

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. *b*), 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

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

Principio di
"stabilimento"

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 video-sorveglianza. 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).

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

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.

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.

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-

Codici di deontologia di imminente sottoscrizione

D.l. 24 dicembre 2003, n. 354

Modifiche all'art. 132 del Codice

Rischi segnalati dal Garante

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.

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.

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

Le preoccupazioni
manifestate dal Garante

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;

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

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 <i>privacy</i> 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

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).

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.

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

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.

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.

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.

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.

Aziende e imprese

Cittadini

La situazione italiana

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 (*Prov. 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.

Sempre con riferimento al diritto di accesso del lavoratore ai dati che lo riguardano, il Garante ha stabilito (*Prov. 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