servizio di persone invalide, ovvero per il transito e la sosta in zone a traffico limitato, e che devono essere esposti su veicoli, contengono i soli dati indispensabili ad individuare l'autorizzazione rilasciata e senza l'apposizione di simboli o diciture dai quali può desumersi la speciale natura dell'autorizzazione per effetto della sola visione del contrassegno.

2. Le generalità e l'indirizzo della persona fisica interessata sono riportati sui contrassegni con modalità che non consentono, parimenti, la loro diretta visibilità se non in caso di richiesta di esibizione o necessità di accertamento.

3. La disposizione di cui al comma 2 si applica anche in caso di fissazione a qualunque titolo di un obbligo di esposizione sui veicoli di copia del libretto di circolazione o di altro documento.

4. Per il trattamento dei dati raccolti mediante impianti per la rilevazione degli accessi di veicoli ai centri storici ed alle zone a traffico limitato continuano, altresì, ad applicarsi le disposizioni del decreto del Presidente della Repubblica 22 giugno 1999, n. 250.

TITOLO V - TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

CAPO I - PRINCIPI GENERALI

Art. 75. Ambito applicativo

1. Il presente titolo disciplina il trattamento dei dati personali in ambito sanitario.

Art. 76. Esercenti professioni sanitarie e organismi sanitari pubblici

1. Gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, anche nell'ambito di un'attività di rilevante interesse pubblico ai sensi dell'articolo 85, trattano i dati personali idonei a rivelare lo stato di salute:
a) con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;
b) anche senza il consenso dell'interessato e previa autorizzazione del Garante, se la finalità di cui alla lettera a) riguarda un terzo o la collettività.

2. Nei casi di cui al comma 1 il consenso può essere prestato con le modalità semplificate di cui al capo II.

3. Nei casi di cui al comma 1 l'autorizzazione del Garante è rilasciata, salvi i casi di particolare urgenza, sentito il Consiglio superiore di sanità.

CAPO II - MODALITÀ SEMPLIFICATE PER INFORMATIVA E CONSENSO

Art. 77. Casi di semplificazione

1. Il presente capo individua modalità semplificate utilizzabili dai soggetti di cui al comma 2:
a) per informare l'interessato relativamente ai dati personali raccolti presso il medesimo interessato o presso terzi, ai sensi dell'articolo 13, commi 1 e 4;
b) per manifestare il consenso al trattamento dei dati personali nei casi in cui ciò è richiesto ai sensi dell'articolo 76;

c) per il trattamento dei dati personali.

2. Le modalità semplificate di cui al comma 1 sono applicabili:
a) dagli organismi sanitari pubblici;
b) dagli altri organismi privati e dagli esercenti le professioni sanitarie;
c) dagli altri soggetti pubblici indicati nell'articolo 80.

Art. 78. Informativa del medico di medicina generale o del pediatra

1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1.

2. L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

3. L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'articolo 13, comma 3, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.

4. L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:
a) sostituisce temporaneamente il medico o il pediatra;
b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;
c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;
d) fornisce farmaci prescritti;
e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

5. L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:
a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;
b) nell'ambito della teleassistenza o telemedicina;
c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica.

Art. 79. Informativa da parte di organismi sanitari

1. Gli organismi sanitari pubblici e privati possono avvalersi delle modalità semplificate relative all'informativa e al consenso di cui agli articoli 78 e 81 in riferimento ad una pluralità di prestazioni erogate anche da distinti reparti ed unità dello stesso organismo o di più strutture ospedaliere o territoriali specificamente identificati.

2. Nei casi di cui al comma 1 l'organismo o le strutture annotano l'avvenuta informativa e il consenso con modalità uniformi e tali da permettere una verifica al riguardo da parte di altri reparti ed unità che, anche in tempi diversi, trattano dati relativi al medesimo interessato.

3. Le modalità semplificate di cui agli articoli 78 e 81 possono essere utilizzate in modo omogeneo e coordinato in riferimento all'insieme dei trattamenti di dati personali effettuati nel complesso delle strutture facenti capo alle aziende sanitarie.

4. Sulla base di adeguate misure organizzative in applicazione del comma 3, le modalità semplificate possono essere utilizzate per più trattamenti di dati effettuati nei casi di cui al presente articolo e dai soggetti di cui all'articolo 80.

Art. 80. Informativa da parte di altri soggetti pubblici

1. Oltre a quanto previsto dall'articolo 79, possono avvalersi della facoltà di fornire un'unica informativa per una pluralità di trattamenti di dati effettuati, a fini amministrativi e in tempi diversi, rispetto a dati raccolti presso l'interessato e presso terzi, i competenti servizi o strutture di soggetti pubblici operanti in ambito sanitario o della prevenzione e sicurezza del lavoro.

2. L'informativa di cui al comma 1 è integrata con appositi e idonei cartelli ed avvisi agevolmente visibili al pubblico, affissi e diffusi anche nell'ambito di pubblicazioni istituzionali e mediante reti di comunicazione elettronica, in particolare per quanto riguarda attività amministrative di rilevante interesse pubblico che non richiedono il consenso degli interessati.

Art. 81. Prestazione del consenso

1. Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, nei casi in cui è necessario ai sensi del presente codice o di altra disposizione di legge, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato, nei modi indicati negli articoli 78, 79 e 80.

2. Quando il medico o il pediatra fornisce l'informativa per conto di più professionisti ai sensi dell'articolo 78, comma 4, oltre quanto previsto dal comma 1, il consenso è reso conoscibile ai medesimi professionisti con adeguate modalità, anche attraverso menzione, annotazione o apposizione di un bollino o tagliando su una carta elettronica o sulla tessera sanitaria, contenente un richiamo al medesimo articolo 78, comma 4, e alle eventuali diverse specificazioni apposte all'informativa ai sensi del medesimo comma.

Art. 82. Emergenze e tutela della salute e dell'incolumità fisica

1. L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, nel caso di emergenza sanitaria o di igiene pubblica per la quale la competente autorità ha adottato un'ordinanza contingibile ed urgente ai sensi dell'articolo 117 del decreto legislativo 31 marzo 1998, n. 112.

2. L'informativa e il consenso al trattamento dei dati personali possono altresì intervenire senza ritardo, successivamente alla prestazione, in caso di:

a) impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;

b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato.

3. L'informativa e il consenso al trattamento dei dati personali possono intervenire senza ritardo, successivamente alla prestazione, anche in caso di prestazione medica che può essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia.

4. Dopo il raggiungimento della maggiore età l'informativa è fornita all'interessato anche ai fini della acquisizione di una nuova manifestazione del consenso quando questo è necessario.

Art. 83. Altre misure per il rispetto dei diritti degli interessati

1. I soggetti di cui agli articoli 78, 79 e 80 adottano idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.

2. Le misure di cui al comma 1 comprendono, in particolare:

a) soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;

b) l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;

c) soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;

d) cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

e) il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;

f) la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;

g) la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;

h) la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;

i) la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

Art. 84. Comunicazione di dati all'interessato

1. I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato.

2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati.

CAPO III - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 85. Compiti del Servizio sanitario nazionale

1. Fuori dei casi di cui al comma 2, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità che rientrano nei compiti del Servizio sanitario nazionale e degli altri organismi sanitari pubblici relative alle seguenti attività:

a) attività amministrative correlate a quelle di prevenzione, diagnosi, cura e riabilitazione dei soggetti assistiti dal Servizio sanitario nazionale, ivi compresa l'assistenza degli stranieri in Italia e dei cittadini italiani all'estero, nonché di assistenza sanitaria erogata al personale navigante ed aeroportuale;

b) programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;

c) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria;
d) attività certificatorie;
e) l'applicazione della normativa in materia di igiene e sicurezza nei luoghi di lavoro e di sicurezza e salute della popolazione;
f) le attività amministrative correlate ai trapianti d'organo e di tessuti, nonché alle trasfusioni di sangue umano, anche in applicazione della legge 4 maggio 1990, n. 107;
g) instaurazione, gestione, pianificazione e controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati del Servizio sanitario nazionale.

2. Il comma 1 non si applica ai trattamenti di dati idonei a rivelare lo stato di salute effettuati da esercenti le professioni sanitarie o da organismi sanitari pubblici per finalità di tutela della salute o dell'incolumità fisica dell'interessato, di un terzo o della collettività, per i quali si osservano le disposizioni relative al consenso dell'interessato o all'autorizzazione del Garante ai sensi dell'articolo 76.

3. All'identificazione dei tipi di dati idonei a rivelare lo stato di salute e di operazioni su essi eseguibili è assicurata ampia pubblicità, anche tramite affissione di una copia o di una guida illustrativa presso ciascuna azienda sanitaria e presso gli studi dei medici di medicina generale e dei pediatri di libera scelta.

4. Il trattamento di dati identificativi dell'interessato è lecito da parte dei soli soggetti che perseguono direttamente le finalità di cui al comma 1. L'utilizzazione delle diverse tipologie di dati è consentita ai soli incaricati, preposti, caso per caso, alle specifiche fasi delle attività di cui al medesimo comma, secondo il principio dell'indispensabilità dei dati di volta in volta trattati.

Art. 86. Altre finalità di rilevante interesse pubblico

1. Fuori dei casi di cui agli articoli 76 e 85, si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità, perseguite mediante trattamento di dati sensibili e giudiziari, relative alle attività amministrative correlate all'applicazione della disciplina in materia di:
a) tutela sociale della maternità e di interruzione volontaria della gravidanza, con particolare riferimento a quelle svolte per la gestione di consultori familiari e istituzioni analoghe, per l'informazione, la cura e la degenza delle madri, nonché per gli interventi di interruzione della gravidanza;
b) stupefacenti e sostanze psicotrope, con particolare riferimento a quelle svolte al fine di assicurare, anche avvalendosi di enti ed associazioni senza fine di lucro, i servizi pubblici necessari per l'assistenza socio-sanitaria ai tossicodipendenti, gli interventi anche di tipo preventivo previsti dalle leggi e l'applicazione delle misure amministrative previste;
c) assistenza, integrazione sociale e diritti delle persone handicappate effettuati, in particolare, al fine di:
   1) accertare l'handicap ed assicurare la funzionalità dei servizi terapeutici e riabilitativi, di aiuto personale e familiare, nonché interventi economici integrativi ed altre agevolazioni;
   2) curare l'integrazione sociale, l'educazione, l'istruzione e l'informazione alla famiglia del portatore di handicap, nonché il collocamento obbligatorio nei casi previsti dalla legge;
   3) realizzare comunità-alloggio e centri socio riabilitativi;
   4) curare la tenuta degli albi degli enti e delle associazioni ed organizzazioni di volontariato impegnati nel settore.

2. Ai trattamenti di cui al presente articolo si applicano le disposizioni di cui all'articolo 85, comma 4.

CAPO IV - PRESCRIZIONI MEDICHE

Art. 87. Medicinali a carico del Servizio sanitario nazionale

1. Le ricette relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale sono redatte secondo il modello di cui al comma 2, conformato in modo da permettere di risalire all'identità dell'interessato solo in caso di necessità connesse al controllo della correttezza della prescrizione, ovvero a fini di verifiche amministrative o per scopi epidemiologici e di ricerca, nel rispetto delle norme deontologiche applicabili.

2. Il modello cartaceo per le ricette di medicinali relative a prescrizioni di medicinali a carico, anche parziale, del Servizio sanitario nazionale, di cui agli allegati 1, 3, 5 e 6 del decreto del Ministro della sanità 11 luglio 1988, n. 350, e al capitolo 2, paragrafo 2.2.2. del relativo disciplinare tecnico, è integrato da un tagliando predisposto su carta o con tecnica di tipo copiativo e unito ai bordi delle zone indicate nel comma 3.

3. Il tagliando di cui al comma 2 è apposto sulle zone del modello predisposte per l'indicazione delle generalità e dell'indirizzo dell'assistito, in modo da consentirne la visione solo per effetto di una momentanea separazione del tagliando medesimo che risulti necessaria ai sensi dei commi 4 e 5.

4. Il tagliando può essere momentaneamente separato dal modello di ricetta, e successivamente riunito allo stesso, quando il farmacista lo ritiene indispensabile, mediante sottoscrizione apposta sul tagliando, per una effettiva necessità connessa al controllo della correttezza della prescrizione, anche per quanto riguarda la corretta fornitura del farmaco.

5. Il tagliando può essere momentaneamente separato nei modi di cui al comma 3 anche presso i competenti organi per fini di verifica amministrativa sulla correttezza della prescrizione, o da parte di soggetti legittimati a svolgere indagini epidemiologiche o di ricerca in conformità alla legge, quando è indispensabile per il perseguimento delle rispettive finalità.

6. Con decreto del Ministro della salute, sentito il Garante, può essere individuata una ulteriore soluzione tecnica diversa da quella indicata nel comma 1, basata sull'uso di una fascetta adesiva o su altra tecnica equipollente relativa anche a modelli non cartacei.

Art. 88. Medicinali non a carico del Servizio sanitario nazionale

1. Nelle prescrizioni cartacee di medicinali soggetti a prescrizione ripetibile non a carico, anche parziale, del Servizio sanitario nazionale, le generalità dell'interessato non sono indicate.

2. Nei casi di cui al comma 1 il medico può indicare le generalità dell'interessato solo se ritiene indispensabile permettere di risalire alla sua identità, per un'effettiva necessità derivante dalle particolari condizioni del medesimo interessato o da una speciale modalità di preparazione o di utilizzazione.

Art. 89. Casi particolari

1. Le disposizioni del presente capo non precludono l'applicazione di disposizioni normative che prevedono il rilascio di ricette che non identificano l'interessato o recanti particolari annotazioni, contenute anche nel decreto-legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94.

2. Nei casi in cui deve essere accertata l'identità dell'interessato ai sensi del testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni, le ricette sono conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.

CAPO V - DATI GENETICI

Art. 90. Trattamento dei dati genetici e donatori di midollo osseo

1. Il trattamento dei dati genetici da chiunque effettuato è consentito nei soli casi previsti da apposita autorizzazione rilasciata dal Garante sentito il Ministro della salute, che acquisisce, a tal fine, il parere del Consiglio superiore di sanità.

2. L'autorizzazione di cui al comma 1 individua anche gli ulteriori elementi da includere nell'informativa ai sensi dell'articolo 13, con particolare riguardo alla specificazione delle finalità perseguite e dei risultati conseguibili anche in relazione alle notizie inattese che possono essere conosciute per effetto del trattamento dei dati e al diritto di opporsi al medesimo trattamento per motivi legittimi.

3. Il donatore di midollo osseo, ai sensi della legge 6 marzo 2001, n. 52, ha il diritto e il dovere di mantenere l'anonimato sia nei confronti del ricevente sia nei confronti di terzi.

CAPO VI - DISPOSIZIONI VARIE

Art. 91. Dati trattati mediante carte

1. Il trattamento in ogni forma di dati idonei a rivelare lo stato di salute o la vita sessuale eventualmente registrati su carte anche non elettroniche, compresa la carta nazionale dei servizi, o trattati mediante le medesime carte è consentito se necessario ai sensi dell'articolo 3, nell'osservanza di misure ed accorgimenti prescritti dal Garante nei modi di cui all'articolo 17.

Art. 92. Cartelle cliniche

1. Nei casi in cui organismi sanitari pubblici e privati redigono e conservano una cartella clinica in conformità alla disciplina applicabile, sono adottati opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati, ivi comprese informazioni relative a nascituri.

2. Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Art. 93. Certificato di assistenza al parto

1. Ai fini della dichiarazione di nascita il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita. Si osservano, altresì, le disposizioni dell'articolo 109.

2. Il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendono identificabile la madre che abbia dichiarato di non voler essere nominata avvalendosi della facoltà di cui all'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento.

3. Durante il periodo di cui al comma 2 la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati relativi alla madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art. 94. Banche di dati, registri e schedari in ambito sanitario

1. Il trattamento di dati idonei a rivelare lo stato di salute contenuti in banche di dati, schedari, archivi o registri tenuti in ambito sanitario, è effettuato nel rispetto dell'articolo 3 anche presso banche di dati, schedari, archivi o registri già istituiti alla data di entrata in vigore del presente codice e in riferimento ad accessi di terzi previsti dalla disciplina vigente alla medesima data, in particolare presso:

a) il registro nazionale dei casi di mesotelioma asbesto-correlati istituito presso l'Istituto superiore per la prevenzione e la sicurezza del lavoro (Ispesl), di cui all'articolo 1 del decreto del Presidente del Consiglio dei ministri 10 dicembre 2002, n. 308;

b) la banca di dati in materia di sorveglianza della malattia di Creutzfeldt-Jakob o delle varianti e sindromi ad essa correlate, di cui al decreto del Ministro della salute in data 21 dicembre 2001, pubblicato nella *Gazzetta Ufficiale* n. 8 del 10 gennaio 2002;

c) il registro nazionale delle malattie rare di cui all'articolo 3 del decreto del Ministro della sanità in data 18 maggio 2001, n. 279;

d) i registri dei donatori di midollo osseo istituiti in applicazione della legge 6 marzo 2001, n. 52;

e) gli schedari dei donatori di sangue di cui all'articolo 15 del decreto del Ministro della sanità in data 26 gennaio 2001, pubblicato nella *Gazzetta Ufficiale* n. 78 del 3 aprile 2001.

TITOLO VI - ISTRUZIONE

CAPO I - PROFILI GENERALI

Art. 95. Dati sensibili e giudiziari

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario, con particolare riferimento a quelle svolte anche in forma integrata.

Art. 96. Trattamento di dati relativi a studenti

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

TITOLO VII - TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI

CAPO I - PROFILI GENERALI

Art. 97. Ambito applicativo

1. Il presente titolo disciplina il trattamento dei dati personali effettuato per scopi storici, statistici o scientifici.

Art. 98. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità relative ai trattamenti effettuati da soggetti pubblici:

a) per scopi storici, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato e negli archivi storici degli enti pubblici, secondo quanto disposto dal decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice;
b) che fanno parte del Sistema statistico nazionale (Sistan) ai sensi del decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni;
c) per scopi scientifici.

Art. 99. Compatibilità tra scopi e durata del trattamento

1. Il trattamento di dati personali effettuato per scopi storici, statistici o scientifici è considerato compatibile con i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. Il trattamento di dati personali per scopi storici, statistici o scientifici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

3. Per scopi storici, statistici o scientifici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento.

Art. 100. Dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli sensibili o giudiziari.

2. Resta fermo il diritto dell'interessato di opporsi per motivi legittimi ai sensi dell'articolo 7, comma 4, lettera a).

3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della legge 7 agosto 1990, n. 241.

4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

CAPO II - TRATTAMENTO PER SCOPI STORICI

Art. 101. Modalità di trattamento

1. I dati personali raccolti per scopi storici non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 11.

2. I documenti contenenti dati personali, trattati per scopi storici, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.

3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

Art. 102. Codice di deontologia e di buona condotta

1. Il Garante promuove ai sensi dell'articolo 12 la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici.

2. Il codice di deontologia e di buona condotta di cui al comma 1 individua, in particolare:
   a) le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del presente codice applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica;
   b) le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati;
   c) le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a scopi storici, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 103. Consultazione di documenti conservati in archivi

1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati è disciplinata dal decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, come modificato dal presente codice.

CAPO III - TRATTAMENTO PER SCOPI STATISTICI O SCIENTIFICI

Art. 104. Ambito applicativo e dati identificativi per scopi statistici o scientifici

1. Le disposizioni del presente capo si applicano ai trattamenti di dati per scopi statistici o, in quanto compatibili, per scopi scientifici.

2. Agli effetti dell'applicazione del presente capo, in relazione ai dati identificativi si tiene conto dell'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare o da altri per identificare l'interessato, anche in base alle conoscenze acquisite in relazione al progresso tecnico.

Art. 105. Modalità di trattamento

1. I dati personali trattati per scopi statistici o scientifici non possono essere utilizzati per prendere decisioni o provvedimenti relativamente all'interessato, né per trattamenti di dati per scopi di altra natura.

2. Gli scopi statistici o scientifici devono essere chiaramente determinati e resi noti all'interessato, nei modi di cui all'articolo 13 anche in relazione a quanto previsto dall'articolo 106, comma 2, lettera b), del presente codice e dall'articolo 6-*bis* del decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni.

3. Quando specifiche circostanze individuate dai codici di cui all'articolo 106 sono tali da consentire ad un soggetto di rispondere in nome e per conto di un altro, in quanto familiare o convivente, l'informativa all'interessato può essere data anche per il tramite del soggetto rispondente.

4. Per il trattamento effettuato per scopi statistici o scientifici rispetto a dati raccolti per altri scopi, l'informativa all'interessato non è dovuta quando richiede uno sforzo sproporzionato rispetto al diritto tutelato, se sono adottate le idonee forme di pubblicità individuate dai codici di cui all'articolo 106.

Art. 106. Codici di deontologia e di buona condotta

1. Il Garante promuove ai sensi dell'articolo 12 la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi statistici o scientifici.

2. Con i codici di cui al comma 1 sono individuati, tenendo conto, per i soggetti già compresi nell'ambito del Sistema statistico nazionale, di quanto già previsto dal decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni, e, per altri soggetti, sulla base di analoghe garanzie, in particolare:

a) i presupposti e i procedimenti per documentare e verificare che i trattamenti, fuori dai casi previsti dal medesimo decreto legislativo n. 322 del 1989, siano effettuati per idonei ed effettivi scopi statistici o scientifici;

b) per quanto non previsto dal presente codice, gli ulteriori presupposti del trattamento e le connesse garanzie, anche in riferimento alla durata della conservazione dei dati, alle informazioni da rendere agli interessati relativamente ai dati raccolti anche presso terzi, alla comunicazione e diffusione, ai criteri selettivi da osservare per il trattamento di dati identificativi, alle specifiche misure di sicurezza e alle modalità per la modifica dei dati a seguito dell'esercizio dei diritti dell'interessato, tenendo conto dei principi contenuti nelle pertinenti raccomandazioni del Consiglio d'Europa;

c) l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare del trattamento o da altri per identificare l'interessato, anche in relazione alle conoscenze acquisite in base al progresso tecnico;

d) le garanzie da osservare ai fini dell'applicazione delle disposizioni di cui all'articolo 24, comma 1, lettera i), e 43, comma 1, lettera g), che permettono di prescindere dal consenso dell'interessato, tenendo conto dei principi contenuti nelle predette raccomandazioni;

e) modalità semplificate per la prestazione del consenso degli interessati relativamente al trattamento dei dati sensibili;

f) le regole di correttezza da osservare nella raccolta dei dati e le istruzioni da impartire al personale incaricato;

g) le misure da adottare per favorire il rispetto dei principi di pertinenza e non eccedenza dei dati e delle misure di sicurezza di cui all'articolo 31, anche in riferimento alle cautele volte ad impedire l'accesso da parte di persone fisiche che non sono incaricati e l'identificazione non autorizzata degli interessati, all'interconnessione dei sistemi informativi anche nell'ambito del Sistema statistico nazionale e all'interscambio di dati per scopi statistici o scientifici da effettuarsi con enti ed uffici situati all'estero anche sulla base delle garanzie previste dall'articolo 44, comma 1, lettera a);

h) l'impegno al rispetto di regole di condotta degli incaricati che non sono tenuti in base alla legge al segreto d'ufficio o professionale, tali da assicurare analoghi livelli di sicurezza e di riservatezza.

Art. 107. Trattamento di dati sensibili

1. Fermo restando quanto previsto dall'articolo 20 e fuori dei casi di particolari indagini statistiche o di ricerca scientifica previste dalla legge, il consenso dell'interessato al trattamento di dati sensibili, quando è richiesto, può essere prestato con modalità semplificate, individuate dal codice di cui all'articolo 106 e l'autorizzazione del Garante può essere rilasciata anche ai sensi dell'articolo 40.

Art. 108. Sistema statistico nazionale

1. Il trattamento di dati personali da parte di soggetti che fanno parte del Sistema statistico nazionale, oltre a quanto previsto dal codice di deontologia e di buona condotta sottoscritto ai sensi dell'articolo 106, comma 2, resta inoltre disciplinato dal decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni, in particolare per quanto riguarda il trattamento dei dati sensibili indicati nel Programma statistico nazionale, l'informativa all'interessato, l'esercizio dei relativi diritti e i dati non tutelati dal segreto statistico ai sensi dell'articolo 9, comma 4, del medesimo decreto.

Art. 109. Dati statistici relativi all'evento della nascita

1. Per la rilevazione dei dati statistici relativi agli eventi di nascita, compresi quelli relativi ai nati affetti da malformazioni e ai nati morti, nonché per i flussi di dati anche da parte

di direttori sanitari, si osservano, oltre alle disposizioni di cui al decreto del Ministro della sanità 16 luglio 2001, n. 349, le modalità tecniche determinate dall'Istituto nazionale della statistica, sentito il Ministro della salute, dell'interno e il Garante.

Art. 110. Ricerca medica, biomedica ed epidemiologica

1. Il consenso dell'interessato per il trattamento dei dati idonei a rivelare lo stato di salute, finalizzato a scopi di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è prevista da un'espressa disposizione di legge che prevede specificamente il trattamento, ovvero rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del decreto legislativo 30 dicembre 1992, n. 502, e successive modificazioni, e per il quale sono decorsi quarantacinque giorni dalla comunicazione al Garante ai sensi dell'articolo 39. Il consenso non è inoltre necessario quando a causa di particolari ragioni non è possibile informare gli interessati e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale ed è autorizzato dal Garante anche ai sensi dell'articolo 40.

2. In caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 7 nei riguardi dei trattamenti di cui al comma 1, l'aggiornamento, la rettificazione e l'integrazione dei dati sono annotati senza modificare questi ultimi, quando il risultato di tali operazioni non produce effetti significativi sul risultato della ricerca.

TITOLO VIII - LAVORO E PREVIDENZA SOCIALE

CAPO I - PROFILI GENERALI

Art. 111. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato per finalità previdenziali o per la gestione del rapporto di lavoro, prevedendo anche specifiche modalità per l'informativa all'interessato e per l'eventuale prestazione del consenso relativamente alla pubblicazione degli annunci per finalità di occupazione di cui all'articolo 113, comma 3 e alla ricezione di *curricula* contenenti dati personali anche sensibili.

Art. 112. Finalità di rilevante interesse pubblico

1. Si considerano di rilevante interesse pubblico, ai sensi degli articoli 20 e 21, le finalità di instaurazione e gestione da parte di soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato.

2. Tra i trattamenti effettuati per le finalità di cui al comma 1, si intendono ricompresi, in particolare, quelli effettuati al fine di:

a) applicare la normativa in materia di collocamento obbligatorio e assumere personale anche appartenente a categorie protette;
b) garantire le pari opportunità;
c) accertare il possesso di particolari requisiti previsti per l'accesso a specifici impieghi, anche in materia di tutela delle minoranze linguistiche, ovvero la sussistenza dei presupposti per la sospensione o la cessazione dall'impiego o dal servizio, il trasferimento di sede per incompatibilità e il conferimento di speciali abilitazioni;
d) adempiere ad obblighi connessi alla definizione dello stato giuridico ed economico, ivi compreso il riconoscimento della causa di servizio o dell'equo indennizzo, nonché ad obblighi retributivi, fiscali o contabili, relativamente al personale in servizio o in quiescenza, ivi compresa la corresponsione di premi e benefici assistenziali;

e) adempiere a specifici obblighi o svolgere compiti previsti dalla normativa in materia di igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, nonché in materia sindacale;
f) applicare, anche da parte di enti previdenziali ed assistenziali, la normativa in materia di previdenza ed assistenza ivi compresa quella integrativa, anche in applicazione del decreto legislativo del Capo provvisorio dello Stato 29 luglio 1947, n. 804, riguardo alla comunicazione di dati, anche mediante reti di comunicazione elettronica, agli istituti di patronato e di assistenza sociale, alle associazioni di categoria e agli ordini professionali che abbiano ottenuto il consenso dell'interessato ai sensi dell'articolo 23 in relazione a tipi di dati individuati specificamente;
g) svolgere attività dirette all'accertamento della responsabilità civile, disciplinare e contabile ed esaminare i ricorsi amministrativi in conformità alle norme che regolano le rispettive materie;
h) comparire in giudizio a mezzo di propri rappresentanti o partecipare alle procedure di arbitrato o di conciliazione nei casi previsti dalla legge o dai contratti collettivi di lavoro;
i) salvaguardare la vita o l'incolumità fisica dell'interessato o di terzi;
l) gestire l'anagrafe dei pubblici dipendenti e applicare la normativa in materia di assunzione di incarichi da parte di dipendenti pubblici, collaboratori e consulenti;
m) applicare la normativa in materia di incompatibilità e rapporti di lavoro a tempo parziale;
n) svolgere l'attività di indagine e ispezione presso soggetti pubblici;
o) valutare la qualità dei servizi resi e dei risultati conseguiti.

3. La diffusione dei dati di cui alle lettere m), n) ed o) del comma 2 è consentita in forma anonima e, comunque, tale da non consentire l'individuazione dell'interessato.

CAPO II - ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO

Art. 113. Raccolta di dati e pertinenza

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300.

CAPO III - DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO

Art. 114. Controllo a distanza

1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300.

Art. 115. Telelavoro e lavoro a domicilio

1. Nell'ambito del rapporto di lavoro domestico e del telelavoro il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.

2. Il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

CAPO IV - ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE

Art. 116. Conoscibilità di dati su mandato dell'interessato

1. Per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato ai sensi dell'articolo 23.

2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee-guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

TITOLO IX - SISTEMA BANCARIO, FINANZIARIO ED ASSICURATIVO

CAPO I - SISTEMI INFORMATIVI

Art. 117. Affidabilità e puntualità nei pagamenti

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di concessione di crediti al consumo o comunque riguardanti l'affidabilità e la puntualità nei pagamenti da parte degli interessati, individuando anche specifiche modalità per garantire la comunicazione di dati personali esatti e aggiornati nel rispetto dei diritti dell'interessato.

Art. 118. Informazioni commerciali

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale, prevedendo anche, in correlazione con quanto previsto dall'articolo 13, comma 5, modalità semplificate per l'informativa all'interessato e idonei meccanismi per garantire la qualità e l'esattezza dei dati raccolti e comunicati.

Art. 119. Dati relativi al comportamento debitorio

1. Con il codice di deontologia e di buona condotta di cui all'articolo 118 sono altresì individuati termini armonizzati di conservazione dei dati personali contenuti, in particolare, in banche di dati, registri ed elenchi tenuti da soggetti pubblici e privati, riferiti al comportamento debitorio dell'interessato nei casi diversi da quelli disciplinati nel codice di cui all'articolo 117, tenendo conto della specificità dei trattamenti nei diversi ambiti.

Art. 120. Sinistri

1. L'Istituto per la vigilanza sulle assicurazioni private e di interesse collettivo (ISVAP) definisce con proprio provvedimento le procedure e le modalità di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalità di accesso alle informazioni raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.

2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.

3. Per quanto non previsto dal presente articolo si applicano le disposizioni dell'articolo 2, comma 5-*quater*, del decreto legge 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge 26 maggio 2000, n. 137, e successive modificazioni.

TITOLO X - COMUNICAZIONI ELETTRONICHE

CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121. Servizi interessati

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni.

Art. 122. Informazioni raccolte nei riguardi dell'abbonato o dell'utente

1. Salvo quanto previsto dal comma 2, è vietato l'uso di una rete di comunicazione elet-

tronica per accedere a informazioni archiviate nell'apparecchio terminale di un abbonato o di un utente, per archiviare informazioni o per monitorare le operazioni dell'utente.

2. Il codice di deontologia di cui all'articolo 133 individua i presupposti e i limiti entro i quali l'uso della rete nei modi di cui al comma 1, per determinati scopi legittimi relativi alla memorizzazione tecnica per il tempo strettamente necessario alla trasmissione della comunicazione o a fornire uno specifico servizio richiesto dall'abbonato o dall'utente, è consentito al fornitore del servizio di comunicazione elettronica nei riguardi dell'abbonato e dell'utente che abbiano espresso il consenso sulla base di una previa informativa ai sensi dell'articolo 13 che indichi analiticamente, in modo chiaro e preciso, le finalità e la durata del trattamento.

Art. 123. Dati relativi al traffico

1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica, fatte salve le disposizioni dei commi 2, 3 e 5.

2. Il trattamento dei dati relativi al traffico strettamente necessari a fini di fatturazione per l'abbonato, ovvero di pagamenti in caso di interconnessione, è consentito al fornitore, a fini di documentazione in caso di contestazione della fattura o per la pretesa del pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale.

3. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico può trattare i dati di cui al comma 2 nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se l'abbonato o l'utente cui i dati si riferiscono hanno manifestato il proprio consenso, che è revocabile in ogni momento.

4. Nel fornire l'informativa di cui all'articolo 13 il fornitore del servizio informa l'abbonato o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3.

5. Il trattamento dei dati personali relativi al traffico è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30 sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

6. L'Autorità per le garanzie nelle comunicazioni può ottenere i dati relativi alla fatturazione o al traffico necessari ai fini della risoluzione di controversie attinenti, in particolare, all'interconnessione o alla fatturazione.

Art. 124. Fatturazione dettagliata

1. L'abbonato ha diritto di ricevere in dettaglio, a richiesta e senza alcun aggravio di spesa, la dimostrazione degli elementi che compongono la fattura relativi, in particolare, alla data e all'ora di inizio della conversazione, al numero selezionato, al tipo di numerazione, alla località, alla durata e al numero di scatti addebitati per ciascuna conversazione.

2. Il fornitore del servizio di comunicazione elettronica accessibile al pubblico è tenuto ad abilitare l'utente ad effettuare comunicazioni e a richiedere servizi da qualsiasi terminale, gratuitamente ed in modo agevole, avvalendosi per il pagamento di modalità alternative alla fatturazione, anche impersonali, quali carte di credito o di debito o carte prepagate.

3. Nella documentazione inviata all'abbonato relativa alle comunicazioni effettuate non sono evidenziati i servizi e le comunicazioni di cui al comma 2, né le comunicazioni necessarie per attivare le modalità alternative alla fatturazione.

4. Nella fatturazione all'abbonato non sono evidenziate le ultime tre cifre dei numeri chiamati. Ad esclusivi fini di specifica contestazione dell'esattezza di addebiti determinati o riferiti a periodi limitati, l'abbonato può richiedere la comunicazione dei numeri completi delle comunicazioni in questione.

5. Il Garante, accertata l'effettiva disponibilità delle modalità di cui al comma 2, può autorizzare il fornitore ad indicare nella fatturazione i numeri completi delle comunicazioni.

Art. 125. Identificazione della linea

1. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'utente chiamante la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea chiamante, chiamata per chiamata. L'abbonato chiamante deve avere tale possibilità linea per linea.

2. Se è disponibile la presentazione dell'identificazione della linea chiamante, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione delle chiamate entranti.

3. Se è disponibile la presentazione dell'identificazione della linea chiamante e tale indicazione avviene prima che la comunicazione sia stabilita, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità, mediante una funzione semplice e gratuita, di respingere le chiamate entranti se la presentazione dell'identificazione della linea chiamante è stata eliminata dall'utente o abbonato chiamante.

4. Se è disponibile la presentazione dell'identificazione della linea collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico assicura all'abbonato chiamato la possibilità di impedire, gratuitamente e mediante una funzione semplice, la presentazione dell'identificazione della linea collegata all'utente chiamante.

5. Le disposizioni di cui al comma 1 si applicano anche alle chiamate dirette verso Paesi non appartenenti all'Unione europea. Le disposizioni di cui ai commi 2, 3 e 4 si applicano anche alle chiamate provenienti da tali Paesi.

6. Se è disponibile la presentazione dell'identificazione della linea chiamante o di quella collegata, il fornitore del servizio di comunicazione elettronica accessibile al pubblico informa gli abbonati e gli utenti dell'esistenza di tale servizio e delle possibilità previste ai commi 1, 2, 3 e 4.

Art. 126. Dati relativi all'ubicazione

1. I dati relativi all'ubicazione diversi dai dati relativi al traffico, riferiti agli utenti o agli abbonati di reti pubbliche di comunicazione o di servizi di comunicazione elettronica accessibili al pubblico, possono essere trattati solo se anonimi o se l'utente o l'abbonato ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto.

2. Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e gli abbonati sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto.

3. L'utente e l'abbonato che manifestano il proprio consenso al trattamento dei dati rela-

tivi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni.

4. Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente ad incaricati del trattamento che operano ai sensi dell'articolo 30, sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione dell'incaricato che accede ai dati anche mediante un'operazione di interrogazione automatizzata.

Art. 127. Chiamate di disturbo e di emergenza

1. L'abbonato che riceve chiamate di disturbo può richiedere che il fornitore della rete pubblica di comunicazioni o del servizio di comunicazione elettronica accessibile al pubblico renda temporaneamente inefficace la soppressione della presentazione dell'identificazione della linea chiamante e conservi i dati relativi alla provenienza della chiamata ricevuta. L'inefficacia della soppressione può essere disposta per i soli orari durante i quali si verificano le chiamate di disturbo e per un periodo non superiore a quindici giorni.

2. La richiesta formulata per iscritto dall'abbonato specifica le modalità di ricezione delle chiamate di disturbo e nel caso in cui sia preceduta da una richiesta telefonica è inoltrata entro quarantotto ore.

3. I dati conservati ai sensi del comma 1 possono essere comunicati all'abbonato che dichiari di utilizzarli per esclusive finalità di tutela rispetto a chiamate di disturbo. Per i servizi di cui al comma 1 il fornitore assicura procedure trasparenti nei confronti degli abbonati e può richiedere un contributo spese non superiore ai costi effettivamente sopportati.

4. Il fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico predispone procedure trasparenti per garantire, linea per linea, l'inefficacia della soppressione dell'identificazione della linea chiamante, nonché, ove necessario, il trattamento dei dati relativi all'ubicazione, nonostante il rifiuto o il mancato consenso temporanei dell'abbonato o dell'utente, da parte dei servizi abilitati in base alla legge a ricevere chiamate d'emergenza. I servizi sono individuati con decreto del Ministro delle comunicazioni, sentiti il Garante e l'Autorità per le garanzie nelle comunicazioni.

Art. 128. Trasferimento automatico della chiamata

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico adotta le misure necessarie per consentire a ciascun abbonato, gratuitamente e mediante una funzione semplice, di poter bloccare il trasferimento automatico delle chiamate verso il proprio terminale effettuato da terzi.

Art. 129. Elenchi di abbonati

1. Il Garante individua con proprio provvedimento, in cooperazione con l'Autorità per le garanzie nelle comunicazioni ai sensi dell'articolo 154, comma 3, e in conformità alla normativa comunitaria, le modalità di inserimento e di successivo utilizzo dei dati personali relativi agli abbonati negli elenchi cartacei o elettronici a disposizione del pubblico, anche in riferimento ai dati già raccolti prima della data di entrata in vigore del presente codice.

2. Il provvedimento di cui al comma 1 individua idonee modalità per la manifestazione del consenso all'inclusione negli elenchi e, rispettivamente, all'utilizzo dei dati per le finalità di cui all'articolo 7, comma 4, lettera b), in base al principio della massima semplificazione delle modalità di inclusione negli elenchi a fini di mera ricerca dell'abbonato per comunicazioni interpersonali, e del consenso specifico ed espresso qualora il trattamento esuli da tali fini, nonché in tema di verifica, rettifica o cancellazione dei dati senza oneri.

Art. 130. Comunicazioni indesiderate

1. L'uso di sistemi automatizzati di chiamata senza l'intervento di un operatore per l'invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale è consentito con il consenso dell'interessato.

2. La disposizione di cui al comma 1 si applica anche alle comunicazioni elettroniche, effettuate per le finalità ivi indicate, mediante posta elettronica, telefax, messaggi del tipo *Mms (Multimedia messaging service)* o *Sms (Short message service)* o di altro tipo.

3. Fuori dei casi di cui ai commi 1 e 2, ulteriori comunicazioni per le finalità di cui ai medesimi commi effettuate con mezzi diversi da quelli ivi indicati, sono consentite ai sensi degli articoli 23 e 24.

4. Fatto salvo quanto previsto nel comma 1, se il titolare del trattamento utilizza, a fini di vendita diretta di propri prodotti o servizi, le coordinate di posta elettronica fornite dall'interessato nel contesto della vendita di un prodotto o di un servizio, può non richiedere il consenso dell'interessato, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. L'interessato, al momento della raccolta e in occasione dell'invio di ogni comunicazione effettuata per le finalità di cui al presente comma, è informato della possibilità di opporsi in ogni momento al trattamento, in maniera agevole e gratuitamente.

5. È vietato in ogni caso l'invio di comunicazioni per le finalità di cui al comma 1 o, comunque, a scopo promozionale, effettuato camuffando o celando l'identità del mittente o senza fornire un idoneo recapito presso il quale l'interessato possa esercitare i diritti di cui all'articolo 7.

6. In caso di reiterata violazione delle disposizioni di cui al presente articolo il Garante può, provvedendo ai sensi dell'articolo 143, comma 1, lettera b), altresì prescrivere a fornitori di servizi di comunicazione elettronica di adottare procedure di filtraggio o altre misure praticabili relativamente alle coordinate di posta elettronica da cui sono stati inviate le comunicazioni.

Art. 131. Informazioni ad abbonati e utenti

1. Il fornitore di un servizio di comunicazione elettronica accessibile al pubblico informa l'abbonato e, ove possibile, l'utente circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

2. L'abbonato informa l'utente quando il contenuto delle comunicazioni o conversazioni può essere appreso da altri a causa del tipo di apparecchiature terminali utilizzate o del collegamento realizzato tra le stesse presso la sede dell'abbonato medesimo.

3. L'utente informa l'altro utente quando, nel corso della conversazione, sono utilizzati dispositivi che consentono l'ascolto della conversazione stessa da parte di altri soggetti.

Art. 132. Conservazione di dati di traffico per altre finalità (*)

1. Fermo restando quanto previsto dall'articolo 123, comma 2, i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi, per finalità di accertamento e repressione di reati.

2. Decorso il termine di cui al comma 1, i dati relativi al traffico telefonico sono conservati dal fornitore per ulteriori ventiquattro mesi per esclusive finalità di accertamento e repressione dei delitti di cui all'articolo 407, comma 2, lettera a) del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

3. Entro il termine di cui al comma 1, i dati sono acquisiti presso il fornitore con decreto

(*) Articolo cos'sostituito dall'articolo 3 del decreto legge 24 dicembre 2003, n. 354, nel testo modificato dalla legge 26 febbraio 2004, n. 45, di conversione del predetto decreto legge

*motivato del giudice su istanza del pubblico ministero o del difensore dell'imputato, della persona sottoposta alle indagini, della persona offesa e delle altre parti private ferme restando le condizioni di cui all'articolo 8, comma 2, lettera f), per il traffico entrante. Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere, direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall'articolo 391-*quater *del codice di procedura penale.*

4. Dopo la scadenza del termine indicato al comma 1, il giudice autorizza l'acquisizione dei dati, con decreto motivato, se ritiene che sussistano sufficienti indizi dei delitti di cui all'articolo 407, comma 2, lettera a), del codice di procedura penale, nonché dei delitti in danno di sistemi informatici o telematici.

5. Il trattamento dei dati per le finalità di cui ai commi 1 e 2 è effettuato nel rispetto delle misure e degli accorgimenti a garanzia dell'interessato prescritti ai sensi dell'articolo 17, volti anche a:

a. prevedere in ogni caso specifici sistemi di autenticazione informatica e di autorizzazione degli incaricati del trattamento di cui all'Allegato B);
b. disciplinare le modalità di conservazione separata dei dati una volta decorso il termine di cui al comma 1;
c. individuare le modalità di trattamento dei dati da parte di specifici incaricati del trattamento in modo tale che, decorso il termine di cui al comma 1, l'utilizzazione dei dati sia consentita solo nei casi di cui al comma 4 e all'articolo 7;
d. indicare le modalità tecniche per la periodica distruzione dei dati, decorsi i termini di cui ai commi 1 e 2.

Capo II - Internet e reti telematiche

Art. 133. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato da fornitori di servizi di comunicazione e informazione offerti mediante reti di comunicazione elettronica, con particolare riguardo ai criteri per assicurare ed uniformare una più adeguata informazione e consapevolezza degli utenti delle reti di comunicazione elettronica gestite da soggetti pubblici e privati rispetto ai tipi di dati personali trattati e alle modalità del loro trattamento, in particolare attraverso informative fornite in linea in modo agevole e interattivo, per favorire una più ampia trasparenza e correttezza nei confronti dei medesimi utenti e il pieno rispetto dei principi di cui all'articolo 11, anche ai fini dell'eventuale rilascio di certificazioni attestanti la qualità delle modalità prescelte e il livello di sicurezza assicurato.

Capo III - Videosorveglianza

Art. 134. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato con strumenti elettronici di rilevamento di immagini, prevedendo specifiche modalità di trattamento e forme semplificate di informativa all'interessato per garantire la liceità e la correttezza anche in riferimento a quanto previsto dall'articolo 11.

Titolo XI - Libere professioni e investigazione privata

Capo I - Profili generali

Art. 135. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o per far valere o difendere un diritto in sede giudiziaria, in particolare da liberi professionisti o da soggetti che esercitano un'attività di investigazione privata autorizzata in conformità alla legge.

TITOLO XII - GIORNALISMO ED ESPRESSIONE LETTERARIA ED ARTISTICA

CAPO I - PROFILI GENERALI

Art. 136. Finalità giornalistiche e altre manifestazioni del pensiero

1. Le disposizioni del presente titolo si applicano al trattamento:
   a) effettuato nell'esercizio della professione di giornalista e per l'esclusivo perseguimento delle relative finalità;
   b) effettuato dai soggetti iscritti nell'elenco dei pubblicisti o nel registro dei praticanti di cui agli articoli 26 e 33 della legge 3 febbraio 1963, n. 69;
   c) temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica.

Art. 137. Disposizioni applicabili

1. Ai trattamenti indicati nell'articolo 136 non si applicano le disposizioni del presente codice relative:
   a) all'autorizzazione del Garante prevista dall'articolo 26;
   b) alle garanzie previste dall'articolo 27 per i dati giudiziari;
   c) al trasferimento dei dati all'estero, contenute nel Titolo VII della Parte I.

2. Il trattamento dei dati di cui al comma 1 è effettuato anche senza il consenso dell'interessato previsto dagli articoli 23 e 26.

3. In caso di diffusione o di comunicazione dei dati per le finalità di cui all'articolo 136 restano fermi i limiti del diritto di cronaca a tutela dei diritti di cui all'articolo 2 e, in particolare, quello dell'essenzialità dell'informazione riguardo a fatti di interesse pubblico. Possono essere trattati i dati personali relativi a circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico.

Art. 138. Segreto professionale

1. In caso di richiesta dell'interessato di conoscere l'origine dei dati personali ai sensi dell'articolo 7, comma 2, lettera a), restano ferme le norme sul segreto professionale degli esercenti la professione di giornalista, limitatamente alla fonte della notizia.

CAPO II - CODICE DI DEONTOLOGIA

Art. 139. Codice di deontologia relativo ad attività giornalistiche

1. Il Garante promuove ai sensi dell'articolo 12 l'adozione da parte del Consiglio nazionale dell'ordine dei giornalisti di un codice di deontologia relativo al trattamento dei dati di cui all'articolo 136, che prevede misure ed accorgimenti a garanzia degli interessati rapportate alla natura dei dati, in particolare per quanto riguarda quelli idonei a rivelare lo stato di salute e la vita sessuale. Il codice può anche prevedere forme semplificate per le informative di cui all'articolo 13.

2. Nella fase di formazione del codice, ovvero successivamente, il Garante, in cooperazione con il Consiglio, prescrive eventuali misure e accorgimenti a garanzia degli interessati, che il Consiglio è tenuto a recepire.

3. Il codice o le modificazioni od integrazioni al codice di deontologia che non sono adottati dal Consiglio entro sei mesi dalla proposta del Garante sono adottati in via sostitutiva dal Garante e sono efficaci sino a quando diviene efficace una diversa disciplina secondo la procedura di cooperazione.

4. Il codice e le disposizioni di modificazione ed integrazione divengono efficaci quindici giorni dopo la loro pubblicazione nella *Gazzetta Ufficiale* ai sensi dell'articolo 12.

5. In caso di violazione delle prescrizioni contenute nel codice di deontologia, il Garante può vietare il trattamento ai sensi dell'articolo 143, comma 1, lettera c).

TITOLO XIII - MARKETING DIRETTO

CAPO I - PROFILI GENERALI

Art. 140. Codice di deontologia e di buona condotta

1. Il Garante promuove, ai sensi dell'articolo 12, la sottoscrizione di un codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale, prevedendo anche, per i casi in cui il trattamento non presuppone il consenso dell'interessato, forme semplificate per manifestare e rendere meglio conoscibile l'eventuale dichiarazione di non voler ricevere determinate comunicazioni.

PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

TITOLO I - TUTELA AMMINISTRATIVA E GIURISDIZIONALE

CAPO I - TUTELA DINANZI AL GARANTE

Sezione I - Principi generali

Art. 141. Forme di tutela

1. L'interessato può rivolgersi al Garante:
   a) mediante reclamo circostanziato nei modi previsti dall'articolo 142, per rappresentare una violazione della disciplina rilevante in materia di trattamento di dati personali;
   b) mediante segnalazione, se non è possibile presentare un reclamo circostanziato ai sensi della lettera a), al fine di sollecitare un controllo da parte del Garante sulla disciplina medesima;
   c) mediante ricorso, se intende far valere gli specifici diritti di cui all'articolo 7 secondo le modalità e per conseguire gli effetti previsti nella sezione III del presente capo.

Sezione II - Tutela amministrativa

Art. 142. Proposizione dei reclami

1. Il reclamo contiene un'indicazione per quanto possibile dettagliata dei fatti e delle circostanze su cui si fonda, delle disposizioni che si presumono violate e delle misure richieste, nonché gli estremi identificativi del titolare, del responsabile, ove conosciuto, e dell'istante.

2. Il reclamo è sottoscritto dagli interessati, o da associazioni che li rappresentano anche ai sensi dell'articolo 9, comma 2, ed è presentato al Garante senza particolari formalità. Il reclamo reca in allegato la documentazione utile ai fini della sua valutazione e l'eventuale procura, e indica un recapito per l'invio di comunicazioni anche tramite posta elettronica, telefax o telefono.

3. Il Garante può predisporre un modello per il reclamo da pubblicare nel Bollettino e di cui favorisce la disponibilità con strumenti elettronici.

Art. 143. Procedimento per i reclami

1. Esaurita l'istruttoria preliminare, se il reclamo non è manifestamente infondato e sussistono i presupposti per adottare un provvedimento, il Garante, anche prima della definizione del procedimento:
   a) prima di prescrivere le misure di cui alla lettera b), ovvero il divieto o il blocco ai sensi della lettera c), può invitare il titolare, anche in contraddittorio con l'interessato, ad effettuare il blocco spontaneamente;

b) prescrive al titolare le misure opportune o necessarie per rendere il trattamento conforme alle disposizioni vigenti;
c) dispone il blocco o vieta, in tutto o in parte, il trattamento che risulta illecito o non corretto anche per effetto della mancata adozione delle misure necessarie di cui alla lettera b), oppure quando, in considerazione della natura dei dati o, comunque, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante per uno o più interessati;
d) può vietare in tutto o in parte il trattamento di dati relativi a singoli soggetti o a categorie di soggetti che si pone in contrasto con rilevanti interessi della collettività.

2. I provvedimenti di cui al comma 1 sono pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana se i relativi destinatari non sono facilmente identificabili per il numero o per la complessità degli accertamenti.

Art. 144. Segnalazioni

1. I provvedimenti di cui all'articolo 143 possono essere adottati anche a seguito delle segnalazioni di cui all'articolo 141, comma 1, lettera b), se è avviata un'istruttoria preliminare e anche prima della definizione del procedimento.

Sezione III - Tutela alternativa a quella giurisdizionale

Art. 145. Ricorsi

1. I diritti di cui all'articolo 7 possono essere fatti valere dinanzi all'autorità giudiziaria o con ricorso al Garante.

2. Il ricorso al Garante non può essere proposto se, per il medesimo oggetto e tra le stesse parti, è stata già adita l'autorità giudiziaria.

3. La presentazione del ricorso al Garante rende improponibile un'ulteriore domanda dinanzi all'autorità giudiziaria tra le stesse parti e per il medesimo oggetto.

Art. 146. Interpello preventivo

1. Salvi i casi in cui il decorso del termine esporrebbe taluno a pregiudizio imminente ed irreparabile, il ricorso al Garante può essere proposto solo dopo che è stata avanzata richiesta sul medesimo oggetto al titolare o al responsabile ai sensi dell'articolo 8, comma 1, e sono decorsi i termini previsti dal presente articolo, ovvero è stato opposto alla richiesta un diniego anche parziale.

2. Il riscontro alla richiesta da parte del titolare o del responsabile è fornito entro quindici giorni dal suo ricevimento.

3. Entro il termine di cui al comma 2, se le operazioni necessarie per un integrale riscontro alla richiesta sono di particolare complessità, ovvero ricorre altro giustificato motivo, il titolare o il responsabile ne danno comunicazione all'interessato. In tal caso, il termine per l'integrale riscontro è di trenta giorni dal ricevimento della richiesta medesima.

Art. 147. Presentazione del ricorso

1. Il ricorso è proposto nei confronti del titolare e indica:
a) gli estremi identificativi del ricorrente, dell'eventuale procuratore speciale, del titolare e, ove conosciuto, del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7;
b) la data della richiesta presentata al titolare o al responsabile ai sensi dell'articolo 8, comma 1, oppure del pregiudizio imminente ed irreparabile che permette di prescindere dalla richiesta medesima;
c) gli elementi posti a fondamento della domanda;
d) il provvedimento richiesto al Garante;
e) il domicilio eletto ai fini del procedimento.

2. Il ricorso è sottoscritto dal ricorrente o dal procuratore speciale e reca in allegato:
   a) la copia della richiesta rivolta al titolare o al responsabile ai sensi dell'articolo 8, comma 1;
   b) l'eventuale procura;
   c) la prova del versamento dei diritti di segreteria.

3. Al ricorso è unita, altresì, la documentazione utile ai fini della sua valutazione e l'indicazione di un recapito per l'invio di comunicazioni al ricorrente o al procuratore speciale mediante posta elettronica, telefax o telefono.

4. Il ricorso è rivolto al Garante e la relativa sottoscrizione è autenticata. L'autenticazione non è richiesta se la sottoscrizione è apposta presso l'Ufficio del Garante o da un procuratore speciale iscritto all'albo degli avvocati al quale la procura è conferita ai sensi dell'articolo 83 del codice di procedura civile, ovvero con firma digitale in conformità alla normativa vigente.

5. Il ricorso è validamente proposto solo se è trasmesso con plico raccomandato, oppure per via telematica osservando le modalità relative alla sottoscrizione con firma digitale e alla conferma del ricevimento prescritte ai sensi dell'articolo 38, comma 2, ovvero presentato direttamente presso l'Ufficio del Garante.

Art. 148. Inammissibilità del ricorso

1. Il ricorso è inammissibile:
   a) se proviene da un soggetto non legittimato;
   b) in caso di inosservanza delle disposizioni di cui agli articoli 145 e 146;
   c) se difetta di taluno degli elementi indicati nell'articolo 147, commi 1 e 2, salvo che sia regolarizzato dal ricorrente o dal procuratore speciale anche su invito dell'Ufficio del Garante ai sensi del comma 2, entro sette giorni dalla data della sua presentazione o della ricezione dell'invito. In tale caso, il ricorso si considera presentato al momento in cui il ricorso regolarizzato perviene all'Ufficio.

2. Il Garante determina i casi in cui è possibile la regolarizzazione del ricorso.

Art. 149. Procedimento relativo al ricorso

1. Fuori dei casi in cui è dichiarato inammissibile o manifestamente infondato, il ricorso è comunicato al titolare entro tre giorni a cura dell'Ufficio del Garante, con invito ad esercitare entro dieci giorni dal suo ricevimento la facoltà di comunicare al ricorrente e all'Ufficio la propria eventuale adesione spontanea. L'invito è comunicato al titolare per il tramite del responsabile eventualmente designato per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, ove indicato nel ricorso.

2. In caso di adesione spontanea è dichiarato non luogo a provvedere. Se il ricorrente lo richiede, è determinato in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico della controparte o compensati per giusti motivi anche parzialmente.

3. Nel procedimento dinanzi al Garante il titolare, il responsabile di cui al comma 1 e l'interessato hanno diritto di essere sentiti, personalmente o a mezzo di procuratore speciale, e hanno facoltà di presentare memorie o documenti. A tal fine l'invito di cui al comma 1 è trasmesso anche al ricorrente e reca l'indicazione del termine entro il quale il titolare, il medesimo responsabile e l'interessato possono presentare memorie e documenti, nonché della data in cui tali soggetti possono essere sentiti in contraddittorio anche mediante idonea tecnica audiovisiva.

4. Nel procedimento il ricorrente può precisare la domanda nei limiti di quanto chiesto con il ricorso o a seguito di eccezioni formulate dal titolare.

5. Il Garante può disporre, anche d'ufficio, l'espletamento di una o più perizie. Il provvedimento che le dispone precisa il contenuto dell'incarico e il termine per la sua esecu-

zione, ed è comunicato alle parti le quali possono presenziare alle operazioni personalmente o tramite procuratori o consulenti designati. Il provvedimento dispone inoltre in ordine all'anticipazione delle spese della perizia.

6. Nel procedimento, il titolare e il responsabile di cui al comma 1 possono essere assistiti da un procuratore o da altra persona di fiducia.

7. Se gli accertamenti risultano particolarmente complessi o vi è l'assenso delle parti il termine di sessanta giorni di cui all'articolo 150, comma 2, può essere prorogato per un periodo non superiore ad ulteriori quaranta giorni.

8. Il decorso dei termini previsti dall'articolo 150, comma 2 e dall'articolo 151 è sospeso di diritto dal 1° agosto al 15 settembre di ciascun anno e riprende a decorrere dalla fine del periodo di sospensione. Se il decorso ha inizio durante tale periodo, l'inizio stesso è differito alla fine del periodo medesimo. La sospensione non opera nei casi in cui sussiste il pregiudizio di cui all'articolo 146, comma 1, e non preclude l'adozione dei provvedimenti di cui all' articolo 150, comma 1.

Art. 150. Provvedimenti a seguito del ricorso

1. Se la particolarità del caso lo richiede, il Garante può disporre in via provvisoria il blocco in tutto o in parte di taluno dei dati, ovvero l'immediata sospensione di una o più operazioni del trattamento. Il provvedimento può essere adottato anche prima della comunicazione del ricorso ai sensi dell'articolo 149, comma 1, e cessa di avere ogni effetto se non è adottata nei termini la decisione di cui al comma 2. Il medesimo provvedimento è impugnabile unitamente a tale decisione.

2. Assunte le necessarie informazioni il Garante, se ritiene fondato il ricorso, ordina al titolare, con decisione motivata, la cessazione del comportamento illegittimo, indicando le misure necessarie a tutela dei diritti dell'interessato e assegnando un termine per la loro adozione. La mancata pronuncia sul ricorso, decorsi sessanta giorni dalla data di presentazione, equivale a rigetto.

3. Se vi è stata previa richiesta di taluna delle parti, il provvedimento che definisce il procedimento determina in misura forfettaria l'ammontare delle spese e dei diritti inerenti al ricorso, posti a carico, anche in parte, del soccombente o compensati anche parzialmente per giusti motivi.

4. Il provvedimento espresso, anche provvisorio, adottato dal Garante è comunicato alle parti entro dieci giorni presso il domicilio eletto o risultante dagli atti. Il provvedimento può essere comunicato alle parti anche mediante posta elettronica o telefax.

5. Se sorgono difficoltà o contestazioni riguardo all'esecuzione del provvedimento di cui ai commi 1 e 2, il Garante, sentite le parti ove richiesto, dispone le modalità di attuazione avvalendosi, se necessario, del personale dell'Ufficio o della collaborazione di altri organi dello Stato.

6. In caso di mancata opposizione avverso il provvedimento che determina l'ammontare delle spese e dei diritti, o di suo rigetto, il provvedimento medesimo costituisce, per questa parte, titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

Art. 151. Opposizione

1. Avverso il provvedimento espresso o il rigetto tacito di cui all'articolo 150, comma 2, il titolare o l'interessato possono proporre opposizione con ricorso ai sensi dell'articolo 152. L'opposizione non sospende l'esecuzione del provvedimento.

2. Il tribunale provvede nei modi di cui all'articolo 152.

CAPO II - TUTELA GIURISDIZIONALE

Art. 152. Autorità giudiziaria ordinaria

1. Tutte le controversie che riguardano, comunque, l'applicazione delle disposizioni del presente codice, comprese quelle inerenti ai provvedimenti del Garante in materia di protezione dei dati personali o alla loro mancata adozione, sono attribuite all'autorità giudiziaria ordinaria.

2. Per tutte le controversie di cui al comma 1 l'azione si propone con ricorso depositato nella cancelleria del tribunale del luogo ove risiede il titolare del trattamento.

3. Il tribunale decide in ogni caso in composizione monocratica.

4. Se è presentato avverso un provvedimento del Garante anche ai sensi dell'articolo 143, il ricorso è proposto entro il termine di trenta giorni dalla data di comunicazione del provvedimento o dalla data del rigetto tacito. Se il ricorso è proposto oltre tale termine il giudice lo dichiara inammissibile con ordinanza ricorribile per cassazione.

5. La proposizione del ricorso non sospende l'esecuzione del provvedimento del Garante. Se ricorrono gravi motivi il giudice, sentite le parti, può disporre diversamente in tutto o in parte con ordinanza impugnabile unitamente alla decisione che definisce il grado di giudizio.

6. Quando sussiste pericolo imminente di un danno grave ed irreparabile il giudice può emanare i provvedimenti necessari con decreto motivato, fissando, con il medesimo provvedimento, l'udienza di comparizione delle parti entro un termine non superiore a quindici giorni. In tale udienza, con ordinanza, il giudice conferma, modifica o revoca i provvedimenti emanati con decreto.

7. Il giudice fissa l'udienza di comparizione delle parti con decreto con il quale assegna al ricorrente il termine perentorio entro cui notificarlo alle altre parti e al Garante. Tra il giorno della notificazione e l'udienza di comparizione intercorrono non meno di trenta giorni.

8. Se alla prima udienza il ricorrente non compare senza addurre alcun legittimo impedimento, il giudice dispone la cancellazione della causa dal ruolo e dichiara l'estinzione del processo, ponendo a carico del ricorrente le spese di giudizio.

9. Nel corso del giudizio il giudice dispone, anche d'ufficio, omettendo ogni formalità non necessaria al contraddittorio, i mezzi di prova che ritiene necessari e può disporre la citazione di testimoni anche senza la formulazione di capitoli.

10. Terminata l'istruttoria, il giudice invita le parti a precisare le conclusioni ed a procedere, nella stessa udienza, alla discussione orale della causa, pronunciando subito dopo la sentenza mediante lettura del dispositivo. Le motivazioni della sentenza sono depositate in cancelleria entro i successivi trenta giorni. Il giudice può anche redigere e leggere, unitamente al dispositivo, la motivazione della sentenza, che è subito dopo depositata in cancelleria.

11. Se necessario, il giudice può concedere alle parti un termine non superiore a dieci giorni per il deposito di note difensive e rinviare la causa all'udienza immediatamente successiva alla scadenza del termine per la discussione e la pronuncia della sentenza.

12. Con la sentenza il giudice, anche in deroga al divieto di cui all'articolo 4 della legge 20 marzo 1865, n. 2248, allegato E), quando è necessario anche in relazione all'eventuale atto del soggetto pubblico titolare o responsabile, accoglie o rigetta la domanda, in tutto o in parte, prescrive le misure necessarie, dispone sul risarcimento del danno, ove richiesto, e pone a carico della parte soccombente le spese del procedimento.

13. La sentenza non è appellabile, ma è ammesso il ricorso per cassazione.

14. Le disposizioni di cui al presente articolo si applicano anche nei casi previsti dall'articolo 10, comma 5, della legge 1° aprile 1981, n. 121, e successive modificazioni.

TITOLO II - L'AUTORITÀ

CAPO I - IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Art. 153. Il Garante

1. Il Garante opera in piena autonomia e con indipendenza di giudizio e di valutazione.

2. Il Garante è organo collegiale costituito da quattro componenti, eletti due dalla Camera dei deputati e due dal Senato della Repubblica con voto limitato. I componenti sono scelti tra persone che assicurano indipendenza e che sono esperti di riconosciuta competenza delle materie del diritto o dell'informatica, garantendo la presenza di entrambe le qualificazioni.

3. I componenti eleggono nel loro ambito un presidente, il cui voto prevale in caso di parità. Eleggono altresì un vice presidente, che assume le funzioni del presidente in caso di sua assenza o impedimento.

4. Il presidente e i componenti durano in carica quattro anni e non possono essere confermati per più di una volta; per tutta la durata dell'incarico il presidente e i componenti non possono esercitare, a pena di decadenza, alcuna attività professionale o di consulenza, né essere amministratori o dipendenti di enti pubblici o privati, né ricoprire cariche elettive.

5. All'atto dell'accettazione della nomina il presidente e i componenti sono collocati fuori ruolo se dipendenti di pubbliche amministrazioni o magistrati in attività di servizio; se professori universitari di ruolo, sono collocati in aspettativa senza assegni ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni. Il personale collocato fuori ruolo o in aspettativa non può essere sostituito.

6. Al presidente compete una indennità di funzione non eccedente, nel massimo, la retribuzione spettante al primo presidente della Corte di cassazione. Ai componenti compete un'indennità non eccedente nel massimo, i due terzi di quella spettante al presidente. Le predette indennità di funzione sono determinate dall'articolo 6 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501, in misura tale da poter essere corrisposte a carico degli ordinari stanziamenti.

7. Alle dipendenze del Garante è posto l'Ufficio di cui all'articolo 156.

Art. 154. Compiti

1. Oltre a quanto previsto da specifiche disposizioni, il Garante, anche avvalendosi dell'Ufficio e in conformità al presente codice, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile e in conformità alla notificazione, anche in caso di loro cessazione;
b) esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati o dalle associazioni che li rappresentano;
c) prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143;
d) vietare anche d'ufficio, in tutto o in parte, il trattamento illecito o non corretto dei dati o disporne il blocco ai sensi dell'articolo 143, e di adottare gli altri provvedimenti previsti dalla disciplina applicabile al trattamento dei dati personali;
e) promuovere la sottoscrizione di codici ai sensi dell'articolo 12 e dell'articolo 139;
f) segnalare al Parlamento e al Governo l'opportunità di interventi normativi richiesti dalla necessità di tutelare i diritti di cui all'articolo 2 anche a seguito dell'evoluzione del settore;
g) esprimere pareri nei casi previsti;
h) curare la conoscenza tra il pubblico della disciplina rilevante in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati;
i) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;

l) tenere il registro dei trattamenti formato sulla base delle notificazioni di cui all'articolo 37;

m) predisporre annualmente una relazione sull'attività svolta e sullo stato di attuazione del presente codice, che è trasmessa al Parlamento e al Governo entro il 30 aprile dell'anno successivo a quello cui si riferisce.

2. Il Garante svolge altresì, ai sensi del comma 1, la funzione di controllo o assistenza in materia di trattamento dei dati personali prevista da leggi di ratifica di accordi o convenzioni internazionali o da regolamenti comunitari e, in particolare:

a) dalla legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'Accordo di Schengen e alla relativa convenzione di applicazione;

b) dalla legge 23 marzo 1998, n. 93, e successive modificazioni, di ratifica ed esecuzione della convenzione istitutiva dell'Ufficio europeo di polizia (Europol);

c) dal regolamento (Ce) n. 515/97 del Consiglio, del 13 marzo 1997, e dalla legge 30 luglio 1998, n. 291, e successive modificazioni, di ratifica ed esecuzione della convenzione sull'uso dell'informatica nel settore doganale;

d) dal regolamento (Ce) n. 2725/2000 del Consiglio, dell'11 dicembre 2000, che istituisce l'"Eurodac" per il confronto delle impronte digitali e per l'efficace applicazione della convenzione di Dublino;

e) nel capitolo IV della convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981 e resa esecutiva con legge 21 febbraio 1989, n. 98, quale autorità designata ai fini della cooperazione tra Stati ai sensi dell'articolo 13 della convenzione medesima.

3. Il Garante coopera con altre autorità amministrative indipendenti nello svolgimento dei rispettivi compiti. A tale fine, il Garante può anche invitare rappresentanti di un'altra autorità a partecipare alle proprie riunioni, o essere invitato alle riunioni di altra autorità, prendendo parte alla discussione di argomenti di comune interesse; può richiedere, altresì, la collaborazione di personale specializzato addetto ad altra autorità.

4. Il Presidente del Consiglio dei ministri e ciascun ministro consultano il Garante all'atto della predisposizione delle norme regolamentari e degli atti amministrativi suscettibili di incidere sulle materie disciplinate dal presente codice.

5. Fatti salvi i termini più brevi previsti per legge, il parere del Garante è reso nei casi previsti nel termine di quarantacinque giorni dal ricevimento della richiesta. Decorso il termine, l'amministrazione può procedere indipendentemente dall'acquisizione del parere. Quando, per esigenze istruttorie, non può essere rispettato il termine di cui al presente comma, tale termine può essere interrotto per una sola volta e il parere deve essere reso definitivamente entro venti giorni dal ricevimento degli elementi istruttori da parte delle amministrazioni interessate.

6. Copia dei provvedimenti emessi dall'autorità giudiziaria in relazione a quanto previsto dal presente codice o in materia di criminalità informatica è trasmessa, a cura della cancelleria, al Garante.

CAPO II - L'UFFICIO DEL GARANTE

Art. 155. Principi applicabili

1. All'Ufficio del Garante, al fine di garantire la responsabilità e l'autonomia ai sensi della legge 7 agosto 1990, n. 241, e successive modificazioni, e del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, si applicano i principi riguardanti l'individuazione e le funzioni del responsabile del procedimento, nonché quelli relativi alla distinzione fra le funzioni di indirizzo e di controllo, attribuite agli organi di vertice, e le funzioni di gestione attribuite ai dirigenti. Si applicano altresì le disposizioni del medesimo decreto legislativo n. 165 del 2001 espressamente richiamate dal presente codice.

Art. 156. Ruolo organico e personale

1. All'Ufficio del Garante è preposto un segretario generale scelto anche tra magistrati ordinari o amministrativi.

2. Il ruolo organico del personale dipendente è stabilito nel limite di cento unità.

3. Con propri regolamenti pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana, il Garante definisce:

a) l'organizzazione e il funzionamento dell'Ufficio anche ai fini dello svolgimento dei compiti di cui all'articolo 154;

b) l'ordinamento delle carriere e le modalità di reclutamento del personale secondo le procedure previste dall'articolo 35 del decreto legislativo n. 165 del 2001;

c) la ripartizione dell'organico tra le diverse aree e qualifiche;

d) il trattamento giuridico ed economico del personale, secondo i criteri previsti dalla legge 31 luglio 1997, n. 249 e successive modificazioni e, per gli incarichi dirigenziali, dagli articoli 19, comma 6, e 23-bis del decreto legislativo 30 marzo 2001, n. 165, tenuto conto delle specifiche esigenze funzionali e organizzative. Nelle more della più generale razionalizzazione del trattamento economico delle autorità amministrative indipendenti, al personale è attribuito l'ottanta per cento del trattamento economico del personale dell'Autorità per le garanzie nelle comunicazioni;

e) la gestione amministrativa e la contabilità, anche in deroga alle norme sulla contabilità generale dello Stato, l'utilizzo dell'avanzo di amministrazione nel quale sono iscritte le somme già versate nella contabilità speciale, nonché l'individuazione dei casi di riscossione e utilizzazione dei diritti di segreteria o di corrispettivi per servizi resi in base a disposizioni di legge secondo le modalità di cui all'articolo 6, comma 2, della legge 31 luglio 1997, n. 249.

4. L'Ufficio può avvalersi, per motivate esigenze, di dipendenti dello Stato o di altre amministrazioni pubbliche o di enti pubblici collocati in posizione di fuori ruolo o equiparati nelle forme previste dai rispettivi ordinamenti, ovvero in aspettativa ai sensi dell'articolo 13 del decreto del Presidente della Repubblica 11 luglio 1980, n. 382, e successive modificazioni, in numero non superiore, complessivamente, a venti unità e per non oltre il venti per cento delle qualifiche dirigenziali, lasciando non coperto un corrispondente numero di posti di ruolo. Al personale di cui al presente comma è corrisposta un'indennità pari all'eventuale differenza tra il trattamento erogato dall'amministrazione o dall'ente di provenienza e quello spettante al personale di ruolo, sulla base di apposita tabella di corrispondenza adottata dal Garante, e comunque non inferiore al cinquanta per cento della retribuzione in godimento, con esclusione dell'indennità integrativa speciale.

5. In aggiunta al personale di ruolo, l'Ufficio può assumere direttamente dipendenti con contratto a tempo determinato, in numero non superiore a venti unità ivi compresi i consulenti assunti con contratto a tempo determinato ai sensi del comma 7.

6. Si applicano le disposizioni di cui all'articolo 30 del decreto legislativo n. 165 del 2001.

7. Nei casi in cui la natura tecnica o la delicatezza dei problemi lo richiedono, il Garante può avvalersi dell'opera di consulenti, i quali sono remunerati in base alle vigenti tariffe professionali ovvero sono assunti con contratti a tempo determinato, di durata non superiore a due anni, che possono essere rinnovati per non più di due volte.

8. Il personale addetto all'Ufficio del Garante ed i consulenti sono tenuti al segreto su ciò di cui sono venuti a conoscenza, nell'esercizio delle proprie funzioni, in ordine a notizie che devono rimanere segrete.

9. Il personale dell'Ufficio del Garante addetto agli accertamenti di cui all'articolo 158 riveste, in numero non superiore a cinque unità, nei limiti del servizio cui è destinato e secondo le rispettive attribuzioni, la qualifica di ufficiale o agente di polizia giudiziaria.

10. Le spese di funzionamento del Garante sono poste a carico di un fondo stanziato a tale scopo nel bilancio dello Stato e iscritto in apposito capitolo dello stato di previsione del

Ministero dell'economia e delle finanze. Il rendiconto della gestione finanziaria è soggetto al controllo della Corte dei conti.

CAPO III - ACCERTAMENTI E CONTROLLI

Art. 157. Richiesta di informazioni e di esibizione di documenti

1. Per l'espletamento dei propri compiti il Garante può richiedere al titolare, al responsabile, all'interessato o anche a terzi di fornire informazioni e di esibire documenti.

Art. 158. Accertamenti

1. Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

2. I controlli di cui al comma 1 sono eseguiti da personale dell'Ufficio. Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato.

3. Gli accertamenti di cui al comma 1, se svolti in un'abitazione o in un altro luogo di privata dimora o nelle relative appartenenze, sono effettuati con l'assenso informato del titolare o del responsabile, oppure previa autorizzazione del presidente del tribunale competente per territorio in relazione al luogo dell'accertamento, il quale provvede con decreto motivato senza ritardo, al più tardi entro tre giorni dal ricevimento della richiesta del Garante quando è documentata l'indifferibilità dell'accertamento.

Art. 159. Modalità

1. Il personale operante, munito di documento di riconoscimento, può essere assistito ove necessario da consulenti tenuti al segreto ai sensi dell'articolo 156, comma 8. Nel procedere a rilievi e ad operazioni tecniche può altresì estrarre copia di ogni atto, dato e documento, anche a campione e su supporto informatico o per via telematica. Degli accertamenti è redatto sommario verbale nel quale sono annotate anche le eventuali dichiarazioni dei presenti.

2. Ai soggetti presso i quali sono eseguiti gli accertamenti è consegnata copia dell'autorizzazione del presidente del tribunale, ove rilasciata. I medesimi soggetti sono tenuti a farli eseguire e a prestare la collaborazione a tal fine necessaria. In caso di rifiuto gli accertamenti sono comunque eseguiti e le spese in tal caso occorrenti sono poste a carico del titolare con il provvedimento che definisce il procedimento, che per questa parte costituisce titolo esecutivo ai sensi degli articoli 474 e 475 del codice di procedura civile.

3. Gli accertamenti, se effettuati presso il titolare o il responsabile, sono eseguiti dandone informazione a quest'ultimo o, se questo è assente o non è designato, agli incaricati. Agli accertamenti possono assistere persone indicate dal titolare o dal responsabile.

4. Se non è disposto diversamente nel decreto di autorizzazione del presidente del tribunale, l'accertamento non può essere iniziato prima delle ore sette e dopo le ore venti, e può essere eseguito anche con preavviso quando ciò può facilitarne l'esecuzione.

5. Le informative, le richieste e i provvedimenti di cui al presente articolo e agli articoli 157 e 158 possono essere trasmessi anche mediante posta elettronica e telefax.

6. Quando emergono indizi di reato si osserva la disposizione di cui all'articolo 220 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271.

Art. 160. Particolari accertamenti

1. Per i trattamenti di dati personali indicati nei titoli I, II e III della Parte II gli accertamenti sono effettuati per il tramite di un componente designato dal Garante.

2. Se il trattamento non risulta conforme alle disposizioni di legge o di regolamento, il Garante indica al titolare o al responsabile le necessarie modificazioni ed integrazioni e ne verifica l'attuazione. Se l'accertamento è stato richiesto dall'interessato, a quest'ultimo è fornito in ogni caso un riscontro circa il relativo esito, se ciò non pregiudica azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione di reati o ricorrono motivi di difesa o di sicurezza dello Stato.

3. Gli accertamenti non sono delegabili. Quando risulta necessario in ragione della specificità della verifica, il componente designato può farsi assistere da personale specializzato tenuto al segreto ai sensi dell'articolo 156, comma 8. Gli atti e i documenti acquisiti sono custoditi secondo modalità tali da assicurarne la segretezza e sono conoscibili dal presidente e dai componenti del Garante e, se necessario per lo svolgimento delle funzioni dell'organo, da un numero delimitato di addetti all'Ufficio individuati dal Garante sulla base di criteri definiti dal regolamento di cui all'articolo 156, comma 3, lettera a).

4. Per gli accertamenti relativi agli organismi di informazione e di sicurezza e ai dati coperti da segreto di Stato il componente designato prende visione degli atti e dei documenti rilevanti e riferisce oralmente nelle riunioni del Garante.

5. Nell'effettuare gli accertamenti di cui al presente articolo nei riguardi di uffici giudiziari, il Garante adotta idonee modalità nel rispetto delle reciproche attribuzioni e della particolare collocazione istituzionale dell'organo procedente. Gli accertamenti riferiti ad atti di indagine coperti dal segreto sono differiti, se vi è richiesta dell'organo procedente, al momento in cui cessa il segreto.

6. La validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale.

TITOLO III - SANZIONI

CAPO I - VIOLAZIONI AMMINISTRATIVE

Art. 161. Omessa o inidonea informativa all'interessato

1. La violazione delle disposizioni di cui all'articolo 13 è punita con la sanzione amministrativa del pagamento di una somma da tremila euro a diciottomila euro o, nei casi di dati sensibili o giudiziari o di trattamenti che presentano rischi specifici ai sensi dell'articolo 17 o, comunque, di maggiore rilevanza del pregiudizio per uno o più interessati, da cinquemila euro a trentamila euro. La somma può essere aumentata sino al triplo quando risulta inefficace in ragione delle condizioni economiche del contravventore.

Art. 162. Altre fattispecie

1. La cessione dei dati in violazione di quanto previsto dall'articolo 16, comma 1, lettera b), o di altre disposizioni in materia di disciplina del trattamento dei dati personali è punita con la sanzione amministrativa del pagamento di una somma da cinquemila euro a trentamila euro.

2. La violazione della disposizione di cui all'articolo 84, comma 1, è punita con la sanzione amministrativa del pagamento di una somma da cinquecento euro a tremila euro.

Art. 163. Omessa o incompleta notificazione

1. Chiunque, essendovi tenuto, non provvede tempestivamente alla notificazione ai sensi degli articoli 37 e 38, ovvero indica in essa notizie incomplete, è punito con la sanzione amministrativa del pagamento di una somma da diecimila euro a sessantamila euro e con la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

Art. 164. Omessa informazione o esibizione al Garante

1. Chiunque omette di fornire le informazioni o di esibire i documenti richiesti dal Garante ai sensi degli articoli 150, comma 2, e 157 è punito con la sanzione amministrativa del pagamento di una somma da lire quattromila euro a lire ventiquattromila euro.

Art. 165. Pubblicazione del provvedimento del Garante

1. Nei casi di cui agli articoli 161, 162 e 164 può essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, in uno o più giornali indicati nel provvedimento che la applica.

Art. 166. Procedimento di applicazione

1. L'organo competente a ricevere il rapporto e ad irrogare le sanzioni di cui al presente capo e all'articolo 179, comma 3, è il Garante. Si osservano, in quanto applicabili, le disposizioni della legge 24 novembre 1981, n. 689, e successive modificazioni. I proventi, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 10, e sono utilizzati unicamente per l'esercizio dei compiti di cui agli articoli 154, comma 1, lettera h), e 158.

CAPO II - ILLECITI PENALI

Art. 167. Trattamento illecito di dati

1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi.

2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni.

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

1. Chiunque, nella notificazione di cui all'articolo 37 o in comunicazioni, atti, documenti o dichiarazioni resi o esibiti in un procedimento dinanzi al Garante o nel corso di accertamenti, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.

Art. 169. Misure di sicurezza

1. Chiunque, essendovi tenuto, omette di adottare le misure minime previste dall'articolo 33 è punito con l'arresto sino a due anni o con l'ammenda da diecimila euro a cinquantamila euro.

2. All'autore del reato, all'atto dell'accertamento o, nei casi complessi, anche con successivo atto del Garante, è impartita una prescrizione fissando un termine per la regolarizzazione non eccedente il periodo di tempo tecnicamente necessario, prorogabile in caso di particolare complessità o per l'oggettiva difficoltà dell'adempimento e comunque non superiore a sei mesi. Nei sessanta giorni successivi allo scadere del termine, se risulta l'adempimento alla prescrizione, l'autore del reato è ammesso dal Garante a pagare una somma pari al quarto del massimo dell'ammenda stabilita per la contravvenzione. L'adempimento e il pagamento estinguono il reato. L'organo che impartisce la prescrizione e il pubblico ministero provvedono nei modi di cui agli articoli 21, 22, 23 e 24 del decreto legislativo 19 dicembre 1994, n. 758, e successive modificazioni, in quanto applicabili.

Art. 170. Inosservanza di provvedimenti del Garante

1. Chiunque, essendovi tenuto, non osserva il provvedimento adottato dal Garante ai sensi degli articoli 26, comma 2, 90, 150, commi 1 e 2, e 143, comma 1, lettera c), è punito con la reclusione da tre mesi a due anni.

Art. 171. Altre fattispecie

1. La violazione delle disposizioni di cui agli articoli 113, comma 1, e 114 è punita con le sanzioni di cui all'articolo 38 della legge 20 maggio 1970, n. 300.

Art. 172. Pene accessorie

1. La condanna per uno dei delitti previsti dal presente codice importa la pubblicazione della sentenza.

TITOLO IV - DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

CAPO I - DISPOSIZIONI DI MODIFICA

Art. 173. Convenzione di applicazione dell'Accordo di Schengen

1. La legge 30 settembre 1993, n. 388, e successive modificazioni, di ratifica ed esecuzione dei protocolli e degli accordi di adesione all'Accordo di Schengen e alla relativa convenzione di applicazione, è così modificata:

a) il comma 2 dell'articolo 9 è sostituito dal seguente:

"2. Le richieste di accesso, rettifica o cancellazione, nonché di verifica, di cui, rispettivamente, agli articoli 109, 110 e 114, paragrafo 2, della Convenzione, sono rivolte all'autorità di cui al comma 1.";

b) il comma 2 dell'articolo 10 è soppresso;

c) l'articolo 11 è sostituito dal seguente:

"11.1. L'autorità di controllo di cui all'articolo 114 della Convenzione è il Garante per la protezione dei dati personali. Nell'esercizio dei compiti ad esso demandati per legge, il Garante esercita il controllo sui trattamenti di dati in applicazione della Convenzione ed esegue le verifiche previste nel medesimo articolo 114, anche su segnalazione o reclamo dell'interessato all'esito di un inidoneo riscontro alla richiesta rivolta ai sensi dell'articolo 9, comma 2, quando non è possibile fornire al medesimo interessato una risposta sulla base degli elementi forniti dall'autorità di cui all'articolo 9, comma 1. 2. Si applicano le disposizioni dell'articolo 10, comma 5, della legge 1° aprile 1981, n. 121, e successive modificazioni.";

d) l'articolo 12 è abrogato.

Art. 174. Notifiche di atti e vendite giudiziarie

1. All'articolo 137 del codice di procedura civile, dopo il secondo comma, sono inseriti i seguenti:

"Se la notificazione non può essere eseguita in mani proprie del destinatario, tranne che nel caso previsto dal secondo comma dell'articolo 143, l'ufficiale giudiziario consegna o deposita la copia dell'atto da notificare in busta che provvede a sigillare e su cui trascrive il numero cronologico della notificazione, dandone atto nella relazione in calce all'originale e alla copia dell'atto stesso. Sulla busta non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto.

Le disposizioni di cui al terzo comma si applicano anche alle comunicazioni effettuate con biglietto di cancelleria ai sensi degli articoli 133 e 136.".

2. Al primo comma dell'articolo 138 del codice di procedura civile, le parole da: "può sempre eseguire" a "destinatario," sono sostituite dalle seguenti: *"esegue la notificazione di regola mediante consegna della copia nelle mani proprie del destinatario, presso la casa di abitazione oppure, se ciò non è possibile,".*

3. Nel quarto comma dell'articolo 139 del codice di procedura civile, la parola: "l'originale" è sostituita dalle seguenti: *"una ricevuta"*.

4. Nell'articolo 140 del codice di procedura civile, dopo le parole: "affigge avviso del deposito" sono inserite le seguenti: *"in busta chiusa e sigillata"*.

5. All'articolo 142 del codice di procedura civile sono apportate le seguenti modificazioni:

a) il primo e il secondo comma sono sostituiti dal seguente: *"Salvo quanto disposto nel secondo comma, se il destinatario non ha residenza, dimora o domicilio nello Stato e non vi ha eletto domicilio o costituito un procuratore a norma dell'articolo 77, l'atto è notificato mediante spedizione al destinatario per mezzo della posta con raccomandata e mediante consegna di altra copia al pubblico ministero che ne cura la trasmissione al Ministero degli affari esteri per la consegna alla persona alla quale è diretta."*;

b) nell'ultimo comma le parole: "ai commi precedenti" sono sostituite dalle seguenti: *"al primo comma"*.

6. Nell'articolo 143, primo comma, del codice di procedura civile, sono soppresse le parole da: *", e mediante"* fino alla fine del periodo.

7. All'articolo 151, primo comma, del codice di procedura civile dopo le parole: "maggiore celerità" sono aggiunte le seguenti: *", di riservatezza o di tutela della dignità"*.

8. All'articolo 250 del codice di procedura civile dopo il primo comma è aggiunto il seguente: *"L'intimazione di cui al primo comma, se non è eseguita in mani proprie del destinatario o mediante servizio postale, è effettuata in busta chiusa e sigillata."*.

9. All'articolo 490, terzo comma, del codice di procedura civile è aggiunto, in fine, il seguente periodo: *"Nell'avviso è omessa l'indicazione del debitore"*.

10. All'articolo 570, primo comma, del codice di procedura civile le parole: "del debitore," sono soppresse e le parole da: "informazioni" fino alla fine sono sostituite dalle seguenti: *"informazioni, anche relative alle generalità del debitore, possono essere fornite dalla cancelleria del tribunale a chiunque vi abbia interesse"*.

11. All'articolo 14, quarto comma, della legge 24 novembre 1981, n. 689, e successive modificazioni, è aggiunto, in fine, il seguente periodo: *"Quando la notificazione non può essere eseguita in mani proprie del destinatario, si osservano le modalità previste dall'articolo 137, terzo comma, del medesimo codice."*.

12. Dopo l'articolo 15 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è inserito il seguente:

*"Articolo 15-*bis. *(Notificazioni di atti e documenti, comunicazioni ed avvisi) 1. Alla notificazione di atti e di documenti da parte di organi delle pubbliche amministrazioni a soggetti diversi dagli interessati o da persone da essi delegate, nonché a comunicazioni ed avvisi circa il relativo contenuto, si applicano le disposizioni contenute nell'articolo 137, terzo comma, del codice di procedura civile. Nei biglietti e negli inviti di presentazione sono indicate le informazioni strettamente necessarie a tale fine."*.

13. All'articolo 148 del codice di procedura penale sono apportate le seguenti modificazioni:

a) il comma 3 è sostituito dal seguente:

"3. L'atto è notificato per intero, salvo che la legge disponga altrimenti, di regola mediante consegna di copia al destinatario oppure, se ciò non è possibile, alle persone indicate nel presente titolo. Quando la notifica non può essere eseguita in mani proprie del destinatario, l'ufficiale giudiziario o la polizia giudiziaria consegnano la copia dell'atto da notificare, fatta eccezione per il caso di notificazione al difensore o al domiciliatario, dopo averla inserita in busta che provvedono a sigillare trascrivendovi il numero cronologico della notificazione e dandone atto nella relazione in calce all'originale e alla copia dell'atto.";

b) dopo il comma 5 è aggiunto il seguente:

"5-bis. Le comunicazioni, gli avvisi ed ogni altro biglietto o invito consegnati non in busta chiusa a persona diversa dal destinatario recano le indicazioni strettamente necessarie.".

14. All'articolo 157, comma 6, del codice di procedura penale le parole: "è scritta all'esterno del plico stesso" sono sostituite dalle seguenti: *"è effettuata nei modi previsti dall'articolo 148, comma 3".*

15. All'art. 80 delle disposizioni di attuazione del codice di procedura penale, approvate con decreto legislativo 28 luglio 1989, n. 271, il comma 1 è sostituito dal seguente:

"1. Se la copia del decreto di perquisizione locale è consegnata al portiere o a chi ne fa le veci, si applica la disposizione di cui all'articolo 148, comma 3, del codice.".

16. Alla legge 20 novembre 1982, n. 890, sono apportate le seguenti modificazioni:

a) all'articolo 2, primo comma, è aggiunto, in fine, il seguente periodo: *"Sulle buste non sono apposti segni o indicazioni dai quali possa desumersi il contenuto dell'atto.";*

b) all'articolo 8, secondo comma, secondo periodo, dopo le parole: "L'agente postale rilascia avviso" sono inserite le seguenti: *", in busta chiusa, del deposito".*

Art. 175. Forze di polizia

1. Il trattamento effettuato per il conferimento delle notizie ed informazioni acquisite nel corso di attività amministrative ai sensi dell'articolo 21, comma 1, della legge 26 marzo 2001, n. 128, e per le connessioni di cui al comma 3 del medesimo articolo è oggetto di comunicazione al Garante ai sensi dell'articolo 39, commi 2 e 3.

2. I dati personali trattati dalle forze di polizia, dagli organi di pubblica sicurezza e dagli altri soggetti di cui all'articolo 53, comma 1, senza l'ausilio di strumenti elettronici anteriormente alla data di entrata in vigore del presente codice, in sede di applicazione del presente codice possono essere ulteriormente trattati se ne è verificata l'esattezza, completezza ed aggiornamento ai sensi dell'articolo 11.

3. L'articolo 10 della legge 1° aprile 1981, n. 121, e successive modificazioni, è sostituito dal seguente:

"Art. 10. Controlli

1. Il controllo sul Centro elaborazione dati è esercitato dal Garante per la protezione dei dati personali, nei modi previsti dalla legge e dai regolamenti.

2. I dati e le informazioni conservati negli archivi del Centro possono essere utilizzati in procedimenti giudiziari o amministrativi soltanto attraverso l'acquisizione delle fonti originarie indicate nel primo comma dell'articolo 7, fermo restando quanto stabilito dall'articolo 240 del codice di procedura penale. Quando nel corso di un procedimento giurisdizionale o amministrativo viene rilevata l'erroneità o l'incompletezza dei dati e delle informazioni, o l'illegittimità del loro trattamento, l'autorità precedente ne dà notizia al Garante per la protezione dei dati personali.

3. La persona alla quale si riferiscono i dati può chiedere all'ufficio di cui alla lettera a) del primo comma dell'articolo 5 la conferma dell'esistenza di dati personali che lo riguardano, la loro comunicazione in forma intellegibile e, se i dati risultano trattati in violazione di vigenti disposizioni di legge o di regolamento, la loro cancellazione o trasformazione in forma anonima.

4. Esperiti i necessari accertamenti, l'ufficio comunica al richiedente, non oltre trenta giorni dalla richiesta, le determinazioni adottate. L'ufficio può omettere di provvedere sulla richiesta se ciò può pregiudicare azioni od operazioni a tutela dell'ordine e della sicurezza pubblica o di prevenzione e repressione della criminalità, dandone informazione al Garante per la protezione dei dati personali.

5. Chiunque viene a conoscenza dell'esistenza di dati personali che lo riguardano, trattati anche in forma non automatizzata in violazione di disposizioni di legge o di regolamento, può chiedere al tribunale del luogo ove risiede il titolare del trattamento di compiere gli accertamenti necessari e di ordinare la rettifica, l'integrazione, la cancellazione o la trasformazione in forma anonima dei dati medesimi.".

Art. 176. Soggetti pubblici

1. Nell'articolo 24, comma 3, della legge 7 agosto 1990, n. 241, dopo le parole: "mediante strumenti informatici" sono inserite le seguenti: *", fuori dei casi di accesso a dati personali da parte della persona cui i dati si riferiscono,".*

2. Nell'articolo 2 del decreto legislativo 30 marzo 2001, n. 165, in materia di ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche, dopo il comma 1 è inserito il seguente: *"1-bis. I criteri di organizzazione di cui al presente articolo sono attuati nel rispetto della disciplina in materia di trattamento dei dati personali.".*

3. L'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, e successive modificazioni, è sostituito dal seguente: *"1. è istituito il Centro nazionale per l'informatica nella pubblica amministrazione, che opera presso la Presidenza del Consiglio dei ministri per l'attuazione delle politiche del Ministro per l'innovazione e le tecnologie, con autonomia tecnica, funzionale, amministrativa, contabile e finanziaria e con indipendenza di giudizio.".*

4. Al Centro nazionale per l'informatica nella pubblica amministrazione continuano ad applicarsi l'articolo 6 del decreto legislativo 12 febbraio 1993, n. 39, nonché le vigenti modalità di finanziamento nell'ambito dello stato di previsione del Ministero dell'economia e delle finanze.

5. L'articolo 5, comma 1, del decreto legislativo n. 39 del 1993, e successive modificazioni, è sostituito dal seguente: *"1. Il Centro nazionale propone al Presidente del Consiglio dei ministri l'adozione di regolamenti concernenti la sua organizzazione, il suo funzionamento, l'amministrazione del personale, l'ordinamento delle carriere, nonché la gestione delle spese nei limiti previsti dal presente decreto.".*

6. La denominazione: "Autorità per l'informatica nella pubblica amministrazione" contenuta nella vigente normativa è sostituita dalla seguente: *"Centro nazionale per l'informatica nella pubblica amministrazione".*

Art. 177. Disciplina anagrafica, dello stato civile e delle liste elettorali

1. Il comune può utilizzare gli elenchi di cui all'articolo 34, comma 1, del decreto del Presidente della Repubblica 30 maggio 1989, n. 223, per esclusivo uso di pubblica utilità anche in caso di applicazione della disciplina in materia di comunicazione istituzionale.

2. Il comma 7 dell'articolo 28 della legge 4 maggio 1983, n. 184, e successive modificazioni, è sostituito dal seguente: *"7. L'accesso alle informazioni non è consentito nei confronti della madre che abbia dichiarato alla nascita di non volere essere nominata ai sensi dell'articolo 30, comma 1, del decreto del Presidente della Repubblica 3 novembre 2000, n. 396.".*

3. Il rilascio degli estratti degli atti dello stato civile di cui all'articolo 107 del decreto del Presidente della Repubblica 3 novembre 2000, n. 396 è consentito solo ai soggetti cui l'atto si riferisce, oppure su motivata istanza comprovante l'interesse personale e concreto del richiedente a fini di tutela di una situazione giuridicamente rilevante, ovvero decorsi settanta anni dalla formazione dell'atto.

4. Nel primo comma dell'articolo 5 del decreto del Presidente della Repubblica 20 marzo 1967, n. 223, sono soppresse le lettere d) ed e).

5. Nell'articolo 51 del decreto del Presidente della Repubblica 20 marzo 1967, n. 223, il quinto comma è sostituto dal seguente: *"Le liste elettorali possono essere rilasciate in copia*

per finalità di applicazione della disciplina in materia di elettorato attivo e passivo, di studio, di ricerca statistica, scientifica o storica, o carattere socio-assistenziale o per il perseguimento di un interesse collettivo o diffuso.".

Art. 178. Disposizioni in materia sanitaria

1. Nell'articolo 27, terzo e quinto comma, della legge 23 dicembre 1978, n. 833, in materia di libretto sanitario personale, dopo le parole: "il Consiglio sanitario nazionale" e prima della virgola sono inserite le seguenti: *"e il Garante per la protezione dei dati personali".*

2. All'articolo 5 della legge 5 giugno 1990, n. 135, in materia di AIDS e infezione da HIV, sono apportate le seguenti modifiche:

a) il comma 1 è sostituito dal seguente: *"1. L'operatore sanitario e ogni altro soggetto che viene a conoscenza di un caso di AIDS, ovvero di un caso di infezione da HIV, anche non accompagnato da stato morboso, è tenuto a prestare la necessaria assistenza e ad adottare ogni misura o accorgimento occorrente per la tutela dei diritti e delle libertà fondamentali dell'interessato, nonché della relativa dignità.";*

b) nel comma 2, le parole: "decreto del Ministro della sanità" sono sostituite dalle seguenti: *"decreto del Ministro della salute, sentito il Garante per la protezione dei dati personali".*

3. Nell'articolo 5, comma 3, del decreto legislativo 30 dicembre 1992, n. 539, e successive modificazioni, in materia di medicinali per uso umano, è inserito, in fine, il seguente periodo: *"Decorso tale periodo il farmacista distrugge le ricette con modalità atte ad escludere l'accesso di terzi ai dati in esse contenuti.".*

4. All'articolo 2, comma 1, del decreto del Ministro della sanità in data 11 febbraio 1997, pubblicato sulla *Gazzetta Ufficiale* n. 72 del 27 marzo 1997, in materia di importazione di medicinali registrati all'estero, sono soppresse le lettere f) ed h).

5. Nel comma 1, primo periodo, dell'articolo 5-*bis* del decreto legge 17 febbraio 1998, n. 23, convertito, con modificazioni, dalla legge 8 aprile 1998, n. 94, le parole da: "riguarda anche" fino alla fine del periodo sono sostituite dalle seguenti: *"è acquisito unitamente al consenso relativo al trattamento dei dati personali".*

Art. 179. Altre modifiche

1. Nell'articolo 6 della legge 2 aprile 1958, n. 339, sono soppresse le parole: *"; mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare"* e: *"garantire al lavoratore il rispetto della sua personalità e della sua libertà morale;".*

2. Nell'articolo 38, primo comma, della legge 20 maggio 1970, n. 300, sono soppresse le parole: "4," e ",8".

3. Al comma 3 dell'articolo 12 del decreto legislativo 22 maggio 1999, n. 185, in materia di contratti a distanza, sono aggiunte in fine le seguenti parole: *", ovvero, limitatamente alla violazione di cui all'articolo 10, al Garante per la protezione dei dati personali".*

4. Dopo l'articolo 107 del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali, è inserito il seguente:

"Articolo 107-bis. Trattamento di dati personali per scopi storici

1. I documenti per i quali è autorizzata la consultazione ai sensi dell'articolo 107, comma 2, conservano il loro carattere riservato e non possono essere diffusi.

2. I documenti detenuti presso l'Archivio centrale dello Stato e gli Archivi di Stato sono conservati e consultabili anche in caso di esercizio dei diritti dell'interessato ai sensi dell'articolo 13 della legge 31 dicembre 1996, n. 675, qualora ciò risulti necessario per scopi storici. Ai documenti è allegata la documentazione relativa all'esercizio dei diritti. Su richiesta di chiunque vi abbia interesse ai sensi del medesimo articolo 13, può essere comunque disposto il blocco dei dati personali, qualora il loro trattamento comporti un concreto pericolo di lesione della dignità,

della riservatezza o dell'identità personale degli interessati e i dati non siano di rilevante interesse pubblico.".

CAPO II - DISPOSIZIONI TRANSITORIE

Art. 180. Misure di sicurezza

1. Le misure minime di sicurezza di cui agli articoli da 33 a 35 e all'allegato B) che non erano previste dal decreto del Presidente della Repubblica 28 luglio 1999, n. 318, sono adottate entro il 30 giugno 2004.

2. Il titolare che alla data di entrata in vigore del presente codice dispone di strumenti elettronici che, per obiettive ragioni tecniche, non consentono in tutto o in parte l'immediata applicazione delle misure minime di cui all'articolo 34 e delle corrispondenti modalità tecniche di cui all'allegato B), descrive le medesime ragioni in un documento a data certa da conservare presso la propria struttura.

3. Nel caso di cui al comma 2, il titolare adotta ogni possibile misura di sicurezza in relazione agli strumenti elettronici detenuti in modo da evitare, anche sulla base di idonee misure organizzative, logistiche o procedurali, un incremento dei rischi di cui all'articolo 31, adeguando i medesimi strumenti al più tardi entro un anno dall'entrata in vigore del codice.

Art. 181. Altre disposizioni transitorie

1. Per i trattamenti di dati personali iniziati prima del 1° gennaio 2004, in sede di prima applicazione del presente codice:

a) l'identificazione con atto di natura regolamentare dei tipi di dati e di operazioni ai sensi degli articoli 20, commi 2 e 3, e 21, comma 2, è effettuata, ove mancante, entro il 30 settembre 2004;
b) la determinazione da rendere nota agli interessati ai sensi dell'articolo 26, commi 3, lettera a), e 4, lettera a), è adottata, ove mancante, entro il 30 giugno 2004;
c) le notificazioni previste dall'articolo 37 sono effettuate entro il 30 aprile 2004;
d) le comunicazioni previste dall'articolo 39 sono effettuate entro il 30 giugno 2004;
e) le modalità semplificate per l'informativa e la manifestazione del consenso, ove necessario, possono essere utilizzate dal medico di medicina generale, dal pediatra di libera scelta e dagli organismi sanitari anche in occasione del primo ulteriore contatto con l'interessato, al più tardi entro il 30 settembre 2004;
f) l'utilizzazione dei modelli di cui all'articolo 87, comma 2, è obbligatoria a decorrere dal 1° gennaio 2005.

2. Le disposizioni di cui all'articolo 21-bis del decreto del Presidente della Repubblica 30 settembre 1963, n. 1409, introdotto dall'articolo 9 del decreto legislativo 30 luglio 1999, n. 281, restano in vigore fino alla data di entrata in vigore del presente codice.

3. L'individuazione dei trattamenti e dei titolari di cui agli articoli 46 e 53, da riportare nell'allegato C), è effettuata in sede di prima applicazione del presente codice entro il 30 giugno 2004.

4. Il materiale informativo eventualmente trasferito al Garante ai sensi dell'articolo 43, comma 1, della legge 31 dicembre 1996, n. 675, utilizzato per le opportune verifiche, continua ad essere successivamente archiviato o distrutto in base alla normativa vigente.

5. L'omissione delle generalità e degli altri dati identificativi dell'interessato ai sensi dell'articolo 52, comma 4, è effettuata sulle sentenze o decisioni pronunciate o adottate prima dell'entrata in vigore del presente codice solo su diretta richiesta dell'interessato e limitatamente ai documenti pubblicati mediante rete di comunicazione elettronica o sui nuovi prodotti su supporto cartaceo o elettronico. I sistemi informativi utilizzati ai sensi dell'articolo 51, comma 1, sono adeguati alla medesima disposizione entro dodici mesi dalla data di entrata in vigore del presente codice.

6. Le confessioni religiose che, prima dell'adozione del presente codice, abbiano determinato e adottato nell'ambito del rispettivo ordinamento le garanzie di cui all'articolo 26, comma 3, lettera a), possono proseguire l'attività di trattamento nel rispetto delle medesime.

6-bis. *(*) Fino alla data in cui divengono efficaci le misure e gli accorgimenti prescritti ai sensi dell'articolo 132, comma 5, per la conservazione del traffico telefonico si osserva il termine di cui all'articolo 4, comma 2, del decreto legislativo 13 maggio 1998, n. 171.*

Art. 182. Ufficio del Garante

1. Al fine di assicurare la continuità delle attività istituzionali, in sede di prima applicazione del presente codice e comunque non oltre il 31 marzo 2004, il Garante:

a) può individuare i presupposti per l'inquadramento in ruolo, al livello iniziale delle rispettive qualifiche e nei limiti delle disponibilità di organico, del personale appartenente ad amministrazioni pubbliche o ad enti pubblici in servizio presso l'Ufficio del Garante in posizione di fuori ruolo o equiparato alla data di pubblicazione del presente codice;

b) può prevedere riserve di posti nei concorsi pubblici, unicamente nel limite del trenta per cento delle disponibilità di organico, per il personale non di ruolo in servizio presso l'Ufficio del Garante che abbia maturato un'esperienza lavorativa presso il Garante di almeno un anno.

CAPO III - ABROGAZIONI

Art. 183. Norme abrogate

1. Dalla data di entrata in vigore del presente codice sono abrogati:

a) la legge 31 dicembre 1996, n. 675;
b) la legge 3 novembre 2000, n. 325;
c) il decreto legislativo 9 maggio 1997, n. 123;
d) il decreto legislativo 28 luglio 1997, n. 255;
e) l'articolo 1 del decreto legislativo 8 maggio 1998, n. 135;
f) il decreto legislativo 13 maggio 1998, n. 171;
g) il decreto legislativo 6 novembre 1998, n. 389;
h) il decreto legislativo 26 febbraio 1999, n. 51;
i) il decreto legislativo 11 maggio 1999, n. 135;
l) il decreto legislativo 30 luglio 1999, n. 281, ad eccezione degli articoli 8, comma 1, 11 e 12;
m) il decreto legislativo 30 luglio 1999, n. 282;
n) il decreto legislativo 28 dicembre 2001, n. 467;
o) il decreto del Presidente della Repubblica 28 luglio 1999, n. 318.

2. Dalla data di entrata in vigore del presente codice sono abrogati gli articoli 12, 13, 14, 15, 16, 17, 18, 19 e 20 del decreto del Presidente della Repubblica 31 marzo 1998, n. 501.

3. Dalla data di entrata in vigore del presente codice sono o restano, altresì, abrogati:

a) l'art. 5, comma 9, del decreto del Ministro della sanità 18 maggio 2001, n. 279, in materia di malattie rare;
b) l'articolo 12 della legge 30 marzo 2001, n. 152;
c) l'articolo 4, comma 3, della legge 6 marzo 2001, n. 52, in materia di donatori midollo osseo;
d) l'articolo 16, commi 2 e 3, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, in materia di certificati di assistenza al parto;
e) l'art. 2, comma 5, del decreto del Ministro della sanità 27 ottobre 2000, n. 380, in materia di flussi informativi sui dimessi dagli istituti di ricovero;
f) l'articolo 2, comma 5-*quater* 1, secondo e terzo periodo, del decreto legge 28 marzo 2000, n. 70, convertito, con modificazioni, dalla legge 26 maggio 2000, n. 137, e successive modificazioni, in materia di banca dati sinistri in ambito assicurativo;
g) l'articolo 6, comma 4, del decreto legislativo 5 giugno 1998, n. 204, in materia di diffusione di dati a fini di ricerca e collaborazione in campo scientifico e tecnologico;

(*) Comma aggiunto dall'articolo 4 del decreto legge 24 dicembre 2003, n. 354, nel testo modificato dalla legge 26 febbraio 2004, n. 45, di conversione del predetto decreto legge

h) l'articolo 330-bis del decreto legislativo 16 aprile 1994, n. 297, in materia di diffusione di dati relativi a studenti;
i) l'articolo 8, quarto comma, e l'articolo 9, quarto comma, della legge 1° aprile 1981, n. 121.

4. Dalla data in cui divengono efficaci le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 118, i termini di conservazione dei dati personali individuati ai sensi dell'articolo 119, eventualmente previsti da norme di legge o di regolamento, si osservano nella misura indicata dal medesimo codice.

CAPO IV - NORME FINALI

Art. 184. Attuazione di direttive europee

1. Le disposizioni del presente codice danno attuazione alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, e alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002.

2. Quando leggi, regolamenti e altre disposizioni fanno riferimento a disposizioni comprese nella legge 31 dicembre 1996, n. 675, e in altre disposizioni abrogate dal presente codice, il riferimento si intende effettuato alle corrispondenti disposizioni del presente codice secondo la tavola di corrispondenza riportata in allegato.

3. Restano ferme le disposizioni di legge e di regolamento che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati personali.

Art. 185. Allegazione dei codici di deontologia e di buona condotta

1. L'allegato A) riporta, oltre ai codici di cui all'articolo 12, commi 1 e 4, quelli promossi ai sensi degli articoli 25 e 31 della legge 31 dicembre 1996, n. 675, e già pubblicati nella *Gazzetta Ufficiale* della Repubblica italiana alla data di emanazione del presente codice.

Art. 186. Entrata in vigore

1. Le disposizioni di cui al presente codice entrano in vigore il 1° gennaio 2004, ad eccezione delle disposizioni di cui agli articoli 156, 176, commi 3, 4, 5 e 6 e 182, che entrano in vigore il giorno successivo alla data di pubblicazione del presente codice. Dalla medesima data si osservano altresì i termini in materia di ricorsi di cui agli articoli 149, comma 8, e 150, comma 2.

Il presente decreto, munito del sigillo dello Stato, sarà inserito nella Raccolta ufficiale degli atti normativi della Repubblica italiana. È fatto obbligo a chiunque spetti di osservarlo e di farlo osservare.

Dato a Roma, addì 30 giugno 2003

TAVOLA DI CORRISPONDENZA DEI RIFERIMENTI PREVIGENTI

Tavola di corrispondenza dei riferimenti previgenti al Codice in materia di protezione dei dati personali

ARTICOLATO DEL CODICE	RIFERIMENTO PREVIGENTE
PARTE I - DISPOSIZIONI GENERALI	
TITOLO I - PRINCIPI GENERALI	
Art. 1. Diritto alla protezione dei dati personali	—
Art. 2. Finalità	
comma 1	cfr. art. 1, direttiva n. 95/46/CE art. 1, comma 1, legge 31 dicembre 1996, n. 675
comma 2	—
Art. 3. Principio di necessità del trattamento dei dati	
comma 1	—
Art. 4 (Definizioni)	
comma 1, lett. a)	cfr. art. 2, dir. n. 95/46/CE art. 1, comma 2, lett. b), l. n. 675/1996
lett. b)	art. 1, comma 2, lett. c), l. n. 675/1996
lett. c)	art. 10, comma 5, d.lg. 30 luglio 1999, n. 281
lett. d)	cfr. art. 22, comma 1, l. n. 675/1996
lett. e)	cfr. art. 24, comma 1, l. n. 675/1996
lett. f)	art. 1, comma 2, lett. d), l. n. 675/1996
lett. g)	art. 1, comma 2, lett. e), l. n. 675/1996
lett. h)	cfr. art. 19, l. n. 675/1996
lett. i)	art. 1, comma 2, lett. f), l. n. 675/1996
lett. l)	art. 1, comma 2, lett. g), l. n. 675/1996
lett. m)	art. 1, comma 2, lett. h), l. n. 675/1996
lett. n)	art. 1, comma 2, lett. i), l. n. 675/1996
lett. o)	art. 1, comma 2, lett. l), l. n. 675/1996
lett. p)	art. 1, comma 2, lett. a), l. n. 675/1996
lett. q)	art. 1, comma 2, lett. m), l. n. 675/1996
comma 2, lett. a)	cfr. art. 2, par. 2, lett. d), direttiva del Parlamento europeo e del Consiglio n. 2002/58/CE
lett. b)	cfr. art. 2, lett. e), dir. n. 2002/58/CE
lett. c)	cfr. art. 2, par. 1, lett. a), direttiva del Parlamento europeo e del Consiglio n. 2002/21/CE
lett. d)	cfr. art. 2, par. 1, lett. d), dir. n. 2002/21/CE
lett. e)	cfr. art. 2, par. 1, lett. c), dir. n. 2002/21/CE
lett. f)	cfr. art. 2, par. 1, lett. k), dir. n. 2002/21/CE
lett. g)	cfr. art. 2, par. 2, lett. a), dir. n. 2002/58/CE
lett. h)	cfr. art. 2, par. 2,lett. b), dir. n. 2002/58/CE
lett. i)	cfr. art. 2, par. 2, lett. c), dir. n. 2002/58/CE
lett. l)	cfr. art. 2, par. 2, lett. g), dir. n. 2002/58/CE
lett. m)	cfr. art. 2, par. 2, lett. h), dir. n. 2002/58/CE
comma 3, lett. a)	art. 1, comma 1, lett. a), d.P.R. n. 28 luglio 1999, n. 318
lett. b)	art. 1, lett. b, d.P.R. n. 318/1999
lett. c)	—
lett. d)	—
lett. e)	—
lett. f)	—

lett. g)	—
comma 4, lett. a)	art. 1, comma 2, lett. a), d.lg. n. 281/1999
lett. b)	art. 1, comma 2, lett. c), d.lg. n. 281/1999
lett. c)	art. 1, comma 2, lett. b), d.lg. n. 281/1999

Art. 5. Oggetto ed ambito di applicazione

comma 1	cfr. art. 4, dir. n. 95/46/CE
	artt. 2, comma 1, e 6, comma 1, l. n. 675/1996
comma 2	art. 2, commi 1 bis, e 1 ter, l. n. 675/1996
comma 3	cfr. art. 3, par. 2 (secondo periodo), dir. n. 95/46/CE
	art. 3, l. n. 675/1996

Art. 6. Disciplina del trattamento —

TITOLO II - DIRITTI DELL'INTERESSATO

Art. 7. Diritto di accesso ai dati personalied altri diritti

comma 1	cfr. art. 12, dir. n. 95/46/CE
	art. 13, comma 1, lett. c), punto 1 (prima parte) l. n. 675/1996
comma 2	art. 13, comma 1, lett. b) e c), punto 1 (seconda parte) l. n. 675/1996
comma 3	art. 13, comma 1, lett. c), punti 2, 3 e 4, l. n. 675/1996
comma 4	art. 13, comma 1, lett. d) ed e), l. n. 675/1996

Art. 8. Esercizio dei diritti

comma 1	cfr. art. 13, dir. 95/46/CE
	art. 17, comma 1, d.P.R. 31 marzo 1998, n. 501
comma 2	art. 14, comma 1, lett. a), b), c), d), e) ed e-bis) l. n. 675/1996
comma 3	art. 14, comma 2, n. 675/1996
comma 4	—

Art. 9. Modalità di esercizio

comma 1	art. 17, comma 3, d.P.R. n. 501/1998
comma 2	art. 13, comma 4, l. n. 675/1996; art. 17, comma 4, d.P.R. n. 501/1998
comma 3	art. 13, comma 3 , l. n. 675/1996
comma 4	art. 17, comma 2, d.P.R. n. 501/1998
comma 5	art. 13, comma 1, c), punto 1 (secondo periodo), l. n. 675/1996

Art. 10. Riscontro all'interessato

comma 1	art. 17, comma 9, d.P.R. n. 501/1998
comma 2	art. 17, comma 6, d.P.R. n. 501/1998
comma 3	art. 17, comma 5, d.P.R. n. 501/1998
comma 4	—
comma 5	—
comma 6	—
comma 7	art. 13, comma 2, l. n. 675/1996; art. 17, comma 7, d.P.R. n. 501/1998
comma 8	art. 17, comma 7, d.P.R. n. 501/1998
comma 9	art. 17, comma 8, d.P.R. n. 501/1998

TITOLO III - REGOLE GENERALI PER IL TRATTAMENTO DEI DATI

CAPO I - REGOLE PER TUTTI I TRATTAMENTI

Art. 11. Modalità del trattamento e requisiti dei dati

comma 1	cfr. art. 6, dir. n. 95/46/CE
	art. 9, comma 1, l. n. 675/1996
comma 2	—

Art. 12. Codici di deontologia e di buona condotta

comma 1	cfr. art. 27, dir. n. 95/46/CE
	art. 31, comma 1, lett. h), l. n. 675/1996
comma 2	art. 20, comma 4, d.lg. 28 dicembre 2001, n. 467
comma 3	art. 20, comma 3, d.lg. n. 467/2001
comma 4	—

Art. 13. Informativa

comma 1	cfr. art. 10, dir. n. 95/46/CE
	art. 10, comma 1, l. n. 675/1996
comma 2	art. 10, comma 2, l. n. 675/1996
comma 3	—
comma 4	art. 10, comma 3, l. n. 675/1996
comma 5	art. 10, comma 4, l. n. 675/1996

Art. 14. Definizione di profili e della personalità dell'interessato

comma 1	cfr. art. 15, dir. n. 95/46/CE
	art. 17, comma 1, l. n. 675/1996
comma 2	art. 17, comma 2, l. n. 675/1996

Art. 15. Danni cagionati per effetto del trattamento

comma 1	cfr. art. 23, dir. n. 95/46/CE
	art. 18, l. n. 675/1996
comma 2	art. 29, comma 9, l. n. 675/1996

Art. 16. Cessazione del trattamento

comma 1	cfr. art. 19, par. 2, dir. n. 95/46/CE
	art. 16, comma 2, l. n. 675/1996
comma 2	art. 16, comma 3, l. n. 675/1996

Art. 17. Trattamento che presenta rischi specifici

comma 1	cfr. art. 20, dir. n. 95/46/CE
	art. 24-bis, comma 1, l. n. 675/1996
comma 2	art. 24-bis, comma 2, l. n. 675/1996

CAPO II - REGOLE ULTERIORI PER I SOGGETTI PUBBLICI

Art. 18. Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici

comma 1	—
comma 2	cfr. art. 27, comma 1, l. n. 675/1996
comma 3	cfr. art. 27, comma 1, l. n. 675/1996
comma 4	—
comma 5	—

Art. 19. Principi applicabili al trattamento di dati diversi da quelli sensibili e giudiziari

comma 1	art. 7, par. 1, lett. E), dir. n. 95/46/CE
	art. 27, comma 1, l. n. 675/1996
comma 2	art. 27, comma 2, l. n. 675/1996
comma 3	art. 27, comma 3, l. n. 675/1996

Art. 20. Principi applicabili al trattamento di dati sensibili

comma 1	cfr. art. 8, dir. n. 95/46/CE
	art. 22, comma 3, primo periodo, l. n. 675/1996
comma 2	art. 22, comma 3-bis, l. n. 675/1996; art. 5, comma 5, d.lg. 11 maggio 1999, n. 135
comma 3	art. 22, comma 3, secondo periodo, l. n. 675/1996
comma 4	art. 22, comma 3-bis, l. n.675/1996

Art. 21. Principi applicabili al trattamento di dati giudiziari

comma 1	cfr. art. 8, par. 5, dir. n. 95/46/CE

	art. 24, comma 1, l. n. 675/1996
comma 2	art. 5, comma 5-bis, d.lg. n. 135/1999

Art. 22. Principi applicabili al trattamento di dati sensibili e giudiziari

comma 1	—
comma 2	art. 2, comma 2, d.lg. n. 135/1999
comma 3	art. 3, comma 1, d.lg. n. 135/1999
comma 4	art. 3, comma 2, d.lg. n. 135/1999
comma 5	art. 3, comma 3, d.lg. n. 135/1999
comma 6	art. 3, comma 4, d.lg. n. 135/1999
comma 7	art. 3, comma 5, d.lg. n. 135/1999
comma 8	art. 23, comma 4, l. n. 675/1996
comma 9	art. 4, comma 1, d.lg. n. 135/1999
comma 10	art. 4, comma 2, d.lg. n. 135/1999
	art. 3, comma 6, d.lg. n. 135/1999
comma 11	art. 4, comma 3, d.lg. n. 135/1999
comma 12	art. 1, comma 2, lett. c), d.lg. n. 135/1999

CAPO III - REGOLE ULTERIORI PER I PRIVATI ED ENTI PUBBLICI ECONOMICI

Art. 23. Consenso

comma 1	cfr. art. 7, par. 1, lett. A), dir. n. 95/46/CE
	art. 11, comma 1 e 20, comma 1, lett. a) l. n. 675/1996
comma 2	art. 11, comma 2, l. n. 675/1996
comma 3	art. 11, comma 3, l. n. 675/1996
comma 4	cfr. art. 22, comma 1, l. n. 675/1996

Art. 24. Casi nei quali può essere effettuato il trattamento senza il consenso

comma 1, lett. a)	cfr. art. 7, dir. n. 95/46/CE
	artt. 12, comma 1, lett. a) e 20, comma 1, lett. c), l. n. 675/1996
lett. b)	artt. 12, comma 1, lett. b) e 20, comma 1, lett. a-bis), l. n. 675/1996
lett. c)	artt. 12, comma 1, lett. c) e 20, comma 1, lett. b), l. n. 675/1996
lett. d)	artt. 12, comma 1, lett. f) e 20, comma 1, lett. e), l. n. 675/1996
lett. e)	art. 7, par. 1, lett. d), dir. n. 95/46/CE
	artt. 12, comma 1, lett. g) e 20 comma 1, lett. f), l. n. 675/1996
lett. f)	artt. 12, comma 1, lett. h) e 20, comma 1, lett. g), l. n. 675/1996
lett. g)	artt. 12, comma 1, lett. h-bis) e 20, comma 1, lett. h ed h-bis), l. n. 675/1996
lett. h)	—
lett. i)	artt. 12, comma 1, lett. d) e 21, comma 4, lett. a), l. n. 675/1996
	art. 7, comma 4 d.lgs n. 281/1999

Art. 25. Divieti di comunicazione e diffusione

comma 1	art. 21 commi 1 e 2, l. n. 675/1996
comma 2	art. 21, comma 4, lett. b), l. n. 675/1996

Art. 26. Garanzie per i dati sensibili

comma 1	cfr. art. 8, dir. n. 95/46/CE
	art. 22, comma 1, l. n. 675/1996
comma 2	art. 22, comma 2, l. n. 675/1996
comma 3, lett. a)	art. 22, comma 1 bis, l. n. 675/1996
comma 3, lett. b)	art. 22, comma 1 ter, l. n. 675/1996
comma 4	art. 22, comma 4, l. n. 675/1996
comma 5	art. 23, comma 4, l. n. 675/1996

Art. 27. Garanzie per i dati giudiziari

comma 1	cfr. art. 8, par. 5, dir. n. 95/46/CE
	art. 24, comma 1, l. n. 675/1996

TITOLO IV - I SOGGETTI CHE EFFETTUANO IL TRATTAMENTO

Art. 28. Titolare del trattamento	
comma 1	—
Art. 29 (Responsabile del trattamento)	
comma 1	cfr. art. 16, dir. n. 95/46/CE
	art. 8, comma 1, l. n. 675/1996
comma 2	art. 8, comma 1, l. n. 675/1996
comma 3	art. 8, comma 3, l. n. 675/1996
comma 4	art. 8, comma 4, l. n. 675/1996
comma 5	art. 8, comma 2, l. n. 675/1996
Art. 30. Incaricati del trattamento	
comma 1	cfr. art. 17, par. 3, dir. n. 95/46/CE
	artt. 8, comma 5, e 19, l. n. 675/1996
comma 2	art. 19, l. n. 675/1996

TITOLO V - SICUREZZA DEI DATI E DEI SISTEMI

CAPO I - MISURE DI SICUREZZA	cfr. art. 17, dir. n. 95/46/CE
Art. 31. Obblighi di sicurezza	art. 15, comma 1, l. n. 675/1996
Art. 32. Particolari titolari	
comma 1	art. 2, comma 1, d.lg. 13 maggio 1998, n. 171
comma 2	art. 2, comma 2, d.lg. 171/1998
comma 3	art. 2, comma 3, d.lg. 171/1998

CAPO II - MISURE MINIME

Art. 33. Misure minime	cfr. art. 15, comma 2, l. n. 675/1996
Art. 34. Trattamenti con strumenti elettronici	—
Art. 35. Trattamenti senza l'ausilio di strumenti elettronici	—
Art. 36. Adeguamento	cfr. art. 15, comma 3, l. n. 675/1996

TITOLO VI - ADEMPIMENTI

Art. 37. Notificazione del trattamento	
comma 1	art. 18, dir. n. 95/46/CE; cfr. art. 7, comma 1, l. n. 675/1996
comma 2	—
comma 3	art. 28, comma 7, secondo periodo, l. n. 675/1996
comma 4	art. 13, commi 1, 2, 3, 4, d.P.R. n. 501/1998
Art. 38. Modalità di notificazione	
comma 1	art. 19, dir. n. 95/46/CE
	art. 7, comma 2, primo periodo, l. n. 675/1996
comma 2	art. 12, comma 1, primo periodo, d.P.R. n. 501/1998
comma 3	art. 12, comma 1, secondo periodo, d.P.R. n. 501/1998
comma 4	art. 7, comma 2, secondo periodo e art. 16, comma 1, l. n. 675/1996
comma 5	art. 12, comma 6, d.P.R. n. 501/1998
comma 6	—
Art. 39. Obblighi di comunicazione	
comma 1, lett. a)	art. 7, par. 1, lett. E), dir. n. 95/46/CE

	art. 27, comma 2, l. n. 675/1996
lett. b)	—
comma 2	—
comma 3	—
Art. 40. Autorizzazioni generali	
comma 1	art. 41, comma 7, l. n. 675/1996; art. 14, comma 1, d.P.R. n. 501/1998
Art. 41. Richieste di autorizzazione	
comma 1	—
comma 2	art. 14, comma 2, d.P.R. n. 501/1998
comma 3	art. 14, comma 3, d.P.R. n. 501/1998
comma 4	art. 14, comma 4, d.P.R. n. 501/1998
comma 5	art. 14, comma 5, d.P.R. n. 501/1998
TITOLO VII - TRASFERIMENTO DEI DATI ALL'ESTERO	cfr. artt. 25 e 26, dir. n. 95/46/CE
Art. 42. Trasferimenti all'interno dell'Unione europea	
comma 1	—
Art. 43. Trasferimenti consentiti in Paesi terzi	
alinea del comma 1	art. 28, comma 1, l. n. 675/1996
comma 1	artt. 28, comma 4, eccetto la lett. g), e 26, comma 2, l. n. 675/1996 art. 7, comma 4, d.lg n. 281/1999
Art. 44. Altri trasferimenti consentiti	art. 28, comma 4, lett. g), l. n. 675/1996
Art. 45. Trasferimenti vietati	art. 28, comma 3, l. n. 675/1996
PARTE II - DISPOSIZIONI RELATIVE A SPECIFICI SETTORI	
TITOLO I - TRATTAMENTI IN AMBITO GIUDIZIARIO	
CAPO I - PROFILI GENERALI	cfr. art. 3, dir. n. 95/46/CE
Art. 46. Titolari dei trattamenti	—
Art. 47. Trattamenti per ragioni di giustizia	art. 3, par. 2, (primo periodo) dir. n. 95/46/CE art. 4, comma 1, lett. c) e d) e comma 2, l. n. 675/1996
Art. 48. Banche di dati di uffici giudiziari	—
Art. 49. Disposizioni di attuazione	—
CAPO II - MINORI	
Art. 50. Notizie o immagini relative ai minori	—
CAPO III - INFORMATICA GIURIDICA	
Art. 51. Principi generali	—
Art. 52. Dati identificativi degli interessati	—

TITOLO II - TRATTAMENTI DA PARTE DI FORZE DI POLIZIA — cfr. art. 3, dir. n. 95/46/CE
CAPO I - PROFILI GENERALI

Art. 53. Ambito applicativo e titolari dei trattamenti	art. 3, par. 2, (primo periodo) dir. n. 95/46/CE art. 4, comma 1, lett. a) ed e) e comma 2, l. n. 675/1996
Art. 54. Modalità di trattamento e flussi di dati	—
Art. 55. Particolari tecnologie	—
Art. 56. Tutela dell'interessato	—
Art. 57. Disposizioni di attuazione	—

TITOLO III - DIFESA E SICUREZZA DELLO STATO
CAPO I - PROFILI GENERALI — art. 3, dir. n. 95/46/CE

Art. 58. Disposizioni applicabili	
comma 1	art. 4, commi 1, lett. b) e 2, l. n. 675/1996
comma 2	art. 4, commi 1, lett. e) e 2, l. n. 675/1996
comma 3	art. 15, comma 4, l. n. 675/1996
comma 4	—

TITOLO IV - TRATTAMENTI IN AMBITO PUBBLICO
CAPO I - ACCESSO A DOCUMENTI AMMINISTRATIVI

Art. 59. Accesso a documenti amministrativi	art. 43, comma 2, l. n. 675/1996 art. 16, comma 1, lett. c), d.lg. n. 135/1999
Art. 60. Dati idonei a rivelare lo stato di salute e la vita sessuale	art. 16, comma 2, d.lg. n. 135/1999

CAPO II - REGISTRI PUBBLICI E ALBI PROFESSIONALI

Art. 61. Utilizzazione di dati pubblici	
comma 1	art. 20, comma 1, lett. f), d.lg. n. 467/2001
comma 2	—
comma 3	—
comma 4	—

CAPO III - STATO CIVILE, ANAGRAFI E LISTE ELETTORALI

Art. 62. Dati sensibili e giudiziari	art. 6, d.lg. n. 135/1999
Art. 63. Consultazione di atti	—

CAPO IV - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 64. Cittadinanza, immigrazione e condizione dello straniero	
comma 1	art. 7, comma 1, d.lg. n. 135/1999
comma 2	art. 7, comma 3, d.lg. n. 135/1999
comma 3	art. 7, comma 2, d.lg. n. 135/1999
Art. 65. Diritti politici e pubblicità dell'attività di organi	
comma 1	art. 8, commi 1 e 2, d.lg. n. 135/1999
comma 2	art. 8, comma 3, d.lg. n. 135/1999

comma 3	art. 8, comma 4, d.lg. n. 135/1999
comma 4	art. 8, comma 5, d.lg. n. 135/1999
comma 5	art. 8, comma 6, d.lg. n. 135/1999

Art. 66. Materia tributaria e doganale

comma 1	art. 10, comma 1, d.lg. n. 135/1999
comma 2	art. 10, comma 2, d.lg. n. 135/1999

Art. 67. Attività di controllo e ispettive

comma 1, lett. a)	art. 11, comma 1, d.lg. n. 135/1999
lett. b)	art. 11, comma 3, d.lg. n. 135/1999

Art. 68. Benefici economici ed abilitazioni

comma 1	art. 13, comma 1, d.lg. n. 135/1999
comma 2	art. 13, comma 2, d.lg. n. 135/1999
comma 3	art. 13, comma 3, d.lg. n. 135/1999

Art. 69. Onorificenze, ricompense e riconoscimenti art. 14, d.lg. n. 135/1999

Art. 70. Volontariato e obiezione di coscienza

comma 1	art. 15, comma 1, d.lg. n. 135/1999
comma 2	art. 15, comma 2, d.lg. n. 135/1999

Art. 71. Attività sanzionatorie e di tutela

comma 1	art. 16, comma 1, lett. a) e b), d.lg. n. 135/1999
comma 2	art. 16, comma 2, d.lg. n. 135/1999

Art. 72. Rapporti con enti di culto art. 21, d.lg. n. 135/1999

Art. 73. Altre finalità in ambito amministrativo e sociale Provv. Garante n. 1/P/2000 del 30 dicembre 1999 - 13 gennaio 2000

CAPO V - PARTICOLARI CONTRASSEGNI

Art. 74. Contrassegni su veicoli e accessi a centri storici —

TITOLO V - TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

CAPO I - PRINCIPI GENERALI cfr. art. 8, dir. n. 95/46/CE

Art. 75. Ambito applicativo art. 1, d.lg. n. 282/1999

Art. 76. Esercenti professioni sanitarie e organismi sanitari pubblici

comma 1	art. 23, comma 1, l. n. 675/1996
comma 2	—
comma 3	art. 23, comma 3, (primo periodo), l. n. 675/1996

CAPO II - MODALITÀ SEMPLIFICATE PER INFORMATIVA E CONSENSO

Art. 77. Casi di semplificazione —

Art. 78. Informativa del medico di medicina generale o del pediatra —

Art. 79. Informativa da parte di organismi sanitari —

Art. 80. Informativa da parte di altri soggetti pubblici —

Art. 81. Prestazione del consenso	—
Art. 82. Emergenze e tutela della salute e dell'incolumità fisica	
comma 1	—
comma 2	art. 23, comma 1-quater, l. n. 675/1996
comma 3	—
comma 4	—
Art. 83. Altre misure per il rispetto dei diritti degli interessati	—
Art. 84. Comunicazione di dati all'interessato	
comma 1	art. 23, comma 2, l. n. 675/1996
comma 2	—

CAPO III - FINALITÀ DI RILEVANTE INTERESSE PUBBLICO

Art. 85. Compiti del Servizio sanitario nazionale	
comma 1	art. 17, comma 1, d.lg. n. 135/1999
comma 2	—
comma 3	—
comma 4	art. 17, comma 2, d.lg. n. 135/1999
Art. 86. Altre finalità di rilevante interesse pubblico	
comma 1	
lett. a)	art. 18, d.lg. n. 135/1999
lett. b)	art. 19, d.lg. n. 135/1999
lett. c)	art. 20, d.lg. n. 135/1999

CAPO IV - PRESCRIZIONI MEDICHE

Art. 87. Medicinali a carico del Servizio sanitario nazionale	art. 4, comma 2, d.lg. n. 282/1999
Art. 88. Medicinali non a carico del Servizio sanitario nazionale	art. 4, comma 1, d.lg. n. 282/1999
Art. 89. Casi particolari	
comma 1	—
comma 2	art. 4, comma 4, d.lg. n. 282/1999

CAPO V - DATI GENETICI

Art. 90. Trattamento dei dati genetici e donatori di midollo osseo	
comma 1	art. 17, comma 5, d.lg. n. 135/1999
comma 2	—
comma 3	art. 4, comma 3, legge 6 marzo 2001, n. 52

CAPO VI - DISPOSIZIONI VARIE

Art. 91. Dati trattati mediante carte	—
Art. 92. Cartelle cliniche	—
Art. 93. Certificato di assistenza al parto	
comma 1	art. 16, comma 2, d.P.R. 28 dicembre 2000, n. 445
comma 2	—
comma 3	—

Art. 94. Banche di dati, registri e schedari in ambito sanitari —

TITOLO VI - ISTRUZIONE
CAPO I - PROFILI GENERALI

Art. 95. Dati sensibili e giudiziari art. 12, d.lg. n. 135/1999

Art. 96. Trattamento di dati relativi a studenti
comma 1 art. 330-bis, (primo e secondo periodo), d.lg. 16 aprile 1994, n. 297
comma 2 art. 330-bis, (terzo periodo), d.lg. n. 297/1994

TITOLO VII - TRATTAMENTO PER SCOPI STORICI, STATISTICI O SCIENTIFICI
CAPO I - PROFILI GENERALI Cfr. artt. 6, 11, par. 2, 13, par. 2, dir. n. 95/46/CE

Art. 97. Ambito applicativo —

Art. 98. Finalità di rilevante interesse pubblico artt. 22 e 23, d.lg. n. 135/1999

Art. 99. Compatibilità tra scopi e durata del trattamento
comma 1 art. 9, comma 1 bis, l. 675/1996
comma 2 art. 9, comma 1 bis, l. 675/1996
comma 3 art. 16, comma 2, lett. c-bis), l. 675/1996

Art. 100. Dati relativi ad attività di studio e di ricerca art. 6, comma 4, d.lg. n. 204/1998

CAPO II - TRATTAMENTO PER SCOPI STORICI

Art. 101. Modalità di trattamento
comma 1 art. 7, comma 1, d.lg. n. 281/1999
comma 2 art. 7, comma 2, d.lg. n. 281/1999
comma 3 art. 7, comma 3, d.lg. n. 281/1999

Art. 102. Codice di deontologia e di buona condotta
comma 1 art. 6, comma 1, d.lg. n. 281/1999
comma 2 art. 7, comma 5, d.lg. n. 281/1999

Art. 103. Consultazione di documenti conservati in archivi —

CAPO III - TRATTAMENTO PER SCOPI STATISTICI O SCIENTIFICI

Art. 104. Ambito applicativo e dati identificativi per scopi statistici o scientifici
comma 1 art. 10, comma 1, d.lg. n. 281/1999
comma 2 art. 10, comma 5, d.lg. n. 281/1999

Art. 105. Modalità di trattamento
comma 1 art. 10, comma 3, d.lg. n. 281/1999
comma 2 art. 10, comma 2, d.lg. n. 281/1999
comma 3 —
comma 4 —

Art. 106. Codici di deontologia e di buona condotta
comma 1 art. 6, comma 1, d.lg. n. 281/1999
comma 2 art. 10, comma 6, d.lg. n. 281/1999

Art. 107. Trattamento di dati sensibili
comma 1 art. 10, comma 4, d.lg. n. 281/1999

Art. 108. Sistema statistico nazionale —

Art. 109. Dati statistici relativi all'evento della nascita —

Art. 110. Ricerca medica, biomedica ed epidemiologica

comma 1 art. 5, comma 1, d.lg. n. 282/1999

comma 2 art. 5, comma 2, d.lg. n. 282/1999

TITOLO VIII - LAVORO E PREVIDENZA SOCIALE

CAPO I - PROFILI GENERALI

Art. 111. Codice di deontologia e di buona condotta

comma 1 art. 20, comma 2, lett. b), d.lg., n. 467/2001

Art. 112. Finalità di rilevante interesse pubblico

comma 1 art. 9, comma 1, d.lg. n. 135/1999

comma 2 art. 9, comma 2, d.lg. n. 135/1999

comma 3 art. 9, comma 4, d.lg. n. 135/1999

CAPO II - ANNUNCI DI LAVORO E DATI RIGUARDANTI PRESTATORI DI LAVORO

Art. 113. Raccolta di dati e pertinenza cfr. art. 8, legge 20 maggio 1970, n. 300

CAPO III - DIVIETO DI CONTROLLO A DISTANZA E TELELAVORO

Art. 114. Controllo a distanza cfr. art. 4, comma 1, l. n. 300/1970

Art. 115. Telelavoro e lavoro a domicilio

comma 1 e 2 art. 6, legge 2 aprile 1958, n. 339

CAPO IV - ISTITUTI DI PATRONATO E DI ASSISTENZA SOCIALE

Art. 116. Conoscibilità di dati su mandato dell'interessato

commi 1 e 2 art. 12, legge 30 marzo 2001, n. 152

TITOLO IX - SISTEMA BANCARIO, FINANZIARIO ED ASSICURATIVO

CAPO I - SISTEMI INFORMATIVI

Art. 117. Affidabilità e puntualità nei pagamenti)

comma 1 art. 20, comma 1, lett. e), d.lg. n. 467/2001

Art. 118. Informazioni commerciali

comma 1 art. 20, comma 1, lett. d), d.lg. n. 467/2001

Art. 119. Dati relativi al comportamento debitorio —

Art. 120. Sinistri art. 2, comma 5 quater 1, d.l. 28 marzo 2000, n. 70, conv. da l. 26 maggio 2000, n. 137

TITOLO X - COMUNICAZIONI ELETTRONICHE

CAPO I - SERVIZI DI COMUNICAZIONE ELETTRONICA

Art. 121. Servizi interessati cfr. art. 3, dir. n. 2002/58/CE

Art. 122. Informazioni raccolte nei riguardi dell'abbonato e dell'utente cfr. art. 5, par. 3, dir. n. 2002/58/CE

Art. 123. Dati relativi al traffico

comma 1	cfr. art. 6, dir. n. 2002/58/CE
	art. 4, comma 1, d.lg. n. 171/1998
comma 2	art. 4, comma 2, d.lg. n. 171/1998
comma 3	art. 4, comma 3, d.lg. n. 171/1998
comma 4	—
comma 5	art. 4, comma 4, d.lg. n. 171/1998
comma 6	art. 4, comma 5, d.lg. n. 171/1998

Art. 124. Fatturazione dettagliata

comma 1	cfr. art. 7, dir. n. 2002/58/CE
	art. 5, comma 3, primo periodo, d.lg. n. 171/1998
comma 2	art. 5, comma 1, d.lg. n. 171/1998
comma 3	art. 5, comma 2, d.lg. n. 171/1998
comma 4	art. 5, comma 3, secondo periodo, d.lg. n. 171/1998
comma 5	—

Art. 125. Identificazione della linea

comma 1	cfr. art. 8, dir. n. 2002/58/CE
	art. 6, comma 1, d.lg. n. 171/1998
comma 2	art. 6, comma 2, d.lg. n. 171/1998
comma 3	art. 6, comma 3, d.lg. n. 171/1998
comma 4	art. 6, comma 4, d.lg. n. 171/1998
comma 5	art. 6, comma 5, d.lg. n. 171/1998
comma 6	art. 6, comma 6, d.lg. n. 171/1998

Art. 126. Dati relativi all'ubicazione cfr. art. 9, dir. n. 2002/58/CE

Art. 127. Chiamate di disturbo e di emergenza

comma 1	cfr. art. 10, dir. n. 2002/58/CE
	art. 7, comma 1, d.lg. n. 171/1998
comma 2	art. 7, comma 2, d.lg. n. 171/1998
comma 3	—
comma 4	art. 7, comma 2 bis, d.lg. n. 171/1998

Art. 128. Trasferimento automatico della chiamata

comma 1	cfr. art. 11, dir. n. 2002/58/CE
	art. 8, comma 1, d.lg. n. 171/1998

Art. 129. Elenchi di abbonati cfr. art. 12, dir. n. 2002/58/CE
art. 9, d.lg. n. 171/1998

Art. 130. Comunicazioni indesiderate cfr. art. 13, dir. n. 2002/58/CE
art. 10, d.lg. n. 171/1998

Art. 131. Informazioni ad abbonati e utenti art. 3, d.lg. n. 171/1998

Art. 132. Conservazione di dati di traffico per altre finalità cfr. art. 15, dir. n. 2002/58/CE

CAPO II - INTERNET E RETI TELEMATICHE

Art. 133. Codice di deontologia e di buona condotta art. 20, comma 2, lett. a), d.lg. n. 467/2001

CAPO III - VIDEOSORVEGLIANZA

Art. 134. Codice di deontologia e di buona condotta art. 20, comma 2, lett. g), d.lg. n. 467/2001

TITOLO XI - LIBERE PROFESSIONI E INVESTIGAZIONE PRIVATA
CAPO I - PROFILI GENERALI

Art. 135. Codice di deontologia e di buona condotta art. 22, comma 4, lett. c), secondo periodo, l. n. 675/1996

TITOLO XII - GIORNALISMO ED ESPRESSIONE LETTERARIA ED ARTISTICA
CAPO I - PROFILI GENERALI cfr. art. 9, dir. n. 95/46/CE

Art. 136. Finalità giornalistiche ed altre manifestazioni del pensiero

comma 1, lett. a)	art. 25, comma 1, l. n. 675/1996
lett. b) e c)	art. 25, comma 4 bis, l. n. 675/1996

Art. 137. Disposizioni applicabili

comma 1, lett. a)	art. 25, comma 1, l. n. 675/1996
lett. b)	art. 25, comma 1, l. n. 675/1996
lett. c)	art. 28, comma 6, l. n. 675/1996
comma 2	art. 12, comma 1, lett. e), l. n. 675/1996; art. 25, comma 1, l. n. 675/1996
comma 3	art. 20, comma 1, lett. d), e art. 25, comma 1, l. n. 675/1996

Art. 138. Segreto professionale art. 13, comma 5, l. n. 675/1996

CAPO II - CODICE DI DEONTOLOGIA

Art. 139. Codice di deontologia relativo ad attività giornalistiche art. 25, commi 2 , 3 e 4, l. n. 675/1996

TITOLO XIII - MARKETING DIRETTO
CAPO I - PROFILI GENERALI

Art. 140. Codice di deontologia e di buona condotta art. 20, comma 2, lett. c), d.lg. n. 467/2001

PARTE III - TUTELA DELL'INTERESSATO E SANZIONI

TITOLO I - TUTELA AMMINISTRATIVA E GIURISDIZIONALE
CAPO I - TUTELA DINANZI AL GARANTE
Sezione I - Principi generali cfr. art. 22, dir. n. 95/46/CE

Art. 141. Forme di tutela —

Sezione II - Tutela amministrativa

Art. 142. Proposizione dei reclami —

Art. 143. Procedimento per i reclami art. 21, comma 3, l. n. 675/1996
art. 31, comma 1, lett. c) e l), l. n. 675/1996

Art. 144. Segnalazioni —

Sezione III - Tutela alternativa a quella giurisdizionale

Art. 145. Ricorsi

comma 1	art. 29, comma 1, primo periodo, l. n. 675/1996
comma 2	art. 29, comma 1, secondo periodo, l. n. 675/1996

comma 3	art. 29, comma 2, secondo periodo, l. n. 675/1996

Art. 146. Interpello preventivo

comma 1	art. 29, comma 2, primo periodo, l. n. 675/1996
comma 2	art. 29, comma 2, primo periodo, l. n. 675/1996
comma 3	—

Art. 147. Presentazione del ricorso

comma 1, lett. a)	art. 18, comma 1, lett. a), d.P.R. n. 501/1998
lett. b)	art. 18, comma 1, lett. c), -seconda parte- d.P.R. n. 501/1998
lett. c)	art. 18, comma 1, lett. d), d.P.R. n. 501/1998
lett. d)	art. 18, comma 1, lett. c), -prima parte- d.P.R. n. 501/1998
lett. e)	art. 18, comma 1, lett. b), d.P.R. n. 501/1998
alinea del comma 2	art. 18, comma 1, lett. e), d.P.R. n. 501/1998
lett. a), b) e c)	art. 18, comma 3, d.P.R. n. 501/1998
comma 3	art. 18, comma 4, d.P.R. n. 501/1998
comma 4	art. 18, comma 2, d.P.R. n. 501/1998
comma 5	art. 18, alinea del comma 1, d.P.R. n. 501/1998

Art. 148. Inammissibilità del ricorso

comma 1	art. 19, comma 1, d.P.R. n. 501/1998
comma 2	art. 18, comma 5, d.P.R. n. 501/1998

Art. 149. Procedimento relativo al ricorso

comma 1	art. 20, comma 1, d.P.R. n. 501/1998
comma 2	art. 20, comma 2, d.P.R. n. 501/1998
comma 3	art. 29, comma 3, l. n. 675/1996; art. 20, comma 3, d.P.R. n. 501/1998
comma 4	—
comma 5	art. 20, comma 4, d.P.R. n. 501/1998
comma 6	art. 20, comma 5, d.P.R. n. 501/1998
comma 7	art. 20, comma 8, d.P.R. n. 501/1998
comma 8	art. 29, comma 6 bis, l. n. 675/1996

Art. 150. Provvedimenti a seguito del ricorso

comma 1	art. 29, comma 5, l. n. 675/1996
comma 2	art. 29, comma 4, l. n. 675/1996
comma 3	—
comma 4	art. 20, comma 6, d.P.R. n. 501/1998
comma 5	art. 20, comma 11, d.P.R. n. 501/1998
comma 6	—

Art. 151. Opposizione

comma 1	art. 29, comma 6, l. n. 675/1996
comma 2	—

CAPO II - TUTELA GIURISDIZIONALE

Art. 152. Autorità giudiziaria ordinaria

comma 1	art. 29, comma 8, l. n. 675/1996
comma 2	—
comma 3	—
comma 4	—
comma 5	—
comma 6	—
comma 7	—
comma 8	—
comma 9	—
comma 10	—
comma 11	—

comma 12	art. 29, comma 7, primo periodo, l. n. 675/1996
comma 13	art. 29, comma 7, secondo periodo, l. n. 675/1996
Comma 14	—

TITOLO II - L'AUTORITÀ

CAPO I - IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI — cfr. art. 28, dir. n. 95/45/CE

Art. 153. Il Garante

comma 1	art. 30, comma 2, l. n. 675/1996
comma 2	art. 30, comma 3, primo e terzo periodo, l. n. 675/1996
comma 3	art. 30, comma 3, secondo periodo, l. n. 675/1996
comma 4	art. 30, comma 4, l. n. 675/1996
comma 5	art. 30, comma 5, l. n. 675/1996
comma 6	art. 30, comma 6, l. n. 675/1996
comma 7	art. 33, prima frase, l. n. 675/1996

Art. 154. Compiti

alinea del comma 1	art. 31, alinea, l. n. 675/1996
lett. a)	art. 31, comma 1, lett. b), l. n. 675/1996
lett. b)	art. 31, comma 1, lett. d), l. n. 675/1996
lett. c)	art. 31, comma 1, lett. c), l. n. 675/1996
lett. d)	art. 31, comma 1, lett. e) ed l), l. n. 675/1996
lett. e)	art. 31, comma 1, lett. h), l. n. 675/1996
lett. f)	art. 31, comma 1, lett. m), l. n. 675/1996
lett. g)	—
lett. h)	art. 31, comma 1, lett. i), l. n. 675/1996
lett. i)	art. 31, comma 1, lett. g), l. n. 675/1996
lett. l)	art. 31, comma 1, lett. a), l. n. 675/1996
lett. m)	art. 31, comma 1, lett. n), l. n. 675/1996
comma 2	art. 31, comma 1, lett. o), l. n. 675/1996
comma 3	art. 31, commi 5 e 6, l. n. 675/1996
comma 4	art. 31, comma 2, l. n. 675/1996
comma 5	—
comma 6	art. 40, l. n. 675/1996

CAPO II - L'UFFICIO DEL GARANTE

Art. 155. Principi applicabili

comma 1	art. 33, comma 1 sexies, l. n. 675/1996

Art. 156. Ruolo organico e personale

comma 1	art. 33, comma 1, ultimo periodo, l. n. 675/1996
comma 2	—
comma 3	art. 33, commi 1 bis e 1 quater, l. n. 675/1996
comma 4	art. 33, comma 1 ter, l. n. 675/1996
comma 5	art. 33, comma 1 quinquies, l. n. 675/1996
comma 6	—
comma 7	art. 33, comma 4, l. n. 675/1996
comma 8	art. 33, comma 6, l. n. 675/1996
comma 9	art. 33, comma 6 bis, l. n. 675/1996
comma 10	art. 33, comma 2, l. n. 675/1996

CAPO III - ACCERTAMENTI E CONTROLLI

Art. 157. Richiesta di informazioni e di esibizione di documenti

comma 1	art. 32, comma 1, l. n. 675/1996

Art. 158. Accertamenti

comma 1	art. 32, comma 2, l. n. 675/1996
comma 2	art. 32, comma 2, l. n. 675/1996
comma 3	art. 32, comma 3, l. n. 675/1996; art. 15, comma 1, d.P.R. n. 501/1998

Art. 159. Modalità

comma 1	art. 15, commi 6, e 7, secondo periodo, d.P.R. n. 501/1998
comma 2	art. 32, comma 4, l. n. 675/1996; art. 15, comma 5, d.P.R. n. 501/1998
comma 3	art. 15, commi 2, e 7, primo periodo, d.P.R. n. 501/1998
comma 4	art. 15, comma 4, d.P.R. n. 501/1998
comma 5	art. 15, comma 8, d.P.R. n. 501/1998
comma 6	art. 32, comma 5, l. n. 675/1996

Art. 160. Particolari accertamenti

comma 1	art. 32, comma 6, primo periodo, l. n. 675/1996
comma 2	art. 32, comma 6, secondo periodo, l. n. 675/1996
comma 3	art. 32, comma 7, primo e secondo periodo, l. n. 675/1996
comma 4	art. 32, comma 7, terzo periodo, l. n. 675/1996
comma 5	—
comma 6	—

TITOLO III - SANZIONI

CAPO I - VIOLAZIONI AMMINISTRATIVE cfr. art. 24, dir. n. 95/46/CE

Art. 161. Omessa o inidonea informativa all'interessato

comma 1	art. 39, comma 2, primo periodo, l. n. 675/1996

Art. 162. Altre fattispecie

comma 1	art. 16, comma 3, l. n. 675/1996
comma 2	art. 39, comma 2, secondo periodo, l. n. 675/1996

Art. 163. Omessa o incompleta notificazione

comma 1	art. 34, comma 1, l. n. 675/1996

Art. 164. Omessa informazione o esibizione al Garante

comma 1	art. 39, comma 1, l. n. 675/1996

Art. 165. Pubblicazione del provvedimento del Garante

comma 1	—

Art. 166. Procedimento di applicazione

comma 1	art. 39, comma 3, l. n. 675/1996

CAPO II - ILLECITI PENALI

Art. 167. Trattamento illecito di dati

comma 1	art. 35, comma 1, l. n. 675/1996; art. 11, d.lg. 171/1998
comma 2	art. 35, comma 2, l. n. 675/1996

Art. 168. Falsità nelle dichiarazioni e notificazioni al Garante

comma 1	art. 37 bis, comma 1, l. n. 675/1996

Art. 169. Misure di sicurezza

comma 1	art. 36, comma 1, l. n. 675/1996
comma 2	art. 36, comma 2, l. n. 675/1996

Art. 170. Inosservanza di provvedimenti del Garante

comma 1	art. 37, comma 1, l. n. 675/1996

Art. 171. Altre fattispecie	—
Art. 172. Pene accessorie	
comma 1	art. 38, comma 1, l. n. 675/1996

TITOLO IV - DISPOSIZIONI MODIFICATIVE, ABROGATIVE, TRANSITORIE E FINALI

CAPO I - DISPOSIZIONI DI MODIFICA

Art. 173. Convenzione di applicazione dell'Accordo di Schengen	—
Art. 174. Notifiche di atti e vendite giudiziarie	—
Art. 175. Forze di Polizia	—
Art. 176. Soggetti pubblici	—
Art. 177. Disciplina anagrafica, dello stato civile e delle liste elettorali	—
Art. 178. Disposizioni in materia sanitaria	
comma 1	—
comma 2	—
comma 3	art. 4, comma 5, d.lg. n. 282/1999
comma 4	—
comma 5	—
Art. 179. Altre modifiche	—

CAPO II - DISPOSIZIONI TRANSITORIE

Art. 180. Misure di sicurezza	—
Art. 181. Altre disposizioni transitorie	
comma 1	—
comma 2	—
comma 3	—
comma 4	art. 13, comma 5, d.P.R. n. 501/1998
comma 5	—
comma 6	—
Art. 182. Ufficio del Garante	—

CAPO III - ABROGAZIONI

Art. 183. Norme abrogate	—

CAPO IV. NORME FINALI

Art. 184. Attuazione di direttive europee	
comma 1	—
comma 2	—
comma 3	art. 43, comma 2, secondo periodo, l. n. 675/1996
Art. 185. Allegazione dei codici di deontologia e di buona condotta	—
Art. 186. Entrata in vigore	—

ALLEGATI

Codici di deontologia

A1

Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Visto l'art. 25 della legge 31 dicembre 1996, n. 675, come modificato dall'art. 12 del decreto legislativo 13 maggio 1998, n 171, secondo il quale il trattamento dei dati personali nell'esercizio della professione giornalistica deve essere effettuato sulla base di un apposito codice di deontologia, recante misure ed accorgimenti a garanzia degli interessati rapportati alla natura dei dati, in particolare per quanto riguarda i dati idonei a rivelare lo stato di salute e la vita sessuale;

Visto il comma 4-bis dello stesso art. 25, secondo il quale tale codice è applicabile anche all'attività dei pubblicisti e dei praticanti giornalisti, nonché a chiunque tratti temporaneamente i dati personali al fine di utilizzarli per la pubblicazione occasionale di articoli, di saggi e di altre manifestazioni di pensiero;

Visto il comma 2 del medesimo art. 25, secondo il quale il codice di deontologia è adottato dal Consiglio nazionale dell'ordine dei giornalisti in cooperazione con il Garante, il quale ne promuove l'adozione e ne cura la pubblicazione nella *Gazzetta Ufficiale*;

Vista la nota prot. n. 89/GAR del 26 maggio 1997, con la quale il Garante ha invitato il Consiglio nazionale dell'ordine ad adottare il codice entro il previsto termine di sei mesi dalla data di invio della nota stessa;

Vista la nota prot. n. 4640 del 24 novembre 1997, con il quale il Garante ha aderito alla richiesta di breve differimento del predetto termine di sei mesi, presentata il 19 novembre dal presidente del Consiglio nazionale dell'ordine;

Visto il provvedimento prot. n. 5252 del 18 dicembre 1997, con il quale il Garante ha segnalato al Consiglio nazionale dell'ordine alcuni criteri da tenere presenti nel bilanciamento delle libertà e dei diritti coinvolti dall'attività giornalistica;

Vista la nota prot. n. 314 del 23 gennaio 1998, con la quale il Garante ha formulato altre osservazioni sul primo schema di codice elaborato dal Consiglio nazionale dell'ordine e trasmesso al Garante con nota prot. n. 7182 del 30 dicembre 1997;

Vista la nota prot. n. 204 del 15 gennaio 1998, con la quale il Garante, sulla base della prima esperienza di applicazione della legge n. 675/1996 e dello schema di codice elaborato, ha rappresentato al Ministro di grazia e giustizia l'opportunità di una revisione dell'art. 25 della legge, che è stato poi modificato con il citato decreto legislativo n. 171 del 13 maggio 1998;

Vista la nota prot. n. 5876 del 30 giugno 1998, con la quale il Garante ha invitato il Consiglio nazionale dell'ordine ad apportare alcune residuali modifiche all'ulteriore schema approvato dallo stesso Consiglio nella seduta del 26 e 27 marzo 1998 e trasmesso al Garante con nota prot. n. 1074 dell'8 aprile;

(*) Provvedimento del Garante del 29 luglio 1998, in *Gazzetta Ufficiale* 3 agosto 1998, n. 179

Constatata l'idoneità delle misure e degli accorgimenti a garanzia degli interessati previsti dallo schema definitivo del codice di deontologia trasmesso al Garante dal Consiglio nazionale dell'ordine con nota prot. n. 2210 del 15 luglio 1998;

Considerato che, ai sensi dell'art. 25, comma 2, della legge n. 675/1996, il codice deve essere pubblicato nella *Gazzetta Ufficiale*, a cura del Garante, e diviene efficace quindici giorni dopo la sua pubblicazione;

Dispone

La trasmissione del codice di deontologia che figura in allegato all'ufficio pubblicazione leggi e decreti del Ministero di grazia e giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 29 luglio 1998

IL PRESIDENTE

ORDINE DEI GIORNALISTI - CODICE DI DEONTOLOGIA RELATIVO AL TRATTAMENTO DEI DATI PERSONALI NELL'ESERCIZIO DELL'ATTIVITÀ GIORNALISTICA (*)

Art. 1. Principi generali

1. Le presenti norme sono volte a contemperare i diritti fondamentali della persona con il diritto dei cittadini all'informazione e con la libertà di stampa.

2. In forza dell'art. 21 della Costituzione, la professione giornalistica si svolge senza autorizzazioni o censure. In quanto condizione essenziale per l'esercizio del diritto dovere di cronaca, la raccolta, la registrazione, la conservazione e la diffusione di notizie su eventi e vicende relativi a persone, organismi collettivi, istituzioni, costumi, ricerche scientifiche e movimenti di pensiero, attuate nell'ambito dell'attività giornalistica e per gli scopi propri di tale attività, si differenziano nettamente per la loro natura dalla memorizzazione e dal trattamento di dati personali ad opera di banche dati o altri soggetti. Su questi principi trovano fondamento le necessarie deroghe previste dai paragrafi 17 e 37 e dall'art. 9 della direttiva 95/46/CE del Parlamento europeo e del Consiglio dell'Unione europea del 24 ottobre 1995 e dalla legge n. 675/1996.

Art. 2. Banche dati di uso redazionale e tutela degli archivi personali dei giornalisti

1. Il giornalista che raccoglie notizie per una delle operazioni di cui all'art. 1, comma 2, lettera b), della legge n. 675/1996 rende note la propria identità, la propria professione e le finalità della raccolta, salvo che ciò comporti rischi per la sua incolumità o renda altrimenti impossibile l'esercizio della funzione informativa; evita artifici e pressioni indebite. Fatta palese tale attività, il giornalista non è tenuto a fornire gli altri elementi dell'informativa di cui all'art. 10, comma 1, della legge n. 675/1996.

2. Se i dati personali sono raccolti presso banche dati di uso redazionale, le imprese editoriali sono tenute a rendere noti al pubblico, mediante annunci, almeno due volte l'anno, l'esistenza dell'archivio e il luogo dove è possibile esercitare i diritti previsti dalla legge n. 675/1996. Le imprese editoriali indicano altresì fra i dati della gerenza il responsabile del trattamento al quale le persone interessate possono rivolgersi per esercitare i diritti previsti dalla legge n. 675/1996.

3. Gli archivi personali dei giornalisti, comunque funzionali all'esercizio della professione e per l'esclusivo perseguimento delle relative finalità, sono tutelati, per quanto concerne le fonti delle notizie, ai sensi dell'art. 2 della legge n. 69/1963 e dell'art. 13, comma 5, della legge n. 675/1996.

4. Il giornalista può conservare i dati raccolti per tutto il tempo necessario al perseguimento delle finalità proprie della sua professione.

Art. 3. Tutela del domicilio

1. La tutela del domicilio e degli altri luoghi di privata dimora si estende ai luoghi di cura, detenzione o riabilitazione, nel rispetto delle norme di legge e dell'uso corretto di tecniche invasive.

Art. 4. Rettifica

1. Il giornalista corregge senza ritardo errori e inesattezze, anche in conformità al dovere di rettifica nei casi e nei modi stabiliti dalla legge.

Art. 5. Diritto all'informazione e dati personali

1. Nel raccogliere dati personali atti a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesioni a partiti, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, nonchè dati atti

(*) In conformità all'articolo 184, comma 2, d.lg. 30 giugno 2003, n. 196, i riferimenti a disposizioni della legge n. 675/1996 o ad altre disposizioni abrogate, devono intendersi riferiti alle corrispondenti nuove disposizioni in vigore, secondo la tavola di corrispondenza

a rivelare le condizioni di salute e la sfera sessuale, il giornalista garantisce il diritto all'informazione su fatti di interesse pubblico, nel rispetto dell'essenzialità dell'informazione, evitando riferimenti a congiunti o ad altri soggetti non interessati ai fatti.

2. In relazione a dati riguardanti circostanze o fatti resi noti direttamente dagli interessati o attraverso loro comportamenti in pubblico, è fatto salvo il diritto di addurre successivamente motivi legittimi meritevoli di tutela.

Art. 6. Essenzialità dell'informazione

1. La divulgazione di notizie di rilevante interesse pubblico o sociale non contrasta con il rispetto della sfera privata quando l'informazione, anche dettagliata, sia indispensabile in ragione dell'originalità del fatto o della relativa descrizione dei modi particolari in cui è avvenuto, nonché della qualificazione dei protagonisti.

2. La sfera privata delle persone note o che esercitano funzioni pubbliche deve essere rispettata se le notizie o i dati non hanno alcun rilievo sul loro ruolo o sulla loro vita pubblica.

3. Commenti e opinioni del giornalista appartengono alla libertà di informazione nonché alla libertà di parola e di pensiero costituzionalmente garantita a tutti.

Art. 7. Tutela del minore

1. Al fine di tutelarne la personalità, il giornalista non pubblica i nomi dei minori coinvolti in fatti di cronaca, né fornisce particolari in grado di condurre alla loro identificazione.

2. La tutela della personalità del minore si estende, tenuto conto della qualità della notizia e delle sue componenti, ai fatti che non siano specificamente reati.

3. Il diritto del minore alla riservatezza deve essere sempre considerato come primario rispetto al diritto di critica e di cronaca; qualora, tuttavia, per motivi di rilevante interesse pubblico e fermo restando i limiti di legge, il giornalista decida di diffondere notizie o immagini riguardanti minori, dovrà farsi carico della responsabilità di valutare se la pubblicazione sia davvero nell'interesse oggettivo del minore, secondo i principi e i limiti stabiliti dalla "Carta di Treviso".

Art. 8. Tutela della dignità delle persone

1. Salva l'essenzialità dell'informazione, il giornalista non fornisce notizie o pubblica immagini o fotografie di soggetti coinvolti in fatti di cronaca lesive della dignità della persona, né si sofferma su dettagli di violenza, a meno che ravvisi la rilevanza sociale della notizia o dell'immagine.

2. Salvo rilevanti motivi di interesse pubblico o comprovati fini di giustizia e di polizia, il giornalista non riprende né produce immagini e foto di persone in stato di detenzione senza il consenso dell'interessato.

3. Le persone non possono essere presentate con ferri o manette ai polsi, salvo che ciò sia necessario per segnalare abusi.

Art. 9. Tutela del diritto alla non discriminazione

1. Nell'esercitare il diritto dovere di cronaca, il giornalista è tenuto a rispettare il diritto della persona alla non discriminazione per razza, religione, opinioni politiche, sesso, condizioni personali, fisiche o mentali.

Art. 10. Tutela della dignità delle persone malate

1. Il giornalista, nel far riferimento allo stato di salute di una determinata persona, identificata o identificabile, ne rispetta la dignità, il diritto alla riservatezza e al decoro

personale, specie nei casi di malattie gravi o terminali, e si astiene dal pubblicare dati analitici di interesse strettamente clinico.

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e sempre nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica.

Art. 11. Tutela della sfera sessuale della persona

1. Il giornalista si astiene dalla descrizione di abitudini sessuali riferite ad una determinata persona, identificata o identificabile.

2. La pubblicazione è ammessa nell'ambito del perseguimento dell'essenzialità dell'informazione e nel rispetto della dignità della persona se questa riveste una posizione di particolare rilevanza sociale o pubblica.

Art. 12. Tutela del diritto di cronaca nei procedimenti penali

1. Al trattamento dei dati relativi a procedimenti penali non si applica il limite previsto dall'art. 24 della legge n. 675/1996.

2. Il trattamento di dati personali idonei a rivelare provvedimenti di cui all'art. 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale è ammesso nell'esercizio del diritto di cronaca, secondo i principi di cui all'art. 5.

Art. 13. Ambito di applicazione, sanzioni disciplinari

1. Le presenti norme si applicano ai giornalisti professionisti, pubblicisti e praticanti e a chiunque altro, anche occasionalmente, eserciti attività pubblicistica.

2. Le sanzioni disciplinari, di cui al titolo III della legge n. 69/1963, si applicano solo ai soggetti iscritti all'albo dei giornalisti, negli elenchi o nel registro.

A2

Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Ugo De Siervo e dell'ing. Claudio Manganelli, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visto l' art. 31, comma 1, lettera h) della legge 31 dicembre 1996, n. 675, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare il relativo art. 6, comma 1, il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi storici;

Visto l'articolo 7, comma 5, del medesimo decreto legislativo n. 281/1999, relativo ad alcuni profili che devono essere individuati dal codice per i trattamenti di dati per scopi storici;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla *Gazzetta Ufficiale* n. 46 del 25 febbraio 2000, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi del trattamento di dati personali per scopi storici effettuati da archivisti e utenti ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione del medesimo codice in base al principio di rappresentatività a darne comunicazione al Garante entro il 31 marzo 2000;

Viste le comunicazioni pervenute al Garante in risposta al provvedimento del 10 febbraio 2000, con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare alla redazione del codice e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro composto da componenti della Commissione consultiva per le questioni inerenti la consultabilità degli atti d'archivio riservati, del Centro di documentazione ebraica, del Ministero per i beni e le attività culturali, dell'Associazione delle istituzioni culturali italiane, dell'Associazione nazionale archivistica italiana, dell'Istituto nazionale per la storia del movimento di liberazione in Italia, della Società per lo studio della storia contemporanea, dell'Istituto storico italiano per l'età moderna e contemporanea, della Società per gli studi di storia delle istituzioni, della Società italiana delle storiche, dell'Istituto romano per la storia d'Italia dal fascismo alla resistenza;

Considerato che il testo del codice è stato oggetto di ampia diffusione, anche attraverso la sua pubblicazione su alcuni siti Internet, al fine di favorire il più ampio dibattito e di per-

(*) Provvedimento del Garante n. 8/P/21 del 14 marzo 2001, in *Gazzetta Ufficiale* del 5 aprile 2001, n. 80

mettere la raccolta di eventuali osservazioni e integrazioni al testo medesimo da parte di tutti i soggetti interessati;

Vista la nota del 28 febbraio 2001 con cui il gruppo di lavoro ha trasmesso il testo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici approvato e sottoscritto in pari data;

Rilevato che il rispetto delle disposizioni contenute nel codice costituisce condizione essenziale per la liceità del trattamento dei dati personali;

Constatata la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, ed in particolare all'art. 31, comma 1, lettera h) della legge n. 675/1996, nonché agli artt. 6 e 7 del decreto legislativo n. 281/1999;

Considerato che, ai sensi dell'art. 6, comma 1, del decreto legislativo n. 281/1999, il codice deve essere pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana a cura del Garante;

Rilevato che anche dopo tale pubblicazione il codice potrà essere eventualmente sottoscritto da altri soggetti pubblici e privati, società scientifiche ed associazioni professionali interessati;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000, adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana n. 162 del 13 luglio 2000;

Dispone:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici che figura in allegato all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 14 marzo 2001

IL PRESIDENTE
IL RELATORE
IL SEGRETARIO GENERALE

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI PER SCOPI STORICI (*)

Preambolo

I sottoindicati soggetti pubblici e privati sottoscrivono il presente codice sulla base delle seguenti premesse:

1) Chiunque accede ad informazioni e documenti per scopi storici utilizza frequentemente dati di carattere personale per i quali la legge prevede alcune garanzie a tutela degli interessati. In considerazione dell'interesse pubblico allo svolgimento di tali trattamenti, il legislatore -con specifico riguardo agli archivi pubblici e a quelli privati dichiarati di notevole interesse storico ai sensi dell'art. 36 del d.P.R. 30 settembre 1963 n. 1409- ha esentato i soggetti che utilizzano dati personali per le suddette finalità dall'obbligo di richiedere il consenso degli interessati ai sensi degli artt. 12 , 20 e 28 della legge (l. 31 dicembre 1996, n. 675, in particolare art. 27; dd.lg. 11 maggio 1999, n. 135 e 30 luglio 1999, n. 281, in particolare art. 7, comma 4; d.P.R. 30 settembre 1963, n. 1409, e successive modificazioni e integrazioni).

2) L'utilizzazione di tali dati da parte di utenti ed archivisti deve pertanto rispettare le previsioni di legge e quelle del presente codice di deontologia e di buona condotta, l'osservanza del quale, oltre a rappresentare un obbligo deontologico, costituisce condizione essenziale per la liceità del trattamento dei dati (art. 31, comma 1, lettera h), l. 31 dicembre 1996, n. 675; art.6, d. lg. 30 luglio 1999, n.281).

3) L'osservanza di tali regole non deve pregiudicare l'indagine, la ricerca, la documentazione e lo studio ovunque svolti, in relazione a figure, fatti e circostanze del passato.

4) I trattamenti di dati personali concernenti la conservazione, l'ordinamento e la comunicazione dei documenti conservati negli Archivi di Stato e negli archivi storici degli enti pubblici sono considerati di rilevante interesse pubblico (art. 23 d.lg. 11 maggio 1999, n. 135).

5) La sottoscrizione del presente codice è promossa per legge dal Garante, nel rispetto del principio di rappresentatività dei soggetti pubblici e privati interessati. Il codice è espressione delle associazioni professionali e delle categorie interessate, ivi comprese le società scientifiche, ed è volto ad assicurare l'equilibrio delle diverse esigenze connesse alla ricerca e alla rappresentazione di fatti storici con i diritti e le libertà fondamentali delle persone interessate (art. 1, l. 31 dicembre 1996, n. 675).

6) Il presente codice, sulla base delle prescrizioni di legge, individua in particolare: a) alcune regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, armonizzate con quelle che riguardano il diritto di cronaca e la manifestazione del pensiero; b) particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare; c) modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati per scopi storici (art. 7, comma 5, d.lg. 30 luglio 1999, n. 281) .

7) La sottoscrizione del presente codice è effettuata ispirandosi, oltre agli artt. 21 e 33 della Costituzione della Repubblica italiana, alle pertinenti fonti e documenti internazionali in materia di ricerca storica e di archivi e in particolare:

a) agli artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;
b) alla Raccomandazione N. R (2000) 13 del 13 luglio 2000 del Consiglio d'Europa;
c) agli artt. 1, 7, 8, 11 e 13 della Carta dei diritti fondamentali dell'Unione europea;
d) ai Principi direttivi per una legge sugli archivi storici e gli archivi correnti, individuati dal Consiglio internazionale degli archivi al congresso di Ottawa nel 1996, e

(*) In conformità all'articolo 184, comma 2, d.lg. 30 giugno 2003, n. 196, i riferimenti a disposizioni della legge n. 675/1996 o ad altre disposizioni abrogate, devono intendersi riferiti alle corrispondenti nuove disposizioni in vigore, secondo la tavola di corrispondenza

al Codice internazionale di deontologia degli archivisti approvato nel congresso internazionale degli archivi, svoltosi a Pechino nel 1996.

CAPO I - PRINCIPI GENERALI

Art. 1. Finalità e ambito di applicazione

1. Le presenti norme sono volte a garantire che l'utilizzazione di dati di carattere personale acquisiti nell'esercizio della libera ricerca storica e del diritto allo studio e all'informazione, nonché nell'accesso ad atti e documenti, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

2. Il presente codice detta disposizioni per i trattamenti di dati personali effettuati per scopi storici in relazione ai documenti conservati presso archivi delle pubbliche amministrazioni, enti pubblici ed archivi privati dichiarati di notevole interesse storico. Il codice si applica, senza necessità di sottoscrizione, all'insieme dei trattamenti di dati personali comunque effettuati dagli utenti per scopi storici.

3. Il presente codice reca, altresì, principi-guida di comportamento dei soggetti che trattano per scopi storici dati personali conservati presso archivi pubblici e archivi privati dichiarati di notevole interesse storico, e in particolare:

a) nei riguardi degli archivisti, individua regole di correttezza e di non discriminazione nei confronti degli utenti, indipendentemente dalla loro nazionalità, categoria di appartenenza, livello di istruzione;
b) nei confronti degli utenti, individua cautele per la raccolta, l'utilizzazione e la diffusione dei dati contenuti nei documenti.

4. La competente sovrintendenza archivistica riceve comunicazione da parte di proprietari, possessori e detentori di archivi privati non dichiarati di notevole interesse storico o di singoli documenti di interesse storico, i quali manifestano l'intenzione di applicare il presente codice nella misura per essi compatibile.

Art. 2. Definizioni

1. Nell'applicazione del presente codice si tiene conto delle definizioni e delle indicazioni contenute nella disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni citate nel preambolo. Ai medesimi fini si intende, altresì:

a) per "archivista", chiunque, persona fisica o giuridica, ente o associazione, abbia responsabilità di controllare, acquisire, trattare, conservare, restaurare e gestire archivi storici, correnti o di deposito della pubblica amministrazione, archivi privati dichiarati di notevole interesse storico, nonché gli archivi privati di cui al precedente art. 1, comma 4;
b) per "utente", chiunque chieda di accedere o acceda per scopi storici a documenti contenenti dati personali, anche per finalità giornalistiche o di pubblicazione occasionale di articoli, saggi e altre manifestazioni del pensiero;
c) per "documento", qualunque testimonianza scritta, orale o conservata su qualsiasi supporto che contenga dati personali.

CAPO II - REGOLE DI CONDOTTA PER GLI ARCHIVISTI E LICEITÀ DEI RELATIVI TRATTAMENTI

Art. 3. Regole generali di condotta

1. Nel trattare i dati di carattere personale e i documenti che li contengono, gli archivisti adottano, in armonia con la legge e i regolamenti, le modalità più opportune per favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone alle quali si riferiscono i dati trattati.

2. Gli archivisti di enti o istituzioni pubbliche si adoperano per il pieno rispetto, anche da parte dei terzi con cui entrano in contatto per ragioni del proprio ufficio o servizio, delle disposizioni di legge e di regolamento in materia archivistica e, in particolare, di quanto previsto negli artt. 21 e 21-bis del d.P.R. 30 settembre 1963, n. 1409, come modificati dal

d.lg. 30 luglio 1999, n. 281, dall'art. 7 del medesimo d.lg. n. 281, e successive modificazioni ed integrazioni.

3. I soggetti che operano presso enti pubblici svolgendo funzioni archivistiche, nel trattare dati di carattere personale si attengono ai doveri di lealtà, correttezza, imparzialità, onestà e diligenza propri dell'esercizio della professione e della qualifica o livello ricoperti. Essi conformano il proprio operato al principio di trasparenza della attività amministrativa.

4. I dati personali trattati per scopi storici possono essere ulteriormente utilizzati per tali scopi, e sono soggetti in linea di principio alla medesima disciplina indipendentemente dal documento in cui sono contenuti e dal luogo di conservazione, ferme restando le cautele e le garanzie previste per particolari categorie di dati o di trattamenti.

Art. 4. Conservazione e tutela

1. Gli archivisti si impegnano a:
   a) favorire il recupero, l'acquisizione e la tutela dei documenti. A tal fine, operano in conformità con i principi, i criteri metodologici e le pratiche della professione generalmente condivisi ed accettati, curando anche l'aggiornamento sistematico e continuo delle proprie conoscenze storiche, amministrative e tecnologiche;
   b) tutelare l'integrità degli archivi e l'autenticità dei documenti, anche elettronici e multimediali, di cui promuovono la conservazione permanente, in particolare di quelli esposti a rischi di cancellazione, dispersione ed alterazione dei dati;
   c) salvaguardare la conformità delle riproduzioni dei documenti agli originali ed evitare ogni azione diretta a manipolare, dissimulare o deformare fatti, testimonianze, documenti e dati;
   d) assicurare il rispetto delle misure di sicurezza previste dall'art. 15 della legge 31 dicembre 1996, n. 675 e dal d.P.R. 28 luglio 1999, n. 318 e successive integrazioni e modificazioni, sviluppando misure idonee a prevenire l'eventuale distruzione, dispersione o accesso non autorizzato ai documenti, e adottando, in presenza di specifici rischi, particolari cautele quali la consultazione in copia di alcuni documenti e la conservazione degli originali in cassaforte o armadi blindati.

Art. 5. Comunicazione e fruizione

1. Gli archivi sono organizzati secondo criteri tali da assicurare il principio della libera fruibilità delle fonti.

2. L'archivista promuove il più largo accesso agli archivi e, attenendosi al quadro della normativa vigente, favorisce l'attività di ricerca e di informazione nonché il reperimento delle fonti.

3. L'archivista informa il ricercatore sui documenti estratti temporaneamente da un fascicolo perché esclusi dalla consultazione.

4. In caso di rilevazione sistematica dei dati realizzata da un archivio in collaborazione con altri soggetti pubblici o privati, per costituire banche dati di intere serie archivistiche, la struttura interessata sottoscrive una apposita convenzione per concordare le modalità di fruizione e le forme di tutela dei soggetti interessati, attenendosi alle disposizioni della legge, in particolare per quanto riguarda il rapporto tra il titolare, il responsabile e gli incaricati del trattamento, nonché i rapporti con i soggetti esterni interessati ad accedere ai dati.

Art. 6. Impegno di riservatezza

1. Gli archivisti si impegnano a:
   a) non fare alcun uso delle informazioni non disponibili agli utenti o non rese pubbliche, ottenute in ragione della propria attività anche in via confidenziale, per proprie ricerche o per realizzare profitti e interessi privati. Nel caso in cui l'archivista svolga ricerche per fini personali o comunque estranei alla propria attività professionale, è soggetto alle stesse regole e ai medesimi limiti previsti per gli utenti;

b) mantenere riservate le notizie e le informazioni concernenti i dati personali apprese nell'esercizio delle proprie attività.

2. L'archivista osserva tali doveri di riserbo anche dopo la cessazione dalla propria attività.

Art. 7. Aggiornamento dei dati

1. L'archivista favorisce l'esercizio del diritto degli interessati all'aggiornamento, alla rettifica o all'integrazione dei dati, garantendone la conservazione secondo modalità che assicurino la distinzione delle fonti originarie dalla documentazione successivamente acquisita.

2. Ai fini dell'applicazione dell'art. 13 della legge n. 675/1996, in presenza di eventuali richieste generalizzate di accesso ad un'ampia serie di dati o documenti, l'archivista pone a disposizione gli strumenti di ricerca e le fonti pertinenti fornendo al richiedente idonee indicazioni per una loro agevole consultazione.

3. In caso di esercizio di un diritto, ai sensi dell'art. 13, comma 3, della legge n. 675/1996, da parte di chi vi abbia interesse in relazione a dati personali che riguardano persone decedute e documenti assai risalenti nel tempo, la sussistenza dell'interesse è valutata anche in riferimento al tempo trascorso.

Art. 8. Fonti orali

1. In caso di trattamento di fonti orali, è necessario che gli intervistati abbiano espresso il proprio consenso in modo esplicito, eventualmente in forma verbale, anche sulla base di una informativa semplificata che renda nota almeno l'identità e l'attività svolta dall'intervistatore nonché le finalità della raccolta dei dati.

2. Gli archivi che acquisiscono fonti orali richiedono all'autore dell'intervista una dichiarazione scritta dell'avvenuta comunicazione degli scopi perseguiti nell'intervista stessa e del relativo consenso manifestato dagli intervistati.

CAPO III - REGOLE DI CONDOTTA PER GLI UTENTI E CONDIZIONI PER LA LICEITÀ DEI RELATIVI TRATTAMENTI

Art. 9. Regole generali di condotta

1. Nell'accedere alle fonti e nell'esercitare l'attività di studio, ricerca e manifestazione del pensiero, gli utenti, quando trattino i dati di carattere personale, secondo quanto previsto dalla legge e dai regolamenti, adottano le modalità più opportune per favorire il rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate.

2. In applicazione del principio di cui al comma 1, gli utenti utilizzano i documenti sotto la propria responsabilità e conformandosi agli scopi perseguiti e delineati nel progetto di ricerca, nel rispetto dei principi di pertinenza ed indispensabilità di cui all'art. 7, del d.lg. 30 luglio 1999, n. 281.

Art. 10. Accesso agli archivi pubblici

1. L'accesso agli archivi pubblici è libero. Tutti gli utenti hanno diritto ad accedere agli archivi con eguali diritti e doveri.

2. Fanno eccezione, ai sensi delle leggi vigenti, i documenti di carattere riservato relativi alla politica interna ed estera dello Stato che divengono consultabili cinquanta anni dopo la loro data e quelli contenenti i dati di cui agli artt. 22 e 24 della legge n. 675/1996, che divengono liberamente consultabili quaranta anni dopo la loro data. Il termine è di settanta anni se i dati sono idonei a rivelare lo stato di salute o la vita sessuale oppure rapporti riservati di tipo familiare.

3. L'autorizzazione alla consultazione dei documenti di cui al comma 2 può essere rilasciata prima della scadenza dei termini dal Ministro dell'interno, previo parere del direttore dell'Archivio di Stato o del sovrintendente archivistico competenti e udita la Commissione

per le questioni inerenti alla consultabilità degli atti di archivio riservati istituita presso il Ministero dell'interno, secondo la procedura dettata dagli artt. 8 e 9 del decreto legislativo n. 281/1999.

4. In caso di richiesta di autorizzazione a consultare i documenti di cui al comma 2 prima della scadenza dei termini, l'utente presenta all'ente che li conserva un progetto di ricerca che, in relazione alle fonti riservate per le quali chiede l'autorizzazione, illustri le finalità della ricerca e le modalità di diffusione dei dati. Il richiedente ha facoltà di presentare ogni altra documentazione utile.

5. L'autorizzazione di cui al comma 3 alla consultazione è rilasciata a parità di condizioni ad ogni altro richiedente. La valutazione della parità di condizioni avviene sulla base del progetto di ricerca di cui al comma 4.

6. L'autorizzazione alla consultazione dei documenti, di cui al comma 3, prima dello scadere dei termini, può contenere cautele volte a consentire la comunicazione dei dati senza ledere i diritti, le libertà e la dignità delle persone interessate.

7. Le cautele possono consistere anche, a seconda degli obiettivi della ricerca desumibili dal progetto, nell'obbligo di non diffondere i nomi delle persone, nell'uso delle sole iniziali dei nominativi degli interessati, nell'oscuramento dei nomi in una banca dati, nella sottrazione temporanea di singoli documenti dai fascicoli o nel divieto di riproduzione dei documenti. Particolare attenzione è prestata al principio della pertinenza e all'indicazione di fatti o circostanze che possono rendere facilmente individuabili gli interessati.

8. L'autorizzazione di cui al comma 3 è personale e il titolare dell'autorizzazione non può delegare altri al conseguente trattamento dei dati. I documenti mantengono il loro carattere riservato e non possono essere ulteriormente utilizzati da altri soggetti senza la relativa autorizzazione.

Art. 11. Diffusione

1. L'interpretazione dell'utente, nel rispetto del diritto alla riservatezza, del diritto all'identità personale e della dignità degli interessati, rientra nella sfera della libertà di parola e di manifestazione del pensiero costituzionalmente garantite.

2. Nel far riferimento allo stato di salute delle persone l'utente si astiene dal pubblicare dati analitici di interesse strettamente clinico e dal descrivere abitudini sessuali riferite ad una determinata persona identificata o identificabile.

3. La sfera privata delle persone note o che abbiano esercitato funzioni pubbliche deve essere rispettata nel caso in cui le notizie o i dati non abbiano alcun rilievo sul loro ruolo o sulla loro vita pubblica.

4. In applicazione di quanto previsto dall'art. 7, comma 2, del d.lg. n. 281/1999, al momento della diffusione dei dati il principio della pertinenza è valutato dall'utente con particolare riguardo ai singoli dati personali contenuti nei documenti, anziché ai documenti nel loro complesso. L'utente può diffondere i dati personali se pertinenti e indispensabili alla ricerca e se gli stessi non ledono la dignità e la riservatezza delle persone.

5. L'utente non è tenuto a fornire l'informativa di cui all'art. 10, comma 3, della legge n. 675/1996 nei casi in cui tale adempimento comporti l'impiego di mezzi manifestamente sproporzionati.

6. L'utente può utilizzare i dati elaborati o le copie dei documenti contenenti dati personali, accessibili su autorizzazione, solo ai fini della propria ricerca, e ne cura la riservatezza anche rispetto ai terzi.

Art. 12. Applicazione del codice

1. I soggetti pubblici e privati, comprese le società scientifiche e le associazioni professionali, che siano tenuti ad applicare il presente codice si impegnano, con i modi e nelle forme previste dai propri ordinamenti, a promuoverne la massima diffusione e la conoscenza, nonché ad assicurarne il rispetto.

2. Nel caso degli archivi degli enti pubblici e degli archivi privati dichiarati di notevole interesse storico, le sovrintendenze archivistiche promuovono la diffusione e l'applicazione del codice.

Art. 13. Violazione delle regole di condotta

1. Nell'ambito degli archivi pubblici le amministrazioni competenti applicano le sanzioni previste dai rispettivi ordinamenti.

2. Le società e le associazioni tenute ad applicare il presente codice adottano, sulla base dei propri ordinamenti e regolamenti, le opportune misure in caso di violazione del codice stesso, ferme restando le sanzioni di legge.

3. La violazione delle prescrizioni del presente codice da parte degli utenti è comunicata agli organi competenti per il rilascio delle autorizzazioni a consultare documenti riservati prima del decorso dei termini di legge, ed è considerata ai fini del rilascio dell'autorizzazione medesima. L'Amministrazione competente, secondo il proprio ordinamento, può altresì escludere temporaneamente dalle sale di studio i soggetti responsabili della violazione delle regole del presente codice. Gli stessi possono essere esclusi da ulteriori autorizzazioni alla consultazione di documenti riservati.

4. Oltre a quanto previsto dalla legge per la denuncia di reato cui sono tenuti i pubblici ufficiali, i soggetti di cui ai commi 1 e 2 possono segnalare al Garante le violazioni delle regole di condotta per l'eventuale adozione dei provvedimenti e delle sanzioni di competenza.

Art. 14. Entrata in vigore

1. Il presente codice si applica a decorrere dal quindicesimo giorno successivo alla pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

A3

Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale (*)

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella seduta odierna, con la partecipazione del prof. Stefano Rodotà, presidente, del prof. Giuseppe Santaniello, vice presidente, del prof. Gaetano Rasi e del dott. Mauro Paissan, componenti, e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 27 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, secondo cui gli Stati membri e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire, in funzione delle specificità settoriali, alla corretta applicazione delle disposizioni nazionali di attuazione della direttiva adottate dagli Stati membri;

Visto l'art. 31, comma 1, lettera h) della legge 31 dicembre 1996, n. 675, il quale attribuisce al Garante il compito di promuovere nell'ambito delle categorie interessate, nell'osservanza del principio di rappresentatività, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, verificarne la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuire a garantirne la diffusione e il rispetto;

Visto il decreto legislativo 30 luglio 1999, n. 281, in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica, e in particolare il relativo art. 6, comma 1, il quale demanda al Garante il compito di promuovere la sottoscrizione di uno o più codici di deontologia e di buona condotta per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati per scopi di statistica e di ricerca scientifica;

Visto l'articolo 10, comma 6, del medesimo decreto legislativo n. 281/1999, relativo ad alcuni profili che devono essere individuati dal codice per i trattamenti di dati per scopi statistici e di ricerca scientifica;

Visto altresì l'articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322, come modificato dall'articolo 12, comma 6, del decreto legislativo n. 281/1999, nel quale si prevede che la Commissione per la garanzia dell'informazione statistica debba essere sentita ai fini della sottoscrizione dei codici di deontologia e di buona condotta relativi al trattamento dei dati personali nell'ambito del Sistema statistico nazionale;

Visto il provvedimento 10 febbraio 2000 del Garante per la protezione dei dati personali, pubblicato sulla *Gazzetta Ufficiale* n. 46 del 25 febbraio 2000, con il quale il Garante ha promosso la sottoscrizione di uno o più codici di deontologia e di buona condotta relativi del trattamento di dati personali per scopi statistici e di ricerca scientifica ed ha invitato tutti i soggetti aventi titolo a partecipare all'adozione dei medesimi codici in base al principio di rappresentatività a darne comunicazione al Garante entro il 31 marzo 2000;

Viste le comunicazioni pervenute al Garante in risposta al provvedimento del 10 febbraio 2000 , con le quali diversi soggetti pubblici e privati, società scientifiche ed associazioni professionali hanno manifestato la volontà di partecipare alla redazione dei codici e fra i quali è stato conseguentemente costituito un apposito gruppo di lavoro, composto, fra gli altri, da rappresentanti dei seguenti soggetti pubblici: Istituto nazionale di statistica - ISTAT, Istituto di studi e analisi economica - ISAE, Istituto per lo sviluppo della formazione professionale dei lavoratori - ISFOL, Presidenza del Consiglio dei ministri - Dipartimento della funzione pubblica;

Considerato che il testo del codice è stato oggetto di ampia consultazione nell'ambito dei soggetti interessati, che hanno avuto modo di far pervenire osservazioni e proposte;

(*) Provvedimento del Garante n. 13 del 31 luglio 2002, in *Gazzetta Ufficiale* 16 agosto 1999, n. 191

Visto il decreto del Presidente del Consiglio dei ministri 9 marzo 2000, n. 152 contenente le norme per la definizione dei criteri e delle procedure per l'individuazione dei soggetti privati partecipanti al Sistema statistico nazionale (SISTAN) ai sensi dell'articolo 2, comma 1, della legge 28 aprile 1998, n. 125;

Visto il decreto del Presidente del Consiglio dei ministri 9 maggio 2001 in materia di circolazione dei dati all'interno del Sistema statistico nazionale;

Visto il decreto del Presidente del Consiglio dei ministri 28 maggio 2002 sull'inserimento di altri uffici di statistica nell'ambito del SISTAN;

Vista la nota del 2 aprile 2001 con cui il Presidente dell'ISTAT, su mandato del Comitato di indirizzo e coordinamento dell'informazione statistica, ha trasmesso il testo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, sottoscritto dallo stesso a nome dei soggetti interessati;

Vista la deliberazione di questa Autorità n. 23 del 4 luglio 2001 sull'esame preliminare del codice;

Ritenuto opportuno procedere all'esame definitivo del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici effettuati nell'ambito del SISTAN, anche separatamente rispetto al codice che, a norma degli articoli art. 6, comma 1, e 10, comma 6 , del d.lg. n. 281/1999, deve disciplinare l'utilizzo dei dati personali a fini statistici al di fuori del SISTAN;

Sentita la Commissione per la garanzia nell'informazione statistica ai sensi dell'articolo 12, comma 2, del decreto legislativo 6 settembre 1989, n. 322 e sulla base degli approfondimenti curati d'intesa con l'ISTAT;

Rilevato che il rispetto delle disposizioni contenute nel codice costituisce condizione essenziale per la liceità del trattamento dei dati personali;

Constatata la conformità del codice alle leggi e ai regolamenti in materia di protezione delle persone rispetto al trattamento dei dati personali, ed in particolare all'art. 31, comma 1, lettera h) della legge n. 675/1996, nonché agli artt. 6 e 10, 11 e 12 del decreto legislativo n. 281/1999;

Considerato che, ai sensi dell'art. 6, comma 1, del decreto legislativo n. 281/1999, il codice deve essere pubblicato nella *Gazzetta Ufficiale* della Repubblica Italiana a cura del Garante;

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 , adottato con deliberazione n. 15 del 28 giugno 2000 e pubblicato nella *Gazzetta Ufficiale* della Repubblica Italiana n. 162 del 13 luglio 2000;

Dispone:

la trasmissione del codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati nell'ambito del Sistema statistico nazionale, che figura in allegato, all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, 31 luglio 2002

IL PRESIDENTE
IL RELATORE
IL SEGRETARIO GENERALE

CODICE DI DEONTOLOGIA E DI BUONA CONDOTTA PER I TRATTAMENTI DI DATI PERSONALI A SCOPI STATISTICI E DI RICERCA SCIENTIFICA EFFETTUATI NELL'AMBITO DEL SISTEMA STATISTICO NAZIONALE (*)

Preambolo

Il presente codice è volto a garantire che l'utilizzazione di dati di carattere personale per scopi di statistica, considerati dalla legge di rilevante interesse pubblico e fonte dell'informazione statistica ufficiale intesa quale patrimonio della collettività, si svolga nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla riservatezza e del diritto all'identità personale.

Il codice è sottoscritto in attuazione degli articoli 6 e 10, comma 6, del decreto legislativo 30 luglio 1999, n. 281 e si applica ai trattamenti per scopi statistici effettuati nell'ambito del sistema statistico nazionale, per il perseguimento delle finalità di cui al decreto legislativo 6 settembre 1989, n. 322.

La sua sottoscrizione è effettuata ispirandosi alle pertinenti fonti e documenti internazionali in materia di attività statistica e, in particolare:

a) alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950, ratificata dall'Italia con legge 4 agosto 1955, n. 848;
b) alla Carta dei diritti fondamentali dell'Unione Europea del 18 dicembre 2000, con specifico riferimento agli artt. 7 e 8;
c) alla Convenzione n. 108 adottata a Strasburgo il 28 gennaio 1981, ratificata in Italia con legge 21 febbraio 1989, n. 98;
d) alla direttiva n. 95/46/CE del Parlamento europeo e del Consiglio dell'Unione Europea del 24 ottobre 1995;
e) alla Raccomandazione del Consiglio d'Europa n. R(97)18, adottata il 30 settembre 1997;
f) all'articolo 10 del Regolamento (CE) n. 322/97 del Consiglio dell'Unione Europea del 17 febbraio 1997.

Gli enti, gli uffici e i soggetti che applicano il seguente codice sono chiamati ad osservare anche il principio di imparzialità e di non discriminazione nei confronti di altri utilizzatori, in particolare, nell'ambito della comunicazione per scopi statistici di dati depositati in archivi pubblici e trattati da enti pubblici o sulla base di finanziamenti pubblici.

CAPO I - AMBITO DI APPLICAZIONE E PRINCIPI GENERALI

Art. 1. Ambito di applicazione

1. Il codice si applica ai trattamenti di dati personali per scopi statistici effettuati da:
   a) enti ed uffici di statistica che fanno parte o partecipano al Sistema statistico nazionale, per l'attuazione del Programma statistico nazionale o per la produzione di informazione statistica, in conformità ai rispettivi ambiti istituzionali;
   b) strutture diverse dagli uffici di cui alla lettera a), ma appartenenti alla medesima amministrazione o ente, qualora i relativi trattamenti siano previsti dal programma statistico nazionale e gli uffici di statistica attestino le metodologie adottate, osservando le disposizioni contenute nei decreti legislativi 6 settembre 1989, n. 322 e 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni, nonché nel presente codice.

Art. 2. Definizioni

1. Ai fini del presente codice si applicano le definizioni elencate nell'art. 1 della legge 31 dicembre 1996, n. 675 (di seguito denominata "Legge"), nel decreto legislativo 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni. Ai fini medesimi, si intende inoltre per:
   a) "trattamento per scopi statistici", qualsiasi trattamento effettuato per finalità di indagine statistica o di produzione, conservazione e diffusione di risultati statistici in attuazione del Programma statistico nazionale o per effettuare informazione sta-

(*) In conformità all'articolo 184, comma 2, d.lg. 30 giugno 2003, n. 196, i riferimenti a disposizioni della legge n. 675/1996 o ad altre disposizioni abrogate, devono intendersi riferiti alle corrispondenti nuove disposizioni in vigore, secondo la tavola di corrispondenza

tistica in conformità agli ambiti istituzionali dei soggetti di cui all'articolo 1;

b) "risultato statistico", l'informazione ottenuta con il trattamento di dati personali per quantificare aspetti di un fenomeno collettivo;

c) "variabile pubblica", il carattere o la combinazione di caratteri, di tipo qualitativo o quantitativo, oggetto di una rilevazione statistica che faccia riferimento ad informazioni presenti in pubblici registri, elenchi, atti, documenti o fonti conoscibili da chiunque;

d) "unità statistica", l'entità alla quale sono riferiti o riferibili i dati trattati.

Art. 3. Identificabilità dell'interessato

1. Agli effetti dell'applicazione del presente codice:

a) un interessato si ritiene identificabile quando, con l'impiego di mezzi ragionevoli, è possibile stabilire un'associazione significativamente probabile tra la combinazione delle modalità delle variabili relative ad una unità statistica e i dati identificativi della medesima;

b) i mezzi ragionevolmente utilizzabili per identificare un interessato afferiscono, in particolare, alle seguenti categorie:

- risorse economiche;
- risorse di tempo;
- archivi nominativi o altre fonti di informazione contenenti dati identificativi congiuntamente ad un sottoinsieme delle variabili oggetto di comunicazione o diffusione;
- archivi, anche non nominativi, che forniscano ulteriori informazioni oltre a quelle oggetto di comunicazione o diffusione;
- risorse hardware e software per effettuare le elaborazioni necessarie per collegare informazioni non nominative ad un soggetto identificato, tenendo anche conto delle effettive possibilità di pervenire in modo illecito alla sua identificazione in rapporto ai sistemi di sicurezza ed al software di controllo adottati;
- conoscenza delle procedure di estrazione campionaria, imputazione, correzione e protezione statistica adottate per la produzione dei dati;

c) in caso di comunicazione e di diffusione, l'interessato può ritenersi non identificabile se il rischio di identificazione, in termini di probabilità di identificare l'interessato stesso tenendo conto dei dati comunicati o diffusi, è tale da far ritenere sproporzionati i mezzi eventualmente necessari per procedere all'identificazione rispetto alla lesione o al pericolo di lesione dei diritti degli interessati che può derivarne, avuto altresì riguardo al vantaggio che se ne può trarre.

Art. 4. Criteri per la valutazione del rischio di identificazione

1. Ai fini della comunicazione e diffusione di risultati statistici, la valutazione del rischio di identificazione tiene conto dei seguenti criteri:

a) si considerano dati aggregati le combinazioni di modalità alle quali è associata una frequenza non inferiore a una soglia prestabilita, ovvero un'intensità data dalla sintesi dei valori assunti da un numero di unità statistiche pari alla suddetta soglia. Il valore minimo attribuibile alla soglia è pari a tre;

b) nel valutare il valore della soglia si deve tenere conto del livello di riservatezza delle informazioni;

c) i risultati statistici relativi a sole variabili pubbliche non sono soggetti alla regola della soglia;

d) la regola della soglia può non essere osservata qualora il risultato statistico non consenta ragionevolmente l'identificazione di unità statistiche, avuto riguardo al tipo di rilevazione e alla natura delle variabili associate;

e) i risultati statistici relativi a una stessa popolazione possono essere diffusi in modo che non siano possibili collegamenti tra loro o con altre fonti note di informazione, che rendano possibili eventuali identificazioni;

f) si presume che sia adeguatamente tutelata la riservatezza nel caso in cui tutte le unità statistiche di una popolazione presentino la medesima modalità di una variabile.

2. Nel Programma statistico nazionale sono individuate le variabili che possono essere diffuse in forma disaggregata, ove ciò risulti necessario per soddisfare particolari esigenze

conoscitive anche di carattere internazionale o comunitario.

3. Nella comunicazione di collezioni campionarie di dati, il rischio di identificazione deve essere per quanto possibile contenuto. Tale limite e la metodologia per la stima del rischio di identificazione sono individuati dall'ISTAT che, attenendosi ai criteri di cui all'art. 3, comma 1, lett. d), definisce anche le modalità di rilascio dei dati dandone comunicazione alla Commissione per la garanzia dell'informazione statistica.

Art. 5. Trattamento di dati sensibili da parte di soggetti privati

1. I soggetti privati che partecipano al Sistema statistico nazionale ai sensi della legge 28 aprile 1998, n. 125, raccolgono o trattano ulteriormente dati sensibili per scopi statistici di regola in forma anonima, fermo restando quanto previsto dall'art. 6-bis, comma 1, del decreto legislativo 6 settembre 1989, n. 322, come introdotto dal decreto legislativo 30 luglio 1999, n. 281, e successive modificazioni e integrazioni.

2. In casi particolari in cui scopi statistici, legittimi e specifici, del trattamento di dati sensibili non possono essere raggiunti senza l'identificazione anche temporanea degli interessati, per garantire la legittimità del trattamento medesimo è necessario che concorrano i seguenti presupposti:

a) l'interessato abbia espresso liberamente il proprio consenso sulla base degli elementi previsti per l'informativa;
b) il titolare adotti specifiche misure per mantenere separati i dati identificativi già al momento della raccolta, salvo che ciò risulti irragionevole o richieda uno sforzo manifestamente sproporzionato;
c) il trattamento risulti preventivamente autorizzato dal Garante, anche sulla base di un'autorizzazione relativa a categorie di dati o tipologie di trattamenti, o sia compreso nel programma statistico nazionale.

3. Il consenso è manifestato per iscritto. Qualora la raccolta dei dati sensibili sia effettuata con particolari modalità quali interviste telefoniche o assistite da elaboratore che rendano particolarmente gravoso per l'indagine acquisirlo per iscritto, il consenso, purché espresso, può essere documentato per iscritto. In tal caso, la documentazione dell'informativa resa all'interessato e dell'acquisizione del relativo consenso è conservata dal titolare del trattamento per tre anni.

CAPO II - INFORMATIVA, COMUNICAZIONE E DIFFUSIONE

Art. 6. Informativa

1. Oltre alle informazioni di cui all'art. 10 della Legge, all'interessato o alle persone presso le quali i dati personali dell'interessato sono raccolti per uno scopo statistico è rappresentata l'eventualità che essi possono essere trattati per altri scopi statistici, in conformità a quanto previsto dai decreti legislativi 6 settembre 1989, n. 322 e 30 luglio 1999, n. 281, e loro successive modificazioni e integrazioni.

2. Quando il trattamento riguarda dati personali non raccolti presso l'interessato e il conferimento dell'informativa a quest'ultimo richieda uno sforzo sproporzionato rispetto al diritto tutelato, in base a quanto previsto dall'art. 10, comma 4 della Legge, l'informativa stessa si considera resa se il trattamento è incluso nel programma statistico nazionale o è oggetto di pubblicità con idonee modalità da comunicare preventivamente al Garante il quale può prescrivere eventuali misure ed accorgimenti.

3. Nella raccolta di dati per uno scopo statistico, l'informativa alla persona presso la quale i dati sono raccolti può essere differita per la parte riguardante le specifiche finalità, le modalità del trattamento cui sono destinati i dati, qualora ciò risulti necessario per il raggiungimento dell'obiettivo dell'indagine -in relazione all'argomento o alla natura della stessa- e purché il trattamento non riguardi dati sensibili. In tali casi, il completamento dell'informativa deve essere fornito all'interessato non appena vengano a cessare i motivi che ne avevano ritardato la comunicazione, a meno che ciò comporti un impiego di mezzi palesemente sproporzionato. Il soggetto responsabile della ricerca deve redigere un documento -

successivamente conservato per almeno due anni dalla conclusione della ricerca e reso disponibile a tutti i soggetti che esercitano i diritti di cui all'art. 13 della Legge- in cui siano indicate le specifiche motivazioni per le quali si è ritenuto di differire l'informativa, la parte di informativa differita, nonché le modalità seguite per informare gli interessati quando sono venute meno le ragioni che avevano giustificato il differimento.

4. Quando le circostanze della raccolta e gli obiettivi dell'indagine sono tali da consentire ad un soggetto di rispondere in nome e per conto di un altro, in quanto familiare o convivente, l'informativa all'interessato può essere data anche per il tramite del soggetto rispondente.

Art. 7. Comunicazione a soggetti non facenti parte del Sistema statistico nazionale

1. Ai soggetti che non fanno parte del Sistema statistico nazionale possono essere comunicati, sotto forma di collezioni campionarie, dati individuali privi di ogni riferimento che ne permetta il collegamento con gli interessati e comunque secondo modalità che rendano questi ultimi non identificabili.

2. La comunicazione di dati personali a ricercatori di università o ad istituti o enti di ricerca o a soci di società scientifiche a cui si applica il codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e di ricerca scientifica effettuati fuori dal Sistema statistico nazionale, di cui all'articolo 10, comma 6, del decreto legislativo 30 luglio 1999, n. 281 e successive modificazioni e integrazioni, è consentita nell'ambito di specifici laboratori costituiti da soggetti del Sistema statistico nazionale, a condizione che:

a) i dati siano il risultato di trattamenti di cui i medesimi soggetti del Sistema statistico nazionale siano titolari;
b) i dati comunicati siano privi di dati identificativi;
c) le norme in materia di segreto statistico e di protezione dei dati personali, contenute anche nel presente codice, siano rispettate dai ricercatori che accedono al laboratorio anche sulla base di una preventiva dichiarazione di impegno;
d) l'accesso al laboratorio sia controllato e vigilato;
e) non sia consentito l'accesso ad archivi di dati diversi da quello oggetto della comunicazione;
f) siano adottate misure idonee affinché le operazioni di immissione e prelievo di dati siano inibite ai ricercatori che utilizzano il laboratorio;
g) il rilascio dei risultati delle elaborazioni effettuate dai ricercatori che utilizzano il laboratorio sia autorizzato solo dopo una preventiva verifica, da parte degli addetti al laboratorio stesso, del rispetto delle norme di cui alla lettera c).

3. Nell'ambito di progetti congiunti, finalizzati anche al perseguimento di compiti istituzionali del titolare del trattamento che ha originato i dati, i soggetti del sistema statistico nazionale possono comunicare dati personali a ricercatori operanti per conto di università, altre istituzioni pubbliche e organismi aventi finalità di ricerca, purché sia garantito il rispetto delle condizioni seguenti:

a) i dati siano il risultato di trattamenti di cui i medesimi soggetti del sistema statistico nazionale sono titolari;
b) i dati comunicati siano privi di dati identificativi;
c) la comunicazione avvenga sulla base di appositi protocolli di ricerca sottoscritti da tutti i ricercatori che partecipano al progetto;
d) nei medesimi protocolli siano esplicitamente previste, come vincolanti per tutti i ricercatori che partecipano al progetto, le norme in materia di segreto statistico e di protezione dei dati personali contenute anche nel presente codice.

4. È vietato ai ricercatori ammessi alla comunicazione dei dati di effettuare trattamenti per fini diversi da quelli esplicitamente previsti dal protocollo di ricerca, di conservare i dati comunicati oltre i termini di durata del progetto, di comunicare ulteriormente i dati a terzi.

Art. 8. Comunicazione dei dati tra soggetti del Sistema statistico nazionale

1. La comunicazione di dati personali, privi di dati identificativi, tra i soggetti del Sistema statistico nazionale è consentita per i trattamenti statistici, strumentali al perseguì-

mento delle finalità istituzionali del soggetto richiedente, espressamente determinati all'atto della richiesta, fermo restando il rispetto dei principi di pertinenza e di non eccedenza.

2. La comunicazione anche dei dati identificativi di unità statistiche tra i soggetti del Sistema statistico nazionale è consentita, previa motivata richiesta in cui siano esplicitate le finalità perseguite ai sensi del decreto legislativo 6 settembre 1989, n. 322, ivi comprese le finalità di ricerca scientifica per gli enti di cui all'art. 2 del decreto legislativo medesimo, qualora il richiedente dichiari che non sia possibile conseguire altrimenti il medesimo risultato statistico e, comunque, nel rispetto dei principi di pertinenza e di stretta necessità.

3. I dati comunicati ai sensi dei commi 1 e 2 possono essere trattati dal soggetto richiedente, anche successivamente, per le sole finalità perseguite ai sensi del decreto legislativo 6 settembre 1989, n. 322, ivi comprese le finalità di ricerca scientifica per gli enti di cui all'art. 2 del decreto legislativo medesimo, nei limiti previsti dal decreto legislativo 30 luglio 1999, n. 281, e nel rispetto delle misure di sicurezza previste dall'art. 15 della Legge e successive modificazioni e integrazioni.

Art. 9. Autorità di controllo

1. La Commissione per la garanzia dell'informazione statistica di cui all'articolo 12 del decreto legislativo 6 settembre 1989, n. 322 contribuisce alla corretta applicazione delle disposizioni del presente codice e, in particolare, di quanto previsto al precedente art. 8, segnalando al Garante i casi di inosservanza.

Capo III - Sicurezza e regole di condotta

Art. 10. Raccolta dei dati

1. I soggetti di cui all'art. 1 pongono specifica attenzione nella selezione del personale incaricato della raccolta dei dati e nella definizione dell'organizzazione e delle modalità di rilevazione, in modo da garantire il rispetto del presente codice e la tutela dei diritti degli interessati, procedendo altresì alla designazione degli incaricati del trattamento, secondo le modalità di legge.

2. In ogni caso, il personale incaricato della raccolta si attiene alle disposizioni contenute nel presente codice e alle istruzioni ricevute. In particolare:

a) rende nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;
b) fornisce le informazioni di cui all'art. 10 della Legge e di cui all'art. 6 del presente codice, nonché ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici o indebite pressioni;
c) non svolge contestualmente presso gli stessi interessati attività di rilevazione di dati per conto di più titolari, salvo espressa autorizzazione;
d) provvede tempestivamente alla correzione degli errori e delle inesattezze delle informazioni acquisite nel corso della raccolta;
e) assicura una particolare diligenza nella raccolta di dati personali di cui agli articoli 22, 24 e 24 bis della Legge.

Art. 11. Conservazione dei dati

1. I dati personali possono essere conservati anche oltre il periodo necessario per il raggiungimento degli scopi per i quali sono stati raccolti o successivamente trattati, in conformità all'art. 9 della Legge e all'art. 6-bis del decreto legislativo 6 settembre 1989, n. 322 e successive modificazioni e integrazioni. In tali casi, i dati identificativi possono essere conservati fino a quando risultino necessari per:

- indagini continue e longitudinali;
- indagini di controllo, di qualità e di copertura;
- definizione di disegni campionari e selezione di unità di rilevazione;
- costituzione di archivi delle unità statistiche e di sistemi informativi;
- altri casi in cui ciò risulti essenziale e adeguatamente documentato per le finalità perseguite.

2. Nei casi di cui al comma 1, i dati identificativi sono conservati separatamente da ogni altro dato, in modo da consentirne differenti livelli di accesso, salvo che ciò risulti impossibile in ragione delle particolari caratteristiche del trattamento o comporti un impiego di mezzi manifestamente sproporzionati rispetto al diritto tutelato.

Art. 12. Misure di sicurezza

1. Nell'adottare le misure di sicurezza di cui all'art. 15, comma 1, della Legge e di cui al regolamento previsto dal comma 2 del medesimo articolo, il titolare del trattamento determina anche i differenti livelli di accesso ai dati personali con riferimento alla natura dei dati stessi e alle funzioni dei soggetti coinvolti nei trattamenti.

2. I soggetti di cui all'art. 1 adottano le cautele previste dagli articoli 3 e 4 del decreto legislativo 11 maggio 1999, n. 135 in riferimento ai dati di cui agli articoli 22 e 24 della Legge.

Art. 13. Esercizio dei diritti dell'interessato

1. In caso di esercizio dei diritti di cui all'art.13 della Legge, l'interessato può accedere agli archivi statistici contenenti i dati che lo riguardano per chiederne l'aggiornamento, la rettifica o l'integrazione, sempre che tale operazione non risulti impossibile per la natura o lo stato del trattamento, o comporti un impiego di mezzi manifestamente sproporzionati.

2. In attuazione dell'art. 6-bis, comma 8, del decreto legislativo 6 settembre 1989, n. 322, il responsabile del trattamento annota in appositi spazi o registri le modifiche richieste dall'interessato, senza variare i dati originariamente immessi nell'archivio, qualora tali operazioni non producano effetti significativi sull'analisi statistica o sui risultati statistici connessi al trattamento. In particolare, non si procede alla variazione se le modifiche richieste contrastano con le classificazioni e con le metodologie statistiche adottate in conformità alle norme internazionali comunitarie e nazionali.

Art. 14. Regole di condotta

1. I responsabili e gli incaricati del trattamento che, anche per motivi di lavoro, studio e ricerca abbiano legittimo accesso ai dati personali trattati per scopi statistici, conformano il proprio comportamento anche alle seguenti disposizioni:

a) i dati personali possono essere utilizzati soltanto per gli scopi definiti all'atto della progettazione del trattamento;
b) i dati personali devono essere conservati in modo da evitarne la dispersione, la sottrazione e ogni altro uso non conforme alla legge e alle istruzioni ricevute;
c) i dati personali e le notizie non disponibili al pubblico di cui si venga a conoscenza in occasione dello svolgimento dell'attività statistica o di attività ad essa strumentali non possono essere diffusi, né altrimenti utilizzati per interessi privati, propri o altrui;
d) il lavoro svolto deve essere oggetto di adeguata documentazione;
e) le conoscenze professionali in materia di protezione dei dati personali devono essere adeguate costantemente all'evoluzione delle metodologie e delle tecniche;
f) la comunicazione e la diffusione dei risultati statistici devono essere favorite, in relazione alle esigenze conoscitive degli utenti, purché nel rispetto delle norme sulla protezione dei dati personali.

2. I responsabili e gli incaricati del trattamento di cui al comma 1 sono tenuti a conformarsi alle disposizioni del presente codice, anche quando non siano vincolati al rispetto del segreto d'ufficio o del segreto professionale. I titolari del trattamento adottano le misure opportune per garantire la conoscenza di tali disposizioni da parte dei responsabili e degli incaricati medesimi.

3. I comportamenti non conformi alle regole di condotta dettate dal presente codice devono essere immediatamente segnalati al responsabile o al titolare del trattamento.

Misure minime di sicurezza

B

Disciplinare tecnico in materia di misure minime di sicurezza (*)

TRATTAMENTI CON STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

SISTEMA DI AUTENTICAZIONE INFORMATICA

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impar-

(*) Artt. da 33 a 36 del Codice

tite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

SISTEMA DI AUTORIZZAZIONE

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

ALTRE MISURE DI SICUREZZA

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più

rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

MISURE DI TUTELA E GARANZIA

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai sin-

goli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia

C

Si tratta di un allegato che, allo stato, non comprende ancora i decreti in fase di adozione:

- decreto del Ministro della giustizia da adottare ai sensi dell'art. 46 del Codice;
- decreto del Ministro dell'interno da adottare ai sensi dell'art. 53 del Codice.

Artt. 46 e 53 del Codice