La richiesta di riconsiderare il progetto è stata dettata dal pericolo di un allargamento delle originarie finalità del registro per interessi commerciali nonché dalla consapevolezza che il rischio di identificare il singolo, considerata anche la particolare natura dei dati, aumenta notevolmente in un Paese con una popolazione relativamente scarsa.

2.10 Istituti di credito e assicurazioni

Il settore bancario e quello assicurativo sono stati coinvolti in modo rilevante dall'applicazione delle disposizioni sul trattamento dei dati personali. La l. n. 675/1996 ha infatti introdotto precise regole giuridiche a tutela della riservatezza delle persone, che hanno integrato e rafforzato le misure e gli accorgimenti che venivano adottati già dagli operatori di questi settori per garantire la segretezza e la confidenzialità delle informazioni personali acquisite nei rapporti con la clientela.

I problemi maggiori riscontrati dalle banche e dalle assicurazioni, anche nell'anno 1998, sono derivati dalla gestione degli adempimenti relativi all'*informativa* e al *consenso* (v. la *Relazione per l'anno 1997*, cap. 4.4., pagg. 72 e ss.).

In quest'anno il Garante ha svolto un'intensa attività di verifica sul pieno rispetto dei princìpi già affermati in precedenti provvedimenti, soprattutto per quanto riguarda il settore creditizio e finanziario (*v. cap. 2.2)*.

Tale settore è stato interessato da un'apposita indagine conoscitiva, che l'Ufficio ha svolto chiedendo informazioni a numerosi istituti di credito e che ha riguardato oltre 800 modelli sottoposti ai clienti delle diverse banche. Al tempo stesso, l'Autorità ha continuato l'attività di consultazione, anche nell'ambito di specifici gruppi di lavoro, con le principali istituzioni e società bancarie.

In sintesi si è appurato che, a seguito delle indicazioni generali fornite dal Garante, i cui contenuti sono stati ampiamente riportati sulla stampa, varie società operanti nel settore hanno riformulato i modelli già distribuiti ai propri clienti, inviandoli nuovamente a tutta la clientela.

La modulistica distribuita dalle banche, per quanto complessa e non facilmente comprensibile per il cittadino, è apparsa in buona parte conforme ai princìpi evidenziati dall'Autorità, avendo previsto di regola la possibilità per la clientela di esprimere il proprio consenso «informato» nei riguardi dei trattamenti anche non strettamente connessi ai servizi richiesti contrattualmente (in riferimento, ad es., all'invio di materiale pubblicitario e, in genere, all'offerta di prodotti e servizi anche di società terze), senza che ciò abbia alcun riflesso sul contratto medesimo.

Tuttavia, l'Autorità ha constatato che diversi clienti non hanno ancora dato riscontro ai modelli inviati dalle banche e dalle altre società operanti nel settore.

Il problema del mancato ritorno del consenso è stato fronteggiato temporaneamente con la soluzione già prospettata nel 1997 dal Garante in base alla quale, nell'eventuale attesa del rilascio della dichiarazione relativa al consenso, la richiesta di una prestazione da parte del cliente (es.: l'emissione di un assegno, il bonifico bancario) può essere considerata come una manifestazione di volontà equiparabile al consenso per le operazioni di trattamento connesse a quella prestazione, sia pure in via del tutto provvisoria.

Trattandosi di soluzione transitoria, vi è pertanto la necessità che la clientela rimasta inerte sia nuovamente stimolata a esprimere il proprio consenso, in modo da arrivare a una piena regolarizzazione dei trattamenti di dati svolti dagli istituti di credito.

Il Garante stesso, nei primi mesi dell'anno, si è impegnato a formulare schemi di modelli che, pur mantenendo ferme le sostanziali garanzie a tutela dei diritti degli interessati, siano più semplici e meglio comprensibili, in modo da permettere ai clienti di fornire più agevolmente un rapido riscontro alle richieste di consenso formulate dalle società bancarie.

Un primo nuovo schema di informativa e di consenso è stato messo a punto alla fine del 1998, e nei primi giorni di febbraio 1999 l'Autorità, considerato il generale interesse alla tematica, ha ritenuto opportuno renderlo pubblico attraverso gli organi di informazione, sottoponendolo all'attenzione degli istituti di credito, degli utenti e dei loro organismi rappresentativi, anche per avere loro osservazioni e suggerimenti.

Essendosi conclusa l'analisi delle osservazioni pervenute, il Garante trasmetterà il nuovo modello revisionato a tutti gli operatori del settore bancario, che comunque hanno intenzione di inviare alla clientela un opportuno messaggio di richiamo (inserito, in particolare, negli estratti conto).

È evidente che lo schema di modello potrà essere utile anche per altri settori economici, finanziari e produttivi, come appunto quello delle assicurazioni, che hanno spesso riscontrato problemi analoghi a quelli delle banche e hanno più volte chiesto all'Autorità, per il tramite dell'associazione di categoria (ANIA), di avere precise indicazioni al fine di rendere più comprensibile la modulistica già distribuita ai propri clienti.

Una problematica particolarmente delicata affrontata dagli operatori del settore bancario e assicurativo è senz'altro quella del trattamento dei dati aventi natura sensibile (stato di salute, opinioni sindacali o politiche, ecc.).

In attesa delle precise indicazioni che verranno fornite nei decreti delegati previsti entro la fine di luglio 1999, sono applicabili al riguardo le regole più generali previste dalla l. n. 675/1996 (consenso scritto degli interessati, previa autorizzazione del Garante: art. 22, comma 1). Sotto questo profilo, l'Autorità ha rinnovato quest'anno, con alcune lievi modifiche, le autorizzazioni generali già rilasciate nel 1997 per il trattamento di questi dati (v. § 3.1.3), tenendo presenti anche talune particolari esigenze evidenziate dagli operatori (è stata, ad esempio, rilasciata una specifica autorizzazione a una società cooperativa di assicurazione che, a livello statutario, prevede per i propri soci la professione di determinate convinzioni religiose).

Per quanto riguarda, poi, altri temi specifici relativi alla tutela dei dati personali, occorre di seguito soffermare brevemente l'attenzione su alcuni provvedimenti dell'Autorità che rivestono maggiore interesse soprattutto per il settore bancario e finanziario.

L'Autorità ha anzitutto esaminato, a seguito di alcune segnalazioni, la questione del rispetto della cd. distanza di cortesia presso gli sportelli degli istituti di credito (già nota alle banche e, in parte, disciplinata attraverso il Codice di comportamento del settore bancario e finanziario adottato dall'ABI).

Al riguardo il Garante ha evidenziato che, anche in virtù delle disposizioni previste dalla l. n. 675/1996 in materia di sicurezza dei dati personali, le banche devono adottare ogni utile iniziativa per garantire la distanza di cortesia, la quale rappresenta una misura opportuna per prevenire l'impropria conoscenza da parte di terzi delle informazioni eventualmente fornite dal cliente all'operatore di sportello.

L'Autorità garante è dovuta intervenire anche relativamente al cd. *benefondi*, ossia in ordine alla prassi consolidata nell'attività bancaria, basata su accertamenti anche informali, attraverso i quali viene garantita l'esistenza presso la banca di fondi sufficienti a coprire gli assegni emessi. L'intervento si è reso necessario perché, secondo le numerose segnalazioni pervenute all'Ufficio, talune banche si sono rifiutate in nome della *privacy* di rilasciare il *benefondi* su assegni emessi dai propri clienti.

Il Garante, che si era già espresso sull'argomento in precedenti occasioni, ha affermato che la l. n. 675/1996 non ha introdotto alcun divieto nei confronti del *benefondi*. Queste informazioni possono essere fornite dagli istituti di credito nel rispetto dei princìpi generali che la legge stessa prevede per tutti i trattamenti di dati personali svolti dalle banche e secondo le indicazioni generali riportate nei modelli di informativa e di richiesta del consenso distribuiti alla clientela (nelle quali rientra anche questo tipo di operazione necessaria per una corretta esecuzione del rapporto bancario). Si è comunque sottolineata l'esigenza che la prassi del *benefondi* sia svolta correttamente e che le informazioni siano fornite ai soli soggetti legittimati all'incasso o alla negoziazione dell'assegno e non a estranei.

Sempre in ambito bancario, alcune associazioni dei consumatori e diversi cittadini hanno chiesto all'Autorità di verificare la legittimità dell'attività svolta da una società che gestisce carte di credito e di pagamento, la quale, secondo la segnalazione, avrebbe inviato alla propria clientela, con l'estratto conto mensile, materiale pubblicitario non richiesto dai titolari delle carte, ai quali sarebbero stati addebitati, invece, i relativi costi di spedizione.

Anche in questo caso il Garante ha avuto modo di precisare che la l. n. 675/1996 non ha introdotto un divieto generalizzato nei confronti della raccolta e dell'utilizzazione dei dati personali per finalità commerciali o di *marketing*, ma ha individuato, piuttosto, i presupposti fondamentali sulla base dei quali è possibile effettuare tali operazioni - presupposti che sono in buona parte comuni agli altri trattamenti di dati effettuati nel settore (in particolare, l'informativa e, ove necessario, la richiesta del consenso).

Si è inoltre ricordato che la direttiva comunitaria n. 95/46/CE e la l. n. 675/1996 recano alcune norme transitorie che rendono al momento possibile non richiedere il consenso degli interessati qualora il trattamento riguardi dati raccolti prima dell'8 maggio 1997 (data di entrata in vigore della legge stessa), o sia iniziato anteriormente a tale data (sempre che il soggetto che tratta i dati non li divulghi a terzi: v. art. 41, comma 1). Questa disciplina transitoria non preclude però alla persona interessata di avvalersi dei nuovi diritti previsti dall'art. 13 della l. n. 675/1996, chiedendo alla stessa società «titolare del trattamento» (o al soggetto da essa designato come «responsabile») l'immediata cessazione delle operazioni collegate all'invio di materiale pubblicitario, ovvero al compimento di operazioni di *marketing*.

Per quanto riguarda gli aspetti di propria competenza, il Garante ha constatato che la società ha provveduto, anche sulla scorta delle indicazioni fornite nel 1997 dalla stessa Autorità, a inviare ai titolari di carte di credito l'informativa e la richiesta del consenso, prevedendo specifiche opzioni. Tra esse, appunto, quella concernente il trattamento dei dati a fini di informazione e promozione di prodotti o servizi, mediante annunci inseriti nelle comunicazioni periodiche ai titolari. Tale procedura sarebbe stata quindi seguita anche nei riguardi di clienti i cui dati sono stati acquisiti e trattati, anche a scopo pubblicitario, prima dell'entrata in vigore della legge.

L'invio da parte della società di materiale commerciale relativo anche a società terze non comporta, di per se stesso, una comunicazione a tali società dei nominativi e degli indirizzi dei titolari delle carte di credito e non rende al momento necessario raccogliere il consenso dei clienti nei cui confronti tale trattamento sia iniziato prima dell'8 maggio 1997. A diversa conclusione si dovrebbe semmai pervenire nella circostanza, non segnalata all'Ufficio, in cui risultasse una comunicazione dei dati relativi ai clienti rivolta alle società terze alle quali si riferisce la pubblicità inserita negli estratti conto.

L'Autorità ha infine ricordato agli interessati che la società che gestisce le carte di credito ha comunque dichiarato che esaudirà scrupolosamente le eventuali richieste della clientela che non intenda più ricevere materiale pubblicitario riferito anche a società terze, a prescindere dal fatto che gli stessi abbiano eventualmente manifestato un precedente consenso al riguardo.

Più in generale, per ciò che attiene alle problematiche del *direct marketing*, si osserva che, dagli accertamenti effettuati in ambito bancario e finanziario, una parte della clientela ha manifestato, sulla base della modulistica distribuita, un diniego nei riguardi dell'utilizzo dei dati per l'invio di materiale diverso da quello legato al servizio richiesto a livello contrattuale.

In ogni caso, per risolvere le predette problematiche, l'Autorità ha avviato alcune procedure di consultazione con gli operatori del settore e le principali istituzioni finanziarie, il cui lavoro potrebbe essere utile anche in sede di predisposizione da parte del Governo del decreto legislativo che dovrà dettare regole specifiche per questa materia, recependo anche le linee guida indicate nella raccomandazione del Consiglio d'Europa n. R. (85) 20, del 25 ottobre 1985, sui dati utilizzati per fini di *direct marketing*.

2.11 Intermediazione finanziaria

Un problema di tutela dell'interessato di fronte al trattamento di dati personali compiuto da terzi, si può porre, naturalmente, anche con riguardo all'attività di intermediazione finanziaria.

Ciò anzitutto perché, per sua natura, l'attività di prestazione di servizi di investimento e accessori può essere svolta al meglio dall'intermediario soltanto a condizione di avere piena cognizione di talune informazioni di carattere personale (situazione patrimoniale, propensione al rischio, ecc.), che devono essere richieste al risparmiatore (art. 28, reg. CONSOB 1° luglio 1998, n. 11522). In altre parole, ferma restando la possibilità del rifiuto di fornire i dati, sono gli stessi caratteri dell'attività in questione a esprimere il principio del *know your customer* così definito dalla Corte di Cassazione in una recente sentenza (14 novembre 1997, n. 11279).

I dati richiesti possono avere anche carattere sensibile e avendo presente questa non rara ipotesi il Garante ha perciò incluso gli intermediari finanziari (assumendone un'accezione ampia) tra i destinatari dell'autorizzazione generale n. 5 del 1998. Per effetto di essa, a detti soggetti è quindi consentito il trattamento dei dati sensibili di cui all'art. 22, comma 1, della l. 31 dicembre 1996, n. 675, fatta eccezione per i dati idonei a rivelare la vita sessuale.

Per altro verso, nel settore in esame si pone anche un problema di tutela della riservatezza di taluni soggetti che operano dal lato dell'offerta di prodotti finanziari. Per il corretto funzionamento del mercato finanziario, infatti, è essenziale che i potenziali investitori siano in grado di conoscere la maggior quantità possibile di informazioni relative alle società che vi operano, allo scopo di potere compiere quelle che la normativa vigente chiama «consapevoli scelte di investimento».

Tra queste informazioni è evidente che possono assumere grande importanza, nell'apprezzamento del pubblico, anche quelle relative, a seconda dei casi, all'onorabilità, alla professionalità o ai compensi percepiti dagli esponenti aziendali (amministratori, sindaci, ecc.). Al riguardo, però, ognuno intende che simili soggetti hanno, per contro, interesse a non essere esposti ingiustificatamente, e in ogni caso non oltre il necessario, alla curiosità altrui.

In merito il Garante ha avuto occasione di pronunciarsi più volte, nel corso del 1998 (v. il provvedimento del 10 febbraio 1998 relativo all'ISVAP, nonché quello del 18 novembre 1998, relativo all'art. 32 del reg. CONSOB 1° luglio 1998, n. 11520), sancendo l'importante principio secondo il quale il diritto dei potenziali investitori di conoscere le predette informazioni prevale sulle esigenze di riservatezza degli esponenti aziendali, a patto che il sacrificio sia autorizzato da un'idonea fonte normativa (nel minimo un regolamento, non essendo invece sufficiente un mero decreto ministeriale).

Al riguardo si veda anche la pronuncia del 16 febbraio 1999 (di cui si è già detto nel § 2.2.3) nella quale il Garante ha esaminato la nozione di «attività economiche» al fine di chiarire l'ambito di applicazione delle disposizioni della l. n. 675/1996 (artt. 12, comma 1, lett. *f*) e 20, comma 1, lett. *e*) che prevedono, quale ipotesi di esclusione del consenso dell'interessato, il trattamento che «riguardi dati relativi allo svolgimento di attività economiche».

Al di là dei riscontri concreti, che nel numero vanno ben oltre quelli qui ricordati, è in ogni caso agevole prevedere che il settore dell'attività di intermediazione finanziaria sia tra quelli che maggiormente alimenteranno il dibattito scientifico e il contenzioso amministrativo negli anni a venire, in considerazione del suo grado crescente di complessità e di ricchezza di implicazioni.

2.12 Informatica e telecomunicazioni

2.12.1 Telefonia e servizi di telecomunicazioni

L'universo delle telecomunicazioni e, al suo interno, il settore della telefonia ha costituito oggetto di particolare attenzione da parte del Garante nel corso del 1998, sia per le innovazioni legislative che hanno contraddistinto questo ambito, sia per le molte segnalazioni pervenute in merito, che dimostrano la particolare sensibilità dell'opinione pubblica.

2.12.1.1 La nuova normativa di tutela nelle telecomunicazioni

Le innovazioni più significative in materia di protezione della vita privata nel settore delle telecomunicazioni sono state introdotte in Italia con il d.lg. 13 maggio 1998, n. 171, a cui si era fatto già cenno nella *Relazione per l'anno 1997* (con particolare riguardo alla descrizione del provvedimento adottato dal Garante sull'obbligo, previsto dal d.P.R. n. 318/1997 per ogni organismo di telecomunicazione, di rendere disponibili gli elenchi degli abbonati e degli utenti al C.e.d. del Ministero dell'interno: cfr. *Relazione per l'anno 1997*, cap. 4.8, pagg. 87 e ss.).

L'emanazione di un apposito decreto legislativo al fine di adeguare la normativa di settore ai criteri direttivi e ai princìpi della normativa comunitaria e della raccomandazione del Consiglio d'Europa (95) 4 del 7 febbraio 1995 era stata prevista dalla legge delega n. 676/1996 (art. 1, comma 1, lett. *b)*, n. 7).

Una disciplina più specifica in proposito è stata introdotta poi dalla direttiva n. 97/66/CE del Parlamento europeo e del Consiglio «sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni».

Il d.lg. n. 171/1998 ha dato pertanto attuazione a tali disposizioni comunitarie nel quadro dei principi generali contenuti nelle leggi nn. 675/1996 e 676/1996, tenendo conto delle norme delineate dal menzionato d.P.R. n. 318/1997 e dal d.m. 25 novembre 1997 sul rilascio delle licenze individuali, che avevano anticipato già il recepimento nell'ordinamento italiano di un primo corpo di disposizioni comunitarie.

Vengono di seguito segnalate, sinteticamente, alcune disposizioni più significative introdotte dal citato decreto legislativo.

- Definizioni - L'art. 1 propone le definizioni tecniche di abbonato, utente ecc. e, in un sistema ormai aperto alla concorrenza fra diversi operatori, fissa la distinzione fra «rete pubblica di telecomunicazioni» e «servizio di telecomunicazioni», consistente quest'ultimo «nella trasmissione e nell'instradamento di segnali su reti di telecomunicazioni, ivi compreso qualsiasi servizio interattivo anche se relativo a prodotti audiovisivi, esclusa la diffusione circolare dei programmi radiofonici e televisivi» (art. 1, comma 1 lett. *d*)).

- Sicurezza e riservatezza delle comunicazioni - Particolare attenzione è prestata a questi profili con obblighi che rimandano alle prescrizioni dell'art. 15 della l. n. 675/1996 e che impongono un onere di informativa da parte dei fornitori dei servizi di telecomunicazione nei confronti degli abbonati, specie quando sussistano particolari rischi di violazione della sicurezza della rete.

I fornitori di servizi devono informare, altresì, abbonati e utenti circa la «sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti a esse estranei» (art. 3, comma 1).

Analogo obbligo di informativa grava sull'abbonato quando i terminali o comunque le apparecchiature utilizzate possano determinare il rischio che il contenuto delle conversazioni fatte dall'utente sia appreso da estranei (art. 3, comma 2). Va ricordato poi l'obbligo dell'utente di avvisare le persone con le quali conversa, qualora faccia uso del meccanismo cd. «viva voce» (art. 3, comma 3).

Dati relativi a traffico, modalità di pagamento, fatturazione dettagliata - Il decreto definisce con precisione quali dati personali (indirizzo, numero dell'abbonato, numero totale degli scatti nel periodo ecc.) possono essere utilizzati per le esigenze di fatturazione, essendo invece obbligatorio cancellare o rendere anonimo al termine della chiamata ogni altro dato personale eventualmente memorizzato. Tale trattamento a fini di fatturazione è consentito, peraltro, «sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento» (art. 4, comma 2).

Allo scopo di garantire maggiormente la tutela della riservatezza degli utenti la normativa impone ai fornitori dei servizi di adottare anche modalità di pagamento alternative alla tradizionale fatturazione, tali da permettere di utilizzare il terminale con altra modalità di pagamento anche anonimo (ad esempio carte di credito, carte telefoniche prepagate ecc.).

Per quanto concerne l'invio della fattura ordinaria, il d.lg. n. 171 prevede invece il diritto di ricevere, gratuitamente e dietro richiesta, l'indicazione dettagliata degli elementi dimostrativi degli oneri addebitati. Però, se ci si avvale di questo servizio, a garanzia soprattutto della riservatezza dei diversi utenti, devono essere mascherate le ultime 3 cifre del numero chiamato. Quest'ultima prescrizione ha tenuto presenti sia le indicazioni provenienti dal confronto in ambito europeo, sia il rapporto fra cifre mascherate e lunghezza totale dei numeri delle utenze telefoniche.

- Identificazione della linea, chiamate di disturbo e indesiderate - Le nuove tecnologie digitali, che permettono l'identificazione immediata sugli apparecchi telefonici della linea chiamante, hanno imposto l'adozione di apposite misure di sicurezza.

Al riguardo, l'art. 6 prevede le diverse ipotesi che permettono agli abbonati e agli utenti di essere informati su tali servizi e di impedire, a seconda dei casi, l'identificazione della linea chiamante o di quella chiamata.

L'art. 7 prevede invece una procedura agevole per permettere di superare la soppressione dell'identificazione della linea chiamante e, nel contempo, di conoscere i dati relativi alla provenienza della chiamata ricevuta, qualora un abbonato si trovi nella condizione di ricevere chiamate di disturbo.

È previsto poi che le chiamate a scopo pubblicitario o per il compimento di ricerche di mercato o di comunicazione commerciale interattiva siano possibili solo con il consenso espresso dell'abbonato, qualora avvengano con l'utilizzo del telefax o mediante un sistema automatizzato di chiamata.

Ulteriori garanzie sono apprestate poi per permettere a ogni abbonato di poter bloccare il trasferimento automatico, verso la propria linea, di chiamate effettuate da parte di terzi (art. 8).

L'art. 10 prevede, invece, alcuni diritti aggiuntivi dell'abbonato in ordine alla compilazione degli elenchi telefonici. In particolare l'abbonato, «gratuitamente e con richiesta documentata per iscritto, ha diritto di non essere incluso negli elenchi, di ottenere che il suo indirizzo sia in parte omesso e, se ciò è fattibile dal punto di vista linguistico, di non essere contraddistinto da un riferimento che ne riveli il sesso».

2.12.1.2 Prime esperienze applicative

Con l'entrata in vigore di questa nuova disciplina sono emersi però alcuni problemi in ordine alla sua corretta applicazione e il Garante è intervenuto per fornire alcuni primi chiarimenti di carattere generale.

Una questione è stata posta in relazione al termine per la conservazione dei dati relativi al traffico telefonico da parte dei gestori dei servizi di telecomunicazione.

Al riguardo, il Garante ha fatto presente che il d.lg. n. 171/1998 ha fissato un termine che in precedenza era imprecisato. Il decreto ha infatti previsto che i dati possano essere trattati e conservati dal fornitore del servizio telefonico «sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento» (v. l'art. 4, comma 2). Tale termine impone un riferimento all'art. 2948 del c.c. ed è, quindi, di cinque anni.

L'Autorità ha inoltre chiarito che entro il medesimo termine l'autorità giudiziaria può certamente acquisire dati in conformità alla legge, per finalità di indagine, proprio come è avvenuto per gravi fatti di criminalità, senza che sia necessario cancellarli una volta acquisiti agli atti d'indagine.

Il Garante ha affrontato poi la questione relativa alla mancata indicazione da parte dei fornitori dei servizi telefonici delle ultime tre cifre delle utenze telefoniche chiamate nella fatturazione dettagliata richiesta dagli abbonati. Diversi cittadini, liberi professionisti, imprenditori, associazioni, enti e altri organismi (pubblici e privati) abbonati al servizio telefonico hanno lamentato che tale misura non permette loro di verificare l'esattezza delle chiamate addebitate nella bolletta.

A seguito delle numerose segnalazioni ricevute, l'Autorità ha deciso di fornire alcuni chiarimenti, segnalando ai gestori del servizio telefonico alcuni opportuni aggiustamenti, con un provvedimento adottato il 5 ottobre 1998.

Nel provvedimento si è confermata la legittimità della misura del «mascheramento» di alcune cifre delle utenze chiamate, introdotta, come già detto, dal d.lg. n. 171 e praticata da tempo in diversi Paesi europei (anche prima dell'adozione della direttiva comunitaria, con l'oscuramento di un numero di cifre da due a quattro: Austria, Danimarca, Finlandia, Francia, Germania e Lussemburgo). Al

tempo stesso, si è però evidenziato che il «mascheramento» non permette di controllare a fondo l'esattezza di alcuni addebiti e può essere quindi «superato» qualora l'abbonato contesti la bolletta ricevuta e abbia l'esigenza di identificare puntualmente le chiamate effettuate, intendendo tutelare i propri diritti in sede giudiziaria.

Dal punto di vista normativo, sia la direttiva comunitaria, sia il d.lg. n. 171/1998 non mettono in discussione il diritto dell'abbonato di controllare l'esattezza degli addebiti e ne ampliano anzi la tutela, ma cercano di conciliare questo diritto con i diritti di altri soggetti la cui sfera privata è coinvolta anch'essa dalla fatturazione dettagliata: ossia di coloro che effettuano chiamate attraverso gli apparecchi collegati alla stessa linea telefonica (ad esempio, nel caso di utenze domestiche, i vari componenti del nucleo familiare o, nell'ipotesi di un'azienda, i dipendenti e i collaboratori), sia, altresì, dei destinatari delle telefonate (abbonati chiamati).

La l. n. 675/1996 non ostacola l'esercizio dei diritti degli abbonati e permette ai fornitori dei servizi telefonici di comunicare all'abbonato anche le cifre «mascherate» nella fattura in caso di contestazioni riguardanti l'esattezza di determinate chiamate addebitate all'abbonato medesimo, che quest'ultimo possa far valere con un'azione legale.

Qualora, quindi, le verifiche effettuate sulla base delle informazioni già riportate nella fattura dettagliata (che, intrecciate tra di loro, permettono già di riscontrare un congruo numero di situazioni, nonostante le cifre «mascherate») non siano sufficienti a fugare eventuali dubbi sull'effettuazione di determinate chiamate, o addirittura inducano a ritenere sicuramente erroneo l'addebito (ad esempio, nell'ipotesi di temporanea assenza del nucleo familiare dalla propria abitazione), l'abbonato può sollecitare un'attenta verifica dei numeri telefonici oggetto di contestazione.

Concretamente, l'abbonato può rivolgersi al gestore telefonico, senza particolari formalità e con una procedura snella, contestando la circostanza che determinate telefonate siano state effettuate dai propri apparecchi; il gestore deve verificare le chiamate «contestate», comunicando all'abbonato se l'addebito, dopo il controllo, resta fondato. Laddove tale riscontro non giunga, o comunque permanga un giustificato e motivato dubbio nell'abbonato, quest'ultimo ha diritto di chiedere e di ottenere gratuitamente dal gestore la comunicazione per intero dei numeri telefonici oggetto di precisa contestazione.

Il Garante ha quindi ritenuto che, in questi limiti, la comunicazione di determinati dati invece «mascherati» nella fattura dettagliata sia pienamente compatibile con i princìpi sanciti dalla l. n. 675/1996, la quale rende ammissibile per il titolare del trattamento (nel caso di specie, il gestore telefonico) la comunicazione dei dati personali, quando tale operazione risulti necessaria per far valere o difendere un proprio diritto in sede giudiziaria (art. 20, comma 1, lett. *g)*).

L'Autorità ha però aggiunto che le nuove tecnologie permettono oggi di bilanciare in maniera più efficace i diritti dell'abbonato con la *privacy* degli utenti e degli altri abbonati. La direttiva 97/66/CE e il d.lg. 171 prevedono infatti la possibilità di ricorrere a misure alternative al «mascheramento».

In particolare, secondo la direttiva, tali misure possono consistere nell'introduzione di possibilità di pagamento «che permettano un accesso anonimo, o rigorosamente privato, ai servizi di telecomunicazione offerti al pubblico, quali carte telefoniche, oppure possibilità di pagamento con carta di credito» (considerando 18 della direttiva 97/66/CE). In tal modo, sia dalle utenze private sia dai luoghi di lavoro, la persona chiamante - che non sempre corrisponde all'abbonato pagante - potrebbe fare un legittimo uso dell'utenza senza far gravare il costo delle chiamate sull'abbonato; tali chiamate, quindi, non sarebbero riportate nel dettaglio di fatturazione. Anche il decreto ha fatto un passo significativo introducendo, appunto, l'obbligo

per i gestori di consentire «che i servizi richiesti e le chiamate effettuate da qualsiasi terminale possano essere pagate con modalità alternative alla fatturazione, anche anonime, quali le carte di pagamento o prepagate» e che, in questo caso, tali servizi e chiamate non debbano comparire nella fatturazione (art. 5, commi 1 e 2).

Sotto questo aspetto, il Garante ha perciò raccomandato ai fornitori dei servizi di telefonia la necessità di dare rapida attuazione al d.lg. n. 171/1998, rendendo effettiva e agevole la possibilità per gli abbonati e gli utenti di avvalersi, in alternativa alla fatturazione dettagliata, di strumenti di pagamento delle chiamate telefoniche che garantiscano l'anonimato.

In relazione invece alle modalità e ai limiti della procedura concernente la contestazione delle fatture telefoniche e la «messa in chiaro» dei numeri relativi alle telefonate «controverse», l'Autorità ha trasmesso il proprio provvedimento, adottato il 5 ottobre 1998, alle competenti amministrazioni, al fine dell'eventuale aggiornamento, alla luce delle nuove disposizioni del d.lg. n. 171, delle norme regolamentari sulle condizioni di abbonamento al servizio telefonico e di eventuali altre disposizioni in materia.

Successivamente è stata avviata un'indagine per verificare il rispetto da parte delle società che gestiscono il servizio telefonico dei princìpi indicati nel predetto provvedimento. Infatti, da segnalazioni pervenute all'Ufficio è emerso che alcuni gestori non avevano adempiuto alle richieste di utenti volte a conoscere nel dettaglio tutte le cifre delle chiamate contestate. Dall'indagine, tuttora in corso, si è potuto appurare che le aziende che forniscono i servizi telefonici intendono senz'altro aderire alle indicazioni fornite dal Garante, ma adducono la necessità di disporre di tre o quattro mesi per il pieno adeguamento dei servizi.

Alcuni chiarimenti sono stati infine forniti dal Garante con riferimento alla possibilità per i competenti ispettorati del Ministero delle comunicazioni di accedere, presso una società che gestisce il servizio di telefonia mobile, ad alcuni documenti contenenti dati relativi ad abbonati e utenti, presi a campione, al fine di verificare la regolare osservanza degli obblighi assunti dal concessionario e la regolarità del servizio.

Al riguardo, l'Autorità ha sottolineato che vi è una complessa serie di norme che hanno attribuito al Ministero ampi poteri di vigilanza e di controllo sull'operato delle società concessionarie dei servizi telefonici (in particolare, quelle che prevedono la disciplina convenzionale del rapporto di concessione), e che la l. n. 675/1996 non ostacola la comunicazione di dati personali al Ministero medesimo. Spetta però a quest'ultimo, da un lato individuare le disposizioni in presenza delle quali è possibile acquisire i dati anche senza che il privato gestore del servizio telefonico raccolga il consenso degli abbonati interessati e, dall'altro, valutare caso per caso la possibilità di svolgere con pari efficacia i compiti a esso affidati anche sulla base, in tutto o in parte, di informazioni anonime.

È stata infine segnalata al gestore l'esigenza che le informative inviate agli abbonati rechino, ove già non previsto, un generale riferimento alle comunicazioni dei loro dati obbligatorie per legge o regolamento.

2.12.2 Video-sorveglianza

L'Italia manca tuttora di una normativa che disciplini specificamente la video-sorveglianza, a differenza di quanto avviene in altri Paesi europei come la Francia, la Danimarca, l'Islanda e la Norvegia. La direttiva comunitaria n. 95/46/CE del 1995 e la convenzione n. 108/1981 del Consiglio d'Europa applicano in modo vincolante la disciplina del trattamento dei dati personali anche ai suoni e alle immagini

(quali sono quelli registrati nei controlli video) nel caso consentano l'identificazione di un soggetto anche in via indiretta (ad es. mediante collegamento con altre informazioni).

La l. 31 dicembre 1996, n. 675 che ha attuato la convenzione n. 108 e ha recepito la direttiva europea, considera come «dato personale» qualunque informazione che consenta l'identificazione dei soggetti interessati sebbene derivante da suoni e da immagini anziché da dati alfanumerici. Tale legge è quindi senz'altro applicabile ai trattamenti di suoni e di immagini effettuati attraverso sistemi di video-sorveglianza. Anche in caso di non chiara e univoca identificazione dei soggetti inquadrati da telecamere (possono creare a ciò un ostacolo la distanza, l'ampiezza dell'angolo visuale, la qualità degli strumenti, ecc.), va ritenuta sufficiente la possibilità di identificazione attraverso l'interconnessione con documenti di archivio e banche dati di immagini in possesso di altre autorità quali quelle di polizia.

Nell'ambito della sua attività il Garante ha perciò sollecitato il rispetto di alcune specifiche prescrizioni della l. 31 dicembre 1996, n. 675.

In risposta, ad esempio, ai quesiti di alcuni comuni in ordine alla legittimità di taluni progetti relativi all'installazione di telecamere in luoghi pubblici (nella specie, in un parco e in zone deturpate con maggiore frequenza da atti di vandalismo), il Garante ha richiamato l'attenzione su taluni aspetti che devono essere tenuti presenti ogni qualvolta si prospetti l'esigenza di installare sistemi di video-sorveglianza:

a) verificare la legittimità e le finalità dell'iniziativa, controllando anche se la stessa corrisponda alle funzioni istituzionali demandate all'ente pubblico;

b) controllare l'idoneità delle misure che possono essere adottate per assicurare un uso corretto dei dati da parte dei soggetti legittimati (art. 15);

c) vigilare sulle modalità di registrazione iniziale dei dati e della loro conservazione, anche al fine di assicurare la loro pertinenza e non eccedenza rispetto agli scopi perseguiti (art. 9, comma 1, lettera *d)*);

d) definire le procedure e le modalità volte a fornire agli interessati le informazioni previste (art. 10).

In questo quadro il Garante ha manifestato perplessità dinanzi alla prospettiva dell'attivazione di un sistema di video-sorveglianza privo di un insieme articolato di garanzie, che dovrebbero riguardare, in modo particolare, l'eventuale intenzione di conservare le immagini in un apposito archivio, l'individuazione dei soggetti legittimati ad accedere alle registrazioni anche all'interno dell'ente e l'eventuale messa a disposizione delle registrazioni in favore di altri soggetti pubblici.

Fornendo riscontro a una richiesta di parere in ordine alla compatibilità con la l. 31 dicembre 1996, n. 675 del progetto di installazione di apparecchiature di video-sorveglianza presso il pronto soccorso di una azienda ospedaliera, il Garante ha sottolineato come i dati personali che rilevavano nel caso in specie fossero in massima parte dati sensibili, poiché le telecamere da installare riprendevano essenzialmente immagini di persone ammalate.

Il trattamento di dati sensibili da parte di un'azienda ospedaliera è apparso connesso all'assistenza e alla cura dei pazienti ricoverati che rientrano nelle finalità istituzionali proprie degli organismi sanitari pubblici.

Tale generale compito di assistenza, infatti, si specificava in un'attenzione continua ai ricoverati in rianimazione e in un doveroso controllo di sicurezza all'interno del pronto soccorso. Si trattava, quindi, di operazioni condotte da sempre con modalità tradizionali, che verranno ora svolte con l'ausilio di sistemi di video-sorveglianza. Il combinato disposto degli artt. 22, comma 3 e 41, comma 5 della l. n. 675/1996 ha legittimato quindi l'azienda ospedaliera a installare le telecamere e a trattare i relativi dati sensibili. Peraltro, l'installazione del sistema di video-sorve-

glianza ha richiesto che fossero osservate alcune prescrizioni poste dalla l. n. 675/1996. Prima di attivare le apparecchiature di ripresa, la direzione dell'azienda ospedaliera dovrà infatti opportunamente regolamentare i seguenti profili:

a) determinare con precisione la localizzazione delle telecamere e le modalità di ripresa, in aderenza alle finalità che hanno suggerito l'installazione del sistema di video-sorveglianza e nel rispetto dei princìpi fondamentali fissati dall'art. 9 della legge, specie in ordine alla pertinenza e non eccedenza dei dati rispetto agli scopi perseguiti;

b) definire puntualmente i soggetti legittimati a trattare i dati personali in oggetto, individuando eventualmente un soggetto responsabile, ai sensi dell'art. 8 della legge, del sistema di video-sorveglianza nonché gli incaricati del trattamento (personale infermieristico, addetti alla vigilanza, ecc.);

c) stabilire idonee misure di sicurezza ai sensi dell'art. 15 della legge, al fine di assicurare un corretto uso dei dati, evitando il rischio che gli stessi possano entrare nella disponibilità di persone estranee alla struttura o comunque non autorizzate. Si è sollecitata pertanto una particolare attenzione alle modalità di accesso alle riprese video da parte dei familiari dei ricoverati in rianimazione, ai quali andrà consentita, nella misura tecnicamente possibile, la visione delle sole immagini del loro congiunto;

d) fissare parametri precisi per quanto riguarda l'eventuale necessità di conservazione delle immagini registrate, secondo il dettato dell'art. 9, comma 1, lettera *e)* della legge che prescrive la conservazione dei dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;

e) prevedere forme e modalità volte a fornire agli interessati le informazioni previste dall'art. 10 della legge.

Si segnala infine che il Garante segue con attenzione l'attività del Comitato di sorveglianza del programma operativo «Sicurezza per lo sviluppo del Mezzogiorno d'Italia». Nel programma riveste una importanza particolare il progetto relativo al rafforzamento della sicurezza sull'asse autostradale Caserta-Salerno-Reggio Calabria, che prevede l'utilizzo di moderne tecnologie video e audio per il controllo del territorio.

Considerata anche la vastità del territorio oggetto del controllo, è apparso necessario acquisire maggiori elementi sulle finalità di tale sistema di controllo e sulla sua base normativa, per verificare se i trattamenti in questione rientrino fra quelli indicati dall'art. 4 della legge, oppure siano ricompresi tra quelli ai quali la legge si applica senza eccezioni. Il Garante ha chiesto quindi notizie più dettagliate circa:

a) la modalità con la quale verranno gestite le immagini riprese (memorizzazione, conservazione, angolo visuale delle telecamere e limite della possibilità di avvicinamento dell'immagine);

b) le modalità con le quali verranno effettuate eventuali rilevazioni di tipo acustico, appurando, in particolare, se esse si sostanzino in un controllo fonico di ciò che si svolge all'interno delle aree di servizio ovvero si limitino al raggio di azione delle telecamere, e quale sia inoltre il livello di percezione dei suoni;

c) i meccanismi che si intendono predisporre per fornire un'adeguata informazione agli interessati;

d) le misure di sicurezza adottate, considerato che le immagini saranno trasmesse dalle telecamere ai centri operativi attraverso il sistema di comunicazione satellitare.

Il Ministero dell'interno ha già fornito le notizie richieste e gli approfondimenti in atto sono in via di definzione.

Allo scopo di avere un quadro dettagliato e capillare del fenomeno, il Garante ha deciso infine di affidare una ricerca sulle diverse forme di video-sorveglianza utilizzate sempre più intensivamente a scopi di sicurezza sociale in luoghi pubblici, esercizi commerciali, supermercati, banche, ecc. La decisione è stata presa in attesa della complessiva regolamentazione della materia attraverso uno dei decreti che il Governo è stato delegato a emanare (in base all'art. 1, comma 1, lettera *i)* della l. n. 676/1996) e che dovrà fissare le norme per il giusto equilibrio tra il diritto alla riservatezza dei cittadini e le esigenze di pubblica sicurezza e della prevenzione dei reati. La non procrastinabilità di una normativa in materia di video-sorveglianza è peraltro implicitamente evidenziata dal fatto che l'art. 11 della l. n. 449/1997 («collegato» alla finanziaria 1998) prevede per le aziende commerciali e turistiche la possibilità di beneficiare di crediti d'imposta per l'acquisto di sistemi di sicurezza, incluse le telecamere a circuito chiuso.

È da segnalare, peraltro, che se in Italia l'installazione di telecamere in funzione di deterrenza anticrimine o di accertamento di violazioni al codice della strada è stata all'ordine del giorno in varie occasioni, il 1998, all'estero, ha segnato un vero e proprio salto di qualità.

L'efficacia raggiunta dai sistemi elettronici di controllo alimenta paure talvolta irrazionali, ma è anche vero che nella società contemporanea l'equilibrio tra libertà e sicurezza tende a essere risolto, in proposito, trascurando i diritti di libertà.

Alcuni episodi indicati qui a titolo meramente esemplificativo possono risultare utili.

Nel mese di ottobre il comune di Newham (Londra) ha avviato un piano di modernizzazione della rete già esistente di 140 telecamere fisse e 11 mobili. L'intero apparato di video-sorveglianza è stato dotato di un sistema elettronico di riconoscimento visuale collegato a un archivio biometrico: il software, denominato «*Mandrake*», è all'avanguardia nei sistemi di scannerizzazione e si basa su algoritmi di reti neurali (i sistemi di apprendimento sviluppati nel settore dell'intelligenza artificiale). Quando un soggetto entra nel campo visivo della telecamera, il fotogramma del viso viene isolato da un cerchio rosso ed esaminato dal computer. Se il computer riconosce l'immagine nella banca dati suona l'allarme e la polizia (che collega all'introduzione del circuito di controllo video una diminuzione significativa dei reati) viene allertata su una linea speciale.

Sistemi analoghi sono in uso al confine tra USA e Messico (al riguardo si è parlato della costruzione di una nuova «Cortina di silicio» dopo il crollo della «Cortina di ferro» in Europa) e vengono sperimentati negli aeroporti. La novità è costituita dalla potenza del software: «*Mandrake*» è in grado infatti di scannerizzare più visi contemporaneamente, a differenza di altri prodotti informatici in grado di analizzare l'identità di una sola persona per volta.

Al perfezionamento tecnologico degli apparati di sorveglianza corrisponde però una mobilitazione delle associazioni per la difesa dei diritti civili. A New York la NYCLU (affiliata della ACLU, l'American Civil Liberties Union) ha organizzato un censimento delle telecamere funzionanti nelle strade di Manhattan. Nel mese di dicembre sono stati presentati alla stampa i risultati del lavoro: il NYC Surveillance Camera Project ha prodotto una mappa di 2397 telecamere (2117 private e 270 di organismi pubblici) distribuite in 12 zone. La mappa non ha la pretesa di essere esaustiva poiché molte telecamere sono mimetizzate, ma i risultati sono stati sufficienti a definire la grande metropoli statunitense «a surveillance camera town» (comunicato stampa della NYCLU del 13 dicembre 1998).

2.12.3 Commercio elettronico

Il commercio elettronico non rappresenta un fenomeno del tutto nuovo, poiché per molti anni le imprese si sono scambiate dati commerciali usando diverse reti di comunicazione. Dal momento in cui Internet ha iniziato il suo *trend* di maggiore sviluppo, oramai considerato esponenziale anche dagli osservatori più cauti, il commercio elettronico non è più limitato alle grandi aziende, ma si apre a chiunque nel mondo.

Internet somiglia sempre più a un'enorme e infinita fiera commerciale con innumerevoli servizi diffusi in tutto il mondo, accessibili attraverso il *World Wide Web* (WWW). Anche in Italia la crescita del commercio elettronico, soprattutto per quanto riguarda i rapporti fra imprese e consumatori, sarà superiore, a detta degli osservatori, alla crescita media del complessivo volume di affari. Oltre a creare nuove forme di attività, il commercio elettronico influirà profondamente sul modo di condurre gli affari e avrà forti ripercussioni sulla sfera della vita privata degli utenti delle reti e dei consumatori. Di qui l'esigenza di un approccio attento ai diritti della personalità e, al tempo stesso, ben modulato, in modo da non pregiudicare l'uso della telematica per facilitare acquisti e relazioni commerciali via Internet.

Si moltiplicano, al riguardo, le iniziative di riflessione dalle quali emergono, giorno dopo giorno, nuovi temi da approfondire (correttezza e trasparenza delle relazioni con l'utente; consapevolezza da parte dell'utente degli effetti dei suoi comportamenti in rete; presenza ed efficacia di informazioni sintetiche, ma irrinunciabili da fornire agli utenti; distinzione dei trattamenti di dati legati al rapporto commerciale da quelli effettuati per marketing, ricerche di mercato e studi su utenti; sicurezza delle transazioni; diritto all'anonimato).

La delicatezza delle scelte da effettuare emerge anche dalla complessità delle relazioni che si intrecciano a margine delle transazioni elettroniche. Il numero dei soggetti partecipanti moltiplica poi il novero dei trattamenti, alcuni dei quali non vengono individuati in quanto tali dall'utente, ovvero dal *cliente*.

Oltre ai due soggetti più direttamente interessati alla transazione commerciale elettronica, il cliente e il venditore - quest'ultimo nel senso più ampio del termine, che può indicare anche un'amministrazione o un sito *Web* che fornisca informazioni o pubblicità senza concludere una transazione commerciale - occorre infatti identificare anche altri soggetti interessati anch'essi, in qualche modo, dal negozio elettronico. Ci si riferisce, in particolare :

– al *fornitore di accesso Internet* (*Internet access provider*), che fornisce agli utenti l'infrastruttura tecnica di rete necessaria per accedere a Internet;

– al *vettore*, ossia all'organismo di telecomunicazioni che fornisce la rete di base per il trasferimento dei dati;

– al *fornitore di servizio Internet* (*Internet service provider*), che fornisce servizi per la memorizzazione, la trasmissione e la presentazione dei contenuti;

– ai *siti Web* che offrono *motori di ricerca*, sempre più diffusi data l'enorme mole di informazioni disponibile in Rete. Questi siti comportano un duplice rischio: da un lato hanno la possibilità di raccogliere dati su un determinato individuo ricavandoli da più siti, potendone così ricavare un profilo di personalità; in secondo luogo, i fornitori di questi motori di ricerca possono elaborare un profilo dettagliato degli interessi manifestati dai propri utenti;

– alle *banche* e/o alle *istituzioni finanziarie*, che intervengono nelle transazioni commerciali elettroniche.

Uno stesso soggetto può infine offrire servizi diversi in ambiente Internet, direttamente o attraverso soggetti controllati. Ne deriva che sarà difficile individuare i legami e i flussi esistenti fra soggetti che appartengono a uno stesso consorzio/gruppo e fra le funzioni esercitate da uno stesso soggetto.

Da questo quadro sintetico appare chiaro che una delle prime esigenze che si pone è quella di creare per gli utenti un clima di fiducia e di sicurezza circa la liceità, la trasparenza e la correttezza del trattamento dei dati personali nel commercio elettronico. A tale scopo è necessaria una strategia integrata che deve saper coniugare nel loro giusto ruolo un nocciolo «duro» di regole normative con altre norme nascenti «dal basso» attraverso efficaci codici di deontologia e di buona condotta, tecnologie pulite in grado di selezionare l'uso di dati personali specie per piccoli acquisti effettuabili su base anonima, ed eventuali meccanismi di classificazione di siti in base alle garanzie offerte agli utenti, basati su criteri obiettivi e accettati di certificazione.

In altre parole, l'impiego diffuso delle nuove tecnologie dell'informazione e della comunicazione, che rappresenta la caratteristica primaria del commercio elettronico, induce a pensare all'eventualità di un approccio diverso rispetto alla realizzazione dei più comuni strumenti normativi.

Viene soprattutto in rilievo il dato strutturale della rete transnazionale, secondo il quale la diffusione e la circolazione delle informazioni a livello planetario comportano sia una minore possibilità di controllo dei percorsi seguiti (quindi un maggiore rischio di intrusione nella vita privata degli individui che accedono alla rete), sia un problema di individuazione della normativa di tutela di volta in volta applicabile secondo le diverse aree geografiche. Infatti l'organizzazione e gli effetti delle informazioni e dei dati in transito su reti aperte coinvolgono tre livelli: la disciplina internazionale, quella comunitaria e quella degli ordinamenti interni. Tali caratteristiche mettono in luce come i rischi di violazione della riservatezza siano tutt'altro che remoti.

A nuovi rischi devono perciò corrispondere nuovi princìpi e nuovi concetti, al fine di assicurare nei modi opportuni la tutela dei dati di ciascun soggetto.

Lo stesso Consiglio di Stato francese, in un suo documento su Internet e le reti numeriche (2 luglio 1998), evidenzia come «le reti numeriche transfrontaliere inducono una modificazione sostanziale dei modi di regolazione abituale dei sistemi giuridici. Da una parte la regolamentazione di origine statale deve ormai combinarsi con l'autoregolazione dei protagonisti, degli attori, dei servizi comunicativi; d'altra parte, tenuto conto dei limiti inerenti a ogni iniziativa puramente nazionale, spetta alla cooperazione internazionale fra gli Stati far rispettare gli interessi pubblici in uno spazio largamente dominato dall'iniziativa privata. In altri termini, le reti introducono una doppia interdipendenza, tra attori pubblici e privati nell'ambito degli Stati medesimi».

La rapidità dello sviluppo tecnologico da una parte, e l'inevitabile lentezza del processo legislativo dall'altra, rischiano di rendere rapidamente obsoleto un impianto normativo teso a regolamentare in maniera «classica» l'ambiente Internet e le applicazioni che esso consente, fra cui il commercio elettronico.

Non a caso alcune esperienze come quella olandese, ruotano attorno a una normativa a tempo «determinato». La stessa recente legge tedesca (Legge sulla informazione e la comunicazione - IUK Dg 13-6-97, art. 2 (4)) sceglie di individuare e fissare quattro princìpi di tipo generale, idonei ad adattarsi all'innovazione tecnologica.

Il primo è quello della «minimizzazione dei dati» (il titolare deve sottoporre a trattamento il minimo di dati necessario per assicurare il corretto svolgimento del trattamento stesso).

Il secondo è il diritto all'anonimato (riconosciuto anche in altri contesti come quello della firma elettronica; collegato a esso il diritto a utilizzare uno pseudonimo).

Il terzo riguarda la cd. «integrazione delle funzionalità tecnologiche» al fine di dare attuazione ai princìpi di protezione dei dati (esso implica che ogniqualvolta le tecnologie utilizzate per la raccolta o il trattamento dei dati possano essere considerate anche uno strumento per attuare o potenziare i princìpi di protezione dei dati, queste stesse tecnologie debbono essere configurate in modo conforme a tale principio).

Il quarto principio è quello della «realizzazione elettronica dello *status* giuridico dell'interessato» (il che comporta la necessità di garantire la trasparenza e la realizzazione, attraverso tecniche on-line, dei vari diritti degli utenti *Web*, anche attraverso l'intervento tempestivo delle autorità nazionali incaricate della protezione dei dati).

Le innumerevoli possibilità tecniche offerte dalle reti aperte del sistema comunicativo mettono però a dura prova le tradizionali strutture giuridiche in numerosi contesti, riguardanti soprattutto la protezione dei diritti fondamentali della persona. Sorge perciò l'impegno per i molteplici organismi regolatori, sia di diritto interno sia di diritto internazionale, di comporre il quadro delle regole. Di qui la necessità, largamente condivisa a livello comunitario, che le attività condotte su Internet non possano essere svincolate dai princìpi giuridici fondamentali che valgono *off-line* o per altri settori. E se da un lato bisogna accordare piena tutela ai diritti fondamentali, dall'altro anche nel cd. *cyberspazio* deve valere la regola che ogni eventuale limitazione dei diritti e delle libertà fondamentali deve essere adeguatamente giustificata, necessaria e proporzionata anche alla luce delle garanzie previste dalla Convenzione europea dei diritti dell'uomo e delle libertà fondamentali.

Circa la posizione italiana, il nostro Paese, in coerenza con gli orientamenti delle istituzioni europee e in particolare con gli enunciati della Conferenza europea del luglio 1997 a Bonn, ravvisa l'esigenza di costruire una normativa adeguata a un duplice livello, di cui il primo nel quadro delle fonti sovranazionali (v. anche § 4.2.3 per quanto riguarda la proposta di direttiva sul commercio elettronico) e il secondo nell'ambito del diritto nazionale.

E se preminente è la via dell'intervento normativo, non è però da trascurare la prospettiva di una valorizzazione più ampia dei codici di autodisciplina, in quanto il policentrismo delle fonti di regolazione, purché dotate di concreta efficacia, può svolgere anche qui un importante ruolo integrativo. In tal senso va ricordato nuovamente come la l. 31 dicembre 1996, n. 675, preveda esplicitamente tali codici e riconosca loro questa funzione: non tanto, quindi, una rinuncia a legiferare, quanto piuttosto il tentativo di sperimentare modi e sedi di produzione di regole più vicini alla realtà da disciplinare e perciò, forse, più efficaci.

Va ricordato che di recente il nostro legislatore, recependo la direttiva n. 97/66/CE, ha emanato il d.lg. 13 maggio 1998, n. 171, recante disposizioni di tutela della vita privata nel settore delle telecomunicazioni (*v. § 2.12.1*). Il Governo sarà inoltre impegnato a dare attuazione alla delega prevista dalla l. 31 dicembre 1996, n. 676, che all'art. 1, comma 1, lett. *n)* prevede di «stabilire le modalità applicative della legislazione in materia di protezione dei dati personali ai servizi di comunicazione e di informazione offerti per via telematica, individuando i titolari del trattamento di dati inerenti ai servizi accessibili al pubblico e la corrispondenza privata, nonché i compiti del gestore anche in rapporto alle connessioni con reti sviluppate su base internazionale».

La fiducia del cittadino rappresenta sicuramente un elemento chiave per lo sviluppo del commercio elettronico (rilevante per lo sviluppo del sistema economico del Paese) e il pieno rispetto del diritto alla riservatezza e all'identità personale ne costituisce una componente essenziale.

Strettamente connesse al tema sono anche la certezza delle transazioni, garantite da organismi di categoria (infrastrutture bancarie per la componente moneta elettronica e infrastrutture delle imprese o del commercio o dei servizi pubblici e privati per la componente qualità e fedeltà dei servizi e prodotti offerti), la sicurezza contro ogni violazione concernente le informazioni protette o gli strumenti di pagamento, nonché la sobrietà e selettività nel trattamento dei dati personali da parte degli erogatori di servizi.

Va sottolineata poi l'importanza delle tecnologie che garantiscono strumenti sicuri di pagamento elettronico. Per la tutela della riservatezza è necessario esaminare la possibilità che i pagamenti via Internet, per l'acquisto di determinati beni e per le cd. «piccole spese», siano effettuati in modo anonimo (vale a dire senza registrare l'identità di chi ha effettuato il pagamento) e sviluppare sistemi di pagamento elettronico con carte prepagate.

Infine, un *vademecum* esplicativo dei rischi per la riservatezza degli utenti, dei diritti degli utenti *Web* e degli obblighi in materia di protezione dei dati personali che incombono al titolare di un sito nel quale possono essere effettuate transazioni commerciali dovrebbe ricevere la massima diffusione mediante la rete Internet. L'Autorità di protezione dei dati sarà presto presente con un proprio sito *Web* documentato e aggiornato al fine di poter esercitare, anche in questo ambito, i propri fini istituzionali.

2.13 Flussi transfrontalieri di dati

2.13.1 Profili generali

Con l'approvazione della direttiva comunitaria 95/46 CE, il cui termine per il recepimento è scaduto il 24 ottobre scorso, l'Unione europea ha introdotto un quadro di riferimento comune per la protezione dei dati personali destinato a tutti gli Stati membri, in modo da determinare discipline convergenti e omogenee e impedire, così, che situazioni di scarsa protezione in taluni contesti nazionali possano indurre altri Stati a restringere o vietare il flusso e la circolazione dei dati.

Come è noto tale normativa comunitaria è stata recepita in buona parte nella l. 31 dicembre 1996, n. 675, all'art. 28. Da tale quadro discende una situazione che garantisce la circolazione delle informazioni all'interno dell'Unione europea e la possibilità di esportare dati verso quei Paesi terzi che assicurino un livello di protezione «adeguato», anche se non necessariamente equivalente.

Il requisito dell'adeguatezza costituisce il fulcro del dibattito in atto a livello internazionale sul trasferimento dei dati all'estero.

Il meccanismo di valutazione dell'«adeguatezza», infatti, è complesso ed è disciplinato agli artt. 25 e 26 della direttiva, che attribuiscono il giudizio, in primo luogo, alle autorità di garanzia nazionali che cooperano attivamente tra loro, nonché ai giudici nazionali che siano eventualmente investiti del caso.