necessarie per giungere ad una ipotesi di soluzione del negoziato aperto con gli Stati Uniti per definire le modalità attraverso le quali può essere consentito un trasferimento di dati personali verso o da quel Paese

Oltre a tale negoziato (di cui si è fatto cenno nel par. 2.12) per il quale è intervenuto ben cinque volte nel corso dell'anno con l'adozione di pareri e per definire i metodi di lavoro, il Gruppo ha espresso la sua opinione sul livello di protezione dei dati personali in Svizzera ed in Ungheria, (rispettivamente, con i pareri 5/99 doc. WP 22, approvato il 7 giugno 1999, e 6/99 doc. WP 24 approvato il 7 settembre 1999).

Il Gruppo è inoltre intervenuto, adottando specifiche raccomandazioni, su i seguenti profili:

- Trattamento invisibile ed automatico dei dati personali su Internet (Raccomandazione 1/99, doc. WP, 17 adottata il 23 febbraio 1999);
- Rispetto della vita privata nel contesto dell'intercettazione di telecomunicazioni (Raccomandazione 2/99, doc. WP 18, adottata il 3 maggio 1999);
- Conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari (Raccomandazione 3/99, doc. WP 25, adottata il 7 settembre 1999), nonché, in relazione ai lavori che si svolgono per pervenire alla definizione di una Carta europea dei diritti fondamentali, con la Raccomandazione n. 4/99 dedicata a:
- L'inclusione del diritto fondamentale alla protezione dei dati personali nella Carta europea dei diritti fondamentali (doc WP 26, approvato il 7 settembre 1999).

I documenti elaborati dal Gruppo con riferimento al negoziato con gli Stati Uniti, tuttora in corso, sono i seguenti:

- Parere 1/99 sul livello di protezione dei dati personali negli Stati Uniti (doc. WP 15, adottato il 26 gennaio 1999);
- Parere 2/99 riguardante l'adeguatezza dei "principi internazionali per un approdo sicuro" stabiliti dal Ministero del commercio USA il 19 aprile 1999 (doc. WP 19, del 3 maggio 1999);
- Parere 4/99 riguardante le FAQ (domande poste frequentemente) che saranno pubblicate dal Ministero del commercio USA in relazione ai principi "Approdo sicuro" (Safe Harbor) proposti (doc. WP 21 del 7 giugno 1999);
- Documento di lavoro sullo stato attuale delle discussioni in corso tra la Commissione europea e il Governo degli Stati uniti in merito ai principi internazionali dell'"Approdo sicuro" (Safe Harbor) (doc. WP 23 del 7 luglio 1999);
- Parere 7/99 riguardante il livello di tutela dei dati offerto dai principi dell'"Approdo sicuro" (Safe Harbor) pubblicati con le FAQ ed altri documenti in materia dal Ministero del commercio USA il 15 e 16 novembre 1999) (doc. WP 27 del 3 dicembre 1999).

Anche i lavori del Comitato dell'articolo 31 sono stati largamente influenzati dall'importanza del negoziato in corso, tanto che i componenti del Comitato e la Commissione hanno effettuato un viaggio ufficiale negli Stati uniti cui ha preso parte il segretario generale del Garante.

In relazione al più generale tema dell'attuazione di principi della direttiva 95/46/CE, è da segnalare che il termine fissato dalla stessa per il recepimento è, com'è noto, scaduto il 24 ottobre 1998. Analogamente è scaduto il termine per il recepimento della direttiva 97/66/CE. Non tutti i Paesi hanno completato la trasposizione dei principi contenuti in una od entrambe le direttive, tanto che la Commissione ha deciso di aprire la procedura di infrazione per inadempimento nei confronti di Francia, Germania, Irlanda, Lussemburgo, Danimarca e Paesi Bassi. riguardo alla direttiva 95/46/CE.

5.3 Cenni comparativi sul recepimento delle direttive 95/46 CE e 97/66/CE

Nel corso del 1999, tre Stati membri dell'Unione hanno introdotto disposizioni di legge di recepimento della direttiva 95/46/CE: si tratta della Finlandia (legge sui dati personali n. 523/1999, entrata in vigore il 1 giugno 1999), dell'Austria (legge sulla protezione dei dati 2000, entrata in vigore il 1 gennaio 2000) e della Spagna (legge organica n. 15/99 sulla protezione dei dati, entrata in vigore il 14 gennaio 2000). Essi si aggiungono dunque alla Grecia, all'Italia, al Belgio, alla Svezia, al Regno Unito ed al Portogallo, che avevano recepito già la direttiva nei rispettivi ordinamenti (vedi Relazione annuale del Garante per il 1998; una tavola sinottica dello stato di recepimento della direttiva 95/46 e della 97/66, è disponibile in calce al presente capitolo).

Per quanto riguarda le disposizioni specifiche, occorre dire che nei tre Paesi era già in vigore una legge in materia di protezione dei dati; per il recepimento della direttiva si è però preferito emanare un testo del tutto nuovo anziché introdurre emendamenti alla legislazione precedente. La *Ley Organica* spagnola, ad esempio, era in vigore dal 1992 e il governo ha deciso, dopo un travagliato *iter* parlamentare, di riscriverne completamente il testo alla luce dei principi della direttiva 95/46/CE. Questi ultimi hanno dunque trovato pieno recepimento, anche se con alcune importanti differenze. In particolare, la legge spagnola – che si applica a tutti i trattamenti di dati personali, sia automatizzati, sia di tipo manuale – prevede un obbligo generale di notificazione dei trattamenti (v. art. 18 della direttiva) indipendentemente dalla natura dei dati oggetto di trattamento; non vi sono in pratica eccezioni all'obbligo di notificare il trattamento – neppure per quanto riguarda i trattamenti effettuati nell'ambito della professione giornalistica (sul contenuto specifico della notificazione la legge rimanda a disposizioni regolamentari ancora da emanare; la notificazione dovrà contenere almeno l'indicazione del responsabile, le finalità del trattamento, il luogo di conservazione, la tipologia dei dati personali, le misure di sicurezza, i trasferimenti previsti di dati a terzi). Per quanto riguarda il diritto di accesso, rettifica e cancellazione, la legge prevede che esso sia sempre esercitabile in forma gratuita (va detto che l'art. 15 della Ley prescrive che l'accesso non sia esercitabile a intervalli inferiori a 12 mesi – contro i 90 giorni nella legge italiana -, "salvo che l'interessato dimostri un interesse legittimo in materia"); nel caso di dati raccolti presso terzi, il titolare deve informare l'interessato dell'avvenuta registrazione dei suoi dati entro i tre mesi successivi. Va inoltre sottolineato l'obbligo di ottenere sempre il consenso per iscritto in rapporto al trattamento di dati di natura sensibile. Inoltre, la legge prevede in via generale il divieto di trasferire dati personali verso Paesi terzi che non garantiscono "un livello di protezione paragonabile a quello sancito dalla presente legge", salvo l'ottenimento di una previa "autorizzazione" da parte del direttore della Agencia de Protección de Datos; le eccezioni contemplate a tale disposizione sono sostanzialmente analoghe a quelle previste dalla legge italiana.

È interessante osservare che la legge spagnola prevede poi una serie di disposizioni in materia di trattamenti per scopi pubblicitari e di indagine commerciale, in base alle quali i cittadini possono chiedere di essere esclusi da un "registro pubblicitario" che abilita le varie ditte che operano nel settore pubblicitario e del marketing all'invio di materiale pubblicitario o promozionale; la richiesta di esclusione ha effetto immediato. L'articolo 32 della legge promuove, infine, la redazione di codici-modello di natura deontologica per quanto riguarda i trattamenti di dati personali nel settore privato; i codici dovranno essere depositati presso il Registro generale della protezione dei dati e potranno essere rifiutati se, a giudizio del direttore della APD, non risultano conformi alle disposizioni di legge e di regolamento in materia.

In Austria, la nuova legge sulla protezione dei dati è stata promulgata dal Parlamento il 17 agosto del 1999 ed è entrata in vigore, come già indicato, il 1 gennaio del 2000 (Datenschutzgesetz 2000). Si tratta di un testo che ha cercato di conciliare le disposizioni precedentemente in vigore (fissate nella Legge n. 565 del 1978) con i principi sanciti dalla direttiva 95/46/CE; la ricerca di tale

obiettivo ha comportato il "sacrificio" di alcuni principi, o ha condotto ad un'interpretazione restrittiva (anche in rapporto alla legislazione italiana).

In primo luogo va detto che l'articolo 4 della legge fornisce alcune definizioni che non corrispondono perfettamente a quelle della direttiva: si parla infatti non di "trattamento" di dati personali, ma di "impiego" di dati (con ciò intendendo "l'insieme delle operazioni logicamente interconnesse nella loro successione e preordinate al raggiungimento di un risultato specifico (...) effettuate in tutto o in parte con l'ausilio di mezzi automatizzati".) In pratica la legge austriaca (leggendo tale articolo insieme all'articolo 2, comma 1: "L'attività legiferativa in materia di tutela dei dati personali nei flussi di dati automatizzati è di competenza dello Stato federale") riserva ai Länder (i singoli Stati che compongono la federazione austriaca) l'emanazione di norme specifiche in materia di trattamento di dati personali con l'ausilio di strumenti non automatizzati, salvo per le materie in cui la competenza è assegnata per legge allo Stato federale (v. art. 2, comma 2 della Legge). Viene inoltre introdotta la distinzione fra "dati personali" e "dati solo indirettamente personali" – questi ultimi corrispondendo ai dati per i quali il titolare ("committente del trattamento", secondo la definizione di legge) o il destinatario "non sono in grado di determinare l'identità dell'interessato attraverso strumenti giuridicamente leciti".

Per quanto riguarda i diritti fondamentali degli interessati (accesso, informazione, rettifica, opposizione), va sottolineato che la legge impone al titolare l'obbligo di comunicare all'interessato soltanto le finalità dell'impiego" dei dati e le generalità del titolare - senza imporre anche l'obbligo di informativa sugli eventuali destinatari della comunicazione dei dati o sull'esistenza di un diritto di accesso ai dati. Queste informazioni sono ottenibili dall'interessato soltanto previa presentazione di una richiesta per iscritto (o anche verbalmente, se il titolare è d'accordo) (art. 26), e dietro versamento di una somma pari a 260 scellini (a meno che si tratti della prima richiesta presentata nel corso dell'anno o la richiesta riguardi i dati "attualmente" oggetto di trattamento), salva l'esistenza di "interessi pubblici prevalenti" (difesa nazionale, interessi di politica estera, economici o finanziari della Repubblica austriaca, prevenzione o repressione di reati, attività dell'esercito federale austriaco); il titolare ha otto settimane di tempo per fornire i dati richiesti. Da notare che i diritti degli interessati non sono esercitabili in rapporto ai dati che la legge definisce "solo indirettamente personali" (art. 27).

Mentre le disposizioni in materia di notificazione dei trattamenti sono analoghe a quelle previste dalla direttiva (e dalla legge italiana), e contemplano una serie di eccezioni fra cui, in particolare, i trattamenti per scopi di natura pubblicistica (v. infra), vi sono alcune specificità per quanto concerne i rimedi giuridici di cui gli interessati dispongono. La legge austriaca prevede la possibilità per "chiunque" (art. 30) di segnalare alla Commissione per la protezione dei dati presunte violazioni dei propri diritti o degli obblighi che la legge impone ai titolari; tuttavia, la Commissione è competente a conoscere soltanto i ricorsi presentati contro titolari del settore pubblico per presunte violazioni del diritto degli interessati alla riservatezza, alla correzione o alla cancellazione dei dati (art. 31). Per quanto riguarda le presunte violazioni commesse da titolari del settore privato, i diritti degli interessati devono essere fatti valere per via giudiziaria; la Commissione eventualmente può costituirsi in giudizio con l'interessato, su sua esplicita richiesta (art. 32). Inoltre, è previsto un risarcimento del danno da parte del titolare soltanto in caso di comportamento negligente da parte di quest'ultimo.

Va infine rilevato che la legge austriaca prevede alcune eccezioni per le attività di natura pubblicistica (che non sono soggette all'obbligo di notificazione, né di informativa) (art. 48), e che per quanto concerne le "decisioni individuali automatizzate" l'opposizione dell'interessato a tale tipo di trattamenti non può essere fatta valere se la decisione "derivante in via esclusiva da trattamenti automatizzati è prevista espressamente per legge" – anche se l'interessato ha comunque il diritto di conoscere la "logica alla base della decisione automatizzata, in una forma comunemente comprensibile" (art. 49).

Anche il testo di legge licenziato dal Parlamento finlandese nel marzo del 1999 (legge sulla

protezione dei dati n. 523/1999) ha sostituito la legge precedentemente in vigore (n. 471/1987) modificandone l'impianto. La nuova legge ha recepito nella sostanza i principi fondamentali della direttiva, ad iniziare dalle definizioni (art. 3) che sono modellate su quelle della direttiva (anche se manca la definizione di "responsabile" del trattamento, cui si fa riferimento in via indiretta nella definizione di "terzi": "(soggetti) diversi dall'interessato, il titolare, il responsabile del trattamento di dati personali o chiunque tratti dati personali per conto del titolare o del responsabile") e dai principi relativi alla qualità dei dati (art. 9).

Anche l'informativa agli interessati (art. 24) è modellata sulla direttiva, nel senso che il legislatore ha compiuto la scelta di non andare oltre le prescrizioni dell'art. 11 della norma comunitaria (informazioni relative all'identità del titolare, alle finalità del trattamento, ai destinatari dei dati e all'esistenza di un diritto di accesso). Non vengono indicate le modalità con cui l'informativa deve raggiungere l'interessato (essendo previsto soltanto che "il titolare deve fare in modo che l'interessato possa disporre di informazioni..."). Nell'esercizio del diritto di accesso (artt. 26-28) è previsto l'obbligo per l'interessato di presentare una richiesta per iscritto ovvero di recarsi di persona nel luogo ove il titolare effettua il trattamento; il titolare ha tre mesi di tempo per rispondere, sempre per iscritto, ovvero per fornire copia dei dati. In caso di mancata risposta, l'interessato può sottoporre il caso all'attenzione del Data Protection Ombudsman (l'autorità garante della protezione dei dati). In base alla normativa precedente, l'interessato poteva esercitare il diritto di accesso agli archivi contenenti dati che lo riguardavano non più di una volta all'anno; nella legge attuale, l'esercizio del diritto di accesso non è soggetto invece a vincoli del genere, tranne il pagamento di una somma "ragionevole" se è trascorso meno di un anno dall'ultimo accesso effettuato.

È interessante osservare che la notificazione dei trattamenti (artt. 36-37) si fonda su una "descrizione" dell'archivio di dati (non del trattamento) (art. 10) che il titolare è tenuto a compilare e a tenere sempre a disposizione di chiunque voglia prenderne visione. La notificazione deve essere presentata al Data Protection Ombudsman almeno 30 giorni prima di dare corso alla raccolta o alla registrazione dei dati personali. Anche la legge finlandese prevede esenzioni dall'obbligo di notificazione, in particolare per quanto riguarda l'attività giornalistica (esplicitamente menzionata nell'art. 15 ).

Per quanto concerne i poteri del Data Protection Ombudsman, va detto che, oltre alla possibilità di emanare direttive e raccomandazioni (anche in materia di codici deontologici), le sue competenze si limitano all'esame delle segnalazioni degli interessati per il mancato esercizio dei diritti di accesso e rettifica (art. 40), mentre per ogni altra violazione della normativa in materia la competenza è dell'autorità giudiziaria ordinaria ovvero del Data Inspection Board (Commissione per la protezione dei dati) - un ente di nomina governativa già previsto dalla legge precedentemente in vigore. In particolare, il pubblico ministero deve sentire l'Ombudsman prima di formulare un'imputazione per violazione delle norme di protezione dati (art. 41). La legge (art. 44) prevede inoltre che, su richiesta dell'Ombudsman, il Data Protection Board possa emettere ordinanze finalizzate a vietare o bloccare trattamenti illegittimi di dati personali, ovvero ad imporre rimedi giuridici per condotte illecite. Va rilevato che la legge prevede la responsabilità per danni morali e materiali da parte del titolare (art. 47) indipendentemente dalle modalità dell'atto.

Un ulteriore elemento di interesse è l'attenzione dedicata ai trattamenti di dati per fini di marketing diretto (art. 19) o di valutazione della solvibilità (art. 20). In particolare, il trattamento di dati personali per fini di marketing diretto necessita del consenso dell'interessato e presuppone l'inserimento delle sole generalità della persona (compresa età e sesso) e di "un dato distintivo"; nel caso degli archivi contenenti valutazioni della solvibilità il consenso non occorre, ma l'inserimento deve basarsi su una sentenza definitiva (anche in contumacia) di fallimento o su una dichiarazione di protesto, ovvero su una clausola presente in accordi di leasing stipulati fra l'interessato e il titolare. La legge prescrive la cancellazione (art. 21) dei dati contenuti in questi ultimi archivi dopo quattro anni in caso di mancato pagamento, dopo cinque per quanto riguarda i casi di fallimento, e dopo non oltre due anni nei casi restanti.

Per quanto riguarda la direttiva "figlia", ossia la n. 97/66, lo stato della sua trasposizione nel diritto nazionale degli Stati membri dell'UE è piuttosto complesso. Mentre alcuni Stati non hanno sinora adottato le misure legislative necessarie (si tratta, più precisamente, di Grecia, Irlanda e Lussemburgo), ve ne sono altri nei quali si può parlare (anche in base alla documentazione in possesso della Commissione europea - Direzione generale XIII - Società dell'informazione) di "parziale trasposizione" - con ciò intendendo il fatto che alcuni importanti principi della direttiva non sono stati recepiti o lo sono stati in modo solo parziale. Rientrano in questo gruppo:

- il Belgio, dove la direttiva ha trovato parziale trasposizione nella legge sulla protezione dei dati del 1999 e in un decreto reale (del 22 giugno 1998) che fissa gli importi per il servizio di telefonia vocale e la procedura relativa alla concessione delle autorizzazioni individuali. Sono in via di preparazione norme di legge in materia di fatturazione dettagliata e informazioni sul volume del traffico e la fatturazione;
- la Danimarca, dove la direttiva è stata trasposta in misura parziale attraverso un decreto che riguarda i fornitori di reti e servizi di telecomunicazioni e le basi di dati dei servizi di informazioni su abbonati. L'articolo 12 della direttiva (chiamate indesiderate) richiede un emendamento della legge sul marketing ai fini della trasposizione;
- la Francia, dove due leggi in materia di telecomunicazioni (Loi 96-659 e Loi 90-1170) e un decreto (Décret 96-1175 del 29 dicembre 1990) danno parziale attuazione alle disposizioni della direttiva. Mancano però norme che disciplinino l'obbligo di informare gli abbonati in materia di rischi per la sicurezza delle reti, la cancellazione dei dati, le limitazioni relative alla fatturazione dettagliata, l'identificazione della linea chiamante e le chiamate indesiderate;
- i Paesi Bassi, dove esiste una legge sulle telecomunicazioni ed un regolamento sull'identificazione numerica (del 1998); si prevede di introdurre legislazione secondaria per quanto riguarda fatturazione e chiamate indesiderate;
- il Regno Unito, dove esiste un regolamento in materia di telecomunicazioni (Data Protection and Privacy, Direct Marketing) del 1998 che recepisce in misura molto parziale le disposizioni della direttiva. È prevista l'emanazione di normativa secondaria (ma anche primaria) per dare piena attuazione alle disposizioni comunitarie.

Nei restanti Paesi dell'UE la direttiva 97/66 è stata "sostanzialmente" trasposta - il che significa che tutti i principi fondamentali trovano attuazione ed è dunque possibile la realizzazione delle finalità che la direttiva si prefigge. Va detto, comunque, che nei singoli Paesi varia la natura degli atti con cui si è recepito il dettato comunitario, nel senso che spesso occorre fare riferimento ad un complesso insieme di norme primarie, norme secondarie e regolamentari che si applicano specificamente a settori determinati; ad esempio, in Finlandia, oltre alla legge sulla tutela della privacy e la sicurezza dei dati nelle telecomunicazioni, n. 565/1999, esiste un regolamento sulla sicurezza informatica delle telecomunicazioni ed un regolamento sulla tutela fisica dei locali e delle reti di operatori di telecomunicazioni. In Portogallo la trasposizione della direttiva è invece demandata alla Legge 69/98 che regola il trattamento di dati personali e la tutela della riservatezza nel settore delle telecomunicazioni, sostanzialmente analoga nell'impianto al decreto legislativo n. 171/98 che ha recepito la direttiva per l'Italia.

5.4 Altri gruppi di lavoro in materia di protezione dei dati

Sempre collegato al quadro comunitario che ruota attorno alle direttive 95/46/CE e 97/66/CE, va indicato come particolarmente importante per il Garante, che prende parte attiva ai lavori, il Gruppo protezione dei dati.

Nel corso dell'anno è proseguita da parte del Gruppo l'attività di coordinamento per defi-

nire la posizione dei Paesi comunitari rispetto ai documenti e testi normativi in discussione, in particolare presso il Consiglio d'Europa, in materia di protezione dei dati personali e, grazie al positivo esito delle riunioni, è stato possibile completare l'iter relativo alla definizione dei modi per consentire l'adesione delle Comunità europee alla Convenzione n. 108 del Consiglio d'Europa.

È stato inoltre completato l'esame del Protocollo aggiuntivo alla Convenzione n. 108 con il quale si intendono apportare alla stessa importanti modificazioni per allinearla meglio alla direttiva 95/46/CE. Il Protocollo introduce infatti specifiche disposizioni intese a pervenire alla creazione di autorità di controllo nazionali ed a disciplinare compiutamente la trasmissione di dati da e verso Paesi terzi.

Il Gruppo sta ora concentrando la sua attenzione sulla proposta di regolamento del Parlamento e del Consiglio relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni e degli organi della Comunità europea. La proposta, che è stata presentata dalla Commissione al Gruppo protezione dei dati nella riunione dell'8 settembre 1999 (doc. COM (1999) 337 def. del 14 luglio) è intesa a dare attuazione al dettato dell'art. 286 del Trattato di Amsterdam , in base al quale:

- a decorrere dal 1° gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, si applicano alle istituzioni e agli organismi istituiti dal Trattato o sulla base del medesimo;
- anteriormente alla data di cui al paragrafo 1 il Consiglio, deliberando secondo la procedura di cui all'articolo 251, istituisce un organo di controllo indipendente incaricato di sorvegliare l'applicazione di detti atti alle istituzioni e agli organismi comunitari e adotta, se del caso, tutte le altre pertinenti disposizioni.

Il provvedimento mira pertanto ad introdurre all'interno delle istituzioni e degli organismi comunitari un livello di tutela dei dati personali corrispondente a quello assicurato in ciascuno degli Stati membri con la trasposizione delle direttive comunitarie 95/46/CE e 97/66/CE.

Le direttive citate si indirizzano ai soli Stati membri. Tuttavia, già prima del ricordato articolo 286 e precisamente al momento dell'adozione della direttiva 95/46/CE nel 1995, la Commissione ed il Consiglio si impegnarono con un dichiarazione pubblica ad applicarne i principi, impegno divenuto oggi vincolante.

I principi di protezione dei dati contenuti nella proposta di regolamento sono quindi basati sulle disposizioni comunitarie esistenti e li integrano dettando specifiche disposizioni laddove la direttiva quadro 95/46/CE lascia margini attuativi agli Stati.

La proposta è articolata in sei capi e si compone di 49 articoli:

**Capo I** - *Disposizioni generali* (artt. 1-3 riguardanti l'oggetto, le definizioni, il campo di applicazione).

**Capo II** - *Condizioni generali di liceità delle operazioni di trattamento dei dati personali* (artt. 4-28 contenenti diverse sezioni riguardanti i principi di qualità dei dati, di legittimazione al trattamento -inclusi i principi relativi al trasferimento dei dati ed il trattamento dei dati sensibili- la definizione dei diritti degli interessati all'informativa sui trattamenti che li riguardano e le modalità di esercizio del diritto di accesso, la riservatezza e sicurezza del trattamento. Si prevede inoltre l'istituzione della figura del responsabile della protezione dati all'interno di ogni istituzione ed organismo comunitario ed i casi in cui è necessario il preventivo avviso del Garante europeo rispetto a trattamenti di dati personali che possono comportare dei rischi).

**Capo III** - *Mezzi di ricorso e sanzioni* (artt. 29 e 30).

**Capo IV** - *Protezione dei dati personali e tutela della riservatezza nell'ambito delle reti interne di*

*telecomunicazione* (artt. 31-37 largamente incentrati sull'adattamento ai principi della direttiva 97/66/CE relativa alla tutela della vita privata nel settore delle telecomunicazioni).

**Capo V** - *Autorità di vigilanza: il Garante europeo della tutela dei dati* (artt. 38-47 che definiscono i requisiti di indipendenza, le modalità di nomina e revoca, i poteri e la struttura di cui si avvale il Garante).

**Capo VI** - *Disposizioni finali* (artt. 48 e 49).

Risulta quindi giustificata l'attenzione con la quale si procede alla definizione della figura, dei compiti e della struttura della futura autorità di vigilanza, il c.d. "Garante europeo". Quest'ultimo sarà infatti costituito come un organo indipendente e sarà responsabile della vigilanza e del controllo sulla corretta applicazione delle norme in materia di protezione dei dati da parte delle istituzioni e degli organismi comunitari. Avrà pertanto competenze e poteri simili a quelli garantiti alle autorità nazionali di protezione dei dati: in particolare potrà essere adito dai cittadini che si ritengano lesi da comportamenti o atti delle istituzioni tenute all'applicazione del regolamento.

La discussione del regolamento procede con un ritmo abbastanza intenso e ciò ha consentito di concludere la prima lettura del provvedimento all'inizio di gennaio e di iniziare quindi la seconda lettura che dovrebbe concludersi entro il mese di aprile. I lavori si basano sul testo iniziale anche se largamente modificato a seguito della discussione avutasi. La Commissione presenterà una proposta modificata non appena il Parlamento europeo avrà espresso il suo parere sul testo.Da parte di tutte le delegazioni è stato espresso l'auspicio di una rapida adozione del regolamento.

### 5.5 Cooperazione europea nel settore giustizia e affari interni

L'entrata in vigore il 1 maggio 1999 del Trattato di Amsterdam ha determinato, da un lato la progressiva comunitarizzazione di materie come l'immigrazione e l'asilo, che sono disciplinate nei modi e nelle forme previsti dal titolo IV del Trattato e che comprendono modelli di "cooperazione rafforzata" già definiti tra Paesi dell'Unione, come la cooperazione in ambito Schengen.

Il Trattato di Amsterdam prevede infatti l'incorporazione dell'acquis di Schengen nelle attività del Consiglio, secondo modalità fissate in un apposito protocollo. A queste attività, almeno tendenzialmente e fatta salva la competenza dell'Autorità comune di controllo Schengen in relazione alla vigilanza sulla parte centrale del Sistema d'Informazione Schengen, dovrà applicarsi, in quanto svolte da istituzioni e/o organismi comunitari, il regolamento attuativo dell'articolo 286 cui si è fatto cenno. Conseguentemente la vigilanza ed il controllo sulla corretta attuazione dei principi in materia di protezione dei dati sarà attribuita all'istituendo Garante europeo.

La restante parte del titolo VI del Trattato di Maastricht, dedicato alla cooperazione in materia di affari interni e giustizia, forma ora il titolo VI del Trattato di Amsterdam ed è centrato sulla creazione di uno spazio di sicurezza, libertà e giustizia, obiettivo da raggiungere mediante strumenti che affinino la cooperazione di polizia e giudiziaria in materia penale tra gli Stati (non va dimenticata la particolare posizione di Danimarca, Irlanda e Regno Unito).

Lo svilupparsi della cooperazione nel settore, ripresa ora nel testo stesso del Trattato, conferma senz'altro la riflessione del Garante circa la necessità di razionalizzare il quadro esistente ed evitare che si pervenga ad altri accordi che prevedano la creazione di strumenti basati su scambi informatizzati di dati personali in assenza di un riferimento normativo unitario. Infatti la tendenza a prevedere, nelle elaborazioni dei gruppi che lavorano sui diversi aspetti della cooperazione nelle materie previste dal titolo VI, specifiche disposizioni in materia di protezione dei dati personali, non

serve a creare un insieme armonizzato di regole applicabili in via generale a quei trattamenti, ma invece, a differenziare i diritti e le tutele.

Come già evidenziato nella precedente relazione, queste preoccupazioni sono state accolte e, su proposta italiana, il Consiglio dei ministri europei della giustizia e affari interni ha deciso di far effettuare una ricognizione puntuale dei diversi strumenti esistenti ed in corso di definizione, di studiare le forme più idonee per ridurre le disarmonie esistenti nei diversi testi e il rischio di disparità di trattamento nel riconoscimento agli interessati dei diritti previsti in materia di protezione dei dati, nonché di razionalizzare la complessa tematica pervenendo ad un grado più elevato di armonizzazione ed evitando duplicazioni di personale e mezzi.

Per sviluppare eventuali ipotesi, anche normative, di soluzione, è stato costituito presso il Consiglio un apposito gruppo di lavoro, di cui il Garante fa parte.

I lavori del Gruppo, iniziati nel febbraio del 1999, si sono finora articolati seguendo, su impulso di diverse delegazioni, un approccio pragmatico. Partendo dalle perplessità di alcuni Paesi rispetto all'idea che si potesse giungere alla definizione di principi comuni in materia di tutela dei dati volti ad incidere sull'effettività dell'azione di polizia e di magistratura nel contrasto della criminalità organizzata in ambito sovranazionale, si è proposto di partire da un altro angolo visuale ovvero dalle questioni più facilmente risolvibili. Si è così discusso di un problema di funzionalità delle autorità, cioè della costituzione di un segretariato comune, per fornire supporto alle autorità di controllo già previste ed istituite dalle convenzioni Schengen, Europol e Sistema informativo doganale, della sua composizione e della sua autonoma collocazione per farne un ufficio dotato di effettiva indipendenza; si è discusso inoltre dell'unificazione della composizione delle suddette autorità.

Minore attenzione è stata invece posta, almeno sinora, riguardo al tema della definizione dei principi, sebbene con la presidenza di turno portoghese si è tentato di riprendere il discorso in base alla logica iniziale. La presidenza ha infatti presentato di recente un documento recante "principi generali concernenti la protezione dei dati nel terzo pilastro", che costituisce il frutto della riflessione sui principi già consolidati in materia di protezione dei dati derivanti dalla Convenzione n. 108 del Consiglio d'Europa e dalla direttiva 95/46/CE, e di quelli, che, già dettati per l'attività in senso generale "di polizia" dalla Racc. 87(15) del Consiglio d'Europa e dalla Convenzione Europol, potrebbero, in tutto od in parte, essere riconosciuti applicabili alle attività del terzo pilastro.

Il ritorno al senso della proposta iniziale e l'approfondimento degli spunti dalla stessa suggeriti rappresenta una prospettiva di spiccato interesse, pur nel mutato scenario istituzionale. Del resto la profonda convinzione che l'introduzione di norme specifiche in materia di protezione dei dati non solo non costituisce un vulnus dell'attività di inquirenti e forze di polizia nella prevenzione e repressione dei reati, ma che, anzi, ne consente una maggiore incisività e trasparenza, ha determinato il Garante a presentare, come già accennato, nell'ambito del "programma Falcone", un progetto denominato "Lotta alla criminalità organizzata e protezione dei dati", volto, attraverso seminari specificamente dedicati all'approfondimento concreto e lo studio dei casi, proprio alla verifica dell'impatto che la legislazione in materia di protezione dei dati ha avuto ed ha sull'attività ricordata.

### 5.6 Schengen

Nel 1999, come riassunto in altra parte della presente relazione, è proseguita l'opera di controllo svolta dal Garante sul funzionamento dell'archivio della sezione nazionale del Sistema d'Informazione di Schengen.

A seguito dell'entrata in vigore del Trattato di Amsterdam, l'attività di cooperazione svolta

in ambito Schengen è stata ricollocata nel Consiglio. In base allo specifico Protocollo annesso al Trattato, infatti, sono state definite le modalità per l'incorporazione del c.d. "acquis" e la ripartizione delle attività nei diversi titoli del Trattato. Le riunioni si svolgono quindi presso il Consiglio, che è competente anche per gli aspetti finanziari e logistici. Questa nuova collocazione ha avuto immediati ed importanti riflessi anche sul funzionamento dell'Autorità comune di controllo. Con una decisione del 12 maggio 1999 il Consiglio ha adottato specifiche disposizioni, in particolare riguardo alla tenuta delle riunioni ed al finanziamento dell'attività dell'Autorità di controllo comune.

Delicati problemi si pongono con particolare riguardo alla indipendenza dell'Autorità ed alla mancanza di un suo proprio segretariato, problemi cui forse potrà essere data positiva soluzione con l'auspicata istituzione del segretariato comune delle Autorità comuni di controllo già ricordato.

Il Garante partecipa all'Autorità comune di controllo, istituita ai sensi dell'art. 115 della Convenzione di applicazione dell'Accordo di Schengen, contribuendo alla definizione ed adozione di specifiche raccomandazioni e pareri. L'intensa e fattiva opera prestata si riflette nella nomina a vice- presidente dell'ACC del segretario generale dott. Buttarelli, avvenuta nel novembre scorso.

Si allega alla presente relazione il Rapporto dell'ACC relativo al periodo marzo 1998-marzo 1999, che è stato ufficialmente presentato a Firenze il 27 e 28 maggio scorsi. Si differisce invece la pubblicazione di quello relativo al periodo marzo 1999-marzo 2000 la cui predisposizione è ancora in corso.

Come già accennato, a seguito della deliberazione dell'ACC di invito per tutti i Paesi partecipanti al sistema Schengen ad attuare una campagna informativa per il pubblico da svolgere mediante la distribuzione di opuscoli e depliants plurilingue recanti le modalità per esercitare il diritto di accesso ai dati detenuti nel Sistema informativo Schengen da parte dei soggetti interessati, il Garante, ha curato la stampa del materiale necessario, e con la collaborazione delle amministrazioni competenti, Ministero degli Affari Esteri e dell'Interno, ha disposto la distribuzione presso le ambasciate ed i varchi di frontiera. Poiché tra le informazioni fornite negli opuscoli illustrativi distribuiti vi era anche l'indirizzo del Garante come autorità di tutela cui fare riferimento in caso di chiarimenti, doglianze, errori, può senz'altro ascriversi anche ai risultati della campagna l'incremento delle richieste riscontrate nella seconda metà dell'anno.

### 5.7 Europol

La legge 23 marzo 1998, n. 93, ha autorizzato la ratifica e l'esecuzione della Convenzione basata sull'art. K3 del Trattato sull'Unione europea del 25 luglio 1995 che istituisce un Ufficio europeo di polizia (Europol). La stessa legge ha affidato al Garante per la protezione dei dati personali il ruolo di autorità di controllo nazionale ai sensi dell'art. 23 della convenzione stessa.

Spetta quindi al Garante accertare che l'introduzione, la consultazione, la trasmissione, in qualsiasi forma, all'Europol di dati personali da parte dell'Italia avvengano nel rispetto delle norme ed a tal fine il Garante avrà accesso ai dati ed agli archivi. Sulla base dei principi dettati nelle leggi 675 e 676 del 1996, il Garante dovrà inoltre controllare le attività svolte dall'unità nazionale e dagli ufficiali di collegamento per la parte concernente le tutela dei dati personali. In base al disposto della Convenzione, che ha attribuito a chiunque il diritto di chiedere all'autorità di controllo nazionale di verificare la legittimità dell'introduzione e della trasmissione all'Europol di dati che lo riguardano, al Garante spetta inoltre di provvedere sulle specifiche istanze, nel rispetto delle procedure previste dalla legge n. 675.

Dall'entrata in vigore della Convenzione, avvenuta il 1° ottobre 1998, sono state presentate ad Europol due richieste che non hanno dato luogo a ricorso.

Nel corso dell'anno ha continuato i suoi lavori l'Autorità comune di controllo, prevista dall'art. 24 della Convenzione. Questa Autorità, composta da due rappresentanti per Paese delle autorità nazionali di controllo, esercita incisivi controlli sulla gestione degli archivi Europol, che dal luglio 1999 comprendono gli archivi di analisi. L'Autorità valuta, in relazione ai compiti affidati dalla Convenzione gli ordini di apertura dei file di analisi.

L'Autorità ha definito in un regolamento interno, che è stato approvato nel mese di maggio e pubblicato sulla Gazzetta ufficiale delle Comunità europee, le necessarie misure procedurali, anche riguardo al comitato ricorsi, ed ha definito i suoi compiti.

È da ricordare inoltre l'ampio dibattito parlamentare in relazione alla ratifica del Protocollo relativo ai privilegi ed immunità di Europol, volto ad approfondire un tema analizzato anche dal Garante, relativo alle guarentigie riconosciute ad Europol ed ai suoi agenti e rappresentanti. Il Protocollo conferisce infatti ad Europol (art. 2, comma 1) l'immunità giurisdizionale per la responsabilità di cui all'art. 38, paragrafo 1 della Convenzione, rispetto al trattamento di dati illecito o effettuato in modo non corretto, disposizione che sembra introdurre una deroga alla normativa internazionale della protezione dei dati che ingenera il timore di una possibile attenuazione delle garanzie contenute nella Convenzione. Il Parlamento, al momento del voto finale, ha pertanto raccomandato di limitare le immunità ed i privilegi all'essenziale, e cioè alle attività svolte in relazione al mandato iniziale di Europol quale risulta dalla Convenzione e di studiare eventuali interventi di chiarificazione anche attraverso la revisione della Convenzione stessa.

### 5.8 Sistema informativo doganale

Con la legge 30 luglio 1998, n. 291, l'Italia ha autorizzato la ratifica e l'esecuzione della Convenzione sull'uso dell'informatica nel settore doganale, elaborata in base all'articolo K3 del Trattato sull'Unione europea del 26 luglio 1995.

La Convenzione mira ad intensificare la cooperazione tra le amministrazioni doganali dei diversi Paesi dell'Unione europea, particolarmente attraverso lo scambio di dati personali.

A tal fine è stata prevista la creazione di un sistema informativo automatizzato comune (Sistema informativo doganale -SID) che dovrebbe facilitare la prevenzione, la ricerca ed il perseguimento delle infrazioni alle leggi nazionali.

La Convenzione istituisce una autorità comune di controllo, composta di due rappresentanti per ciascun Paese delle autorità nazionali di protezione dei dati.

La Convenzione non è ancora entrata in vigore, né è stata ancora istituita l'autorità comune di controllo.

### 5.9 Eurodac

Il progetto di Convenzione per l'istituzione di un sistema per la raccolta, la memorizzazione, il confronto e lo scambio di dati relativi alle impronte digitali dei richiedenti asilo, basata sull'art. 15 della Convenzione di Dublino relativa alla determinazione dello Stato competente per l'esame delle richieste d'asilo, prosegue i lavori nell'ambito dell'apposito gruppo.

Anche questo progetto di Convenzione rientra nella riflessione generale sull'opportunità di

razionalizzare gli strumenti elaborati od in via di elaborazione nel settore della cooperazione affari interni e giustizia proposta dall'Italia, anche se con l'entrata in vigore del Trattato di Amsterdam l'autorità incaricata della vigilanza e controllo in materia di protezione dei dati dovrebbe essere il c.d. Garante europeo previsto del regolamento attuativo dell'articolo 286 del Trattato.

5.10 Consiglio d'Europa

Il Consiglio d'Europa ha proseguito la sua attività di elaborazione e sviluppo della normativa europea in materia di tutela dei dati personali, in particolare attraverso i lavori dei comitati plenari T-PD e CJ-PD e del gruppo GT-15.

Il Comitato consultivo della Convenzione n. 108 (T-PD), nella riunione plenaria annuale, ha trattato i seguenti temi:

- esame ed approvazione del testo di un protocollo aggiuntivo alla Convenzione, destinato ad introdurre l'obbligo dell'istituzione di autorità nazionali di controllo ed a disciplinare i flussi transfrontalieri di dati;
- modifica delle procedure da seguire per l'adozione di provvedimenti del Consiglio d'Europa, esaminata dal Comitato dei Ministri nel mese di aprile 1999;
- progetto di raccomandazione per estendere, su base volontaria, l'applicazione dei principi della convenzione anche ai dati cartacei;
- questionario sui dati sensibili volto ad accertare l'uniformità delle definizioni adottate dai diversi Paesi e la possibilità di inserirvi altre categorie di dati.

È stata inoltre approvata dal Comitato dei Ministri la modifica alla Convenzione predisposta dal Comitato e discussa nelle riunioni di coordinamento comunitario, volta a permettere l'adesione delle Comunità europee alla Convenzione. La modifica entrerà in vigore quando avrà raggiunto il numero di ratifiche richiesto. La decisione adottata è nel senso di emendarne il testo seguendo la procedura ordinaria prevista dall'art. 21, in quanto questa risulta più flessibile e rapida.

Le modifiche conseguentemente apportate consistono nell'inserimento del riferimento alle Comunità europee accanto a quello agli Stati ed alla modifica delle procedure di voto del Comitato, prevedendosi che nelle materie di competenza comunitaria, le Comunità europee esercitino il diritto di voto esprimendo un numero di voti pari al numero dei Paesi membri dell'Unione che non si sono avvalsi della clausola dell'opting out, liberi questi ultimi (Regno Unito, Irlanda e Danimarca) di accettare caso per caso il coordinamento comunitario.

Sono state adattate di conseguenza le disposizioni del regolamento interno per tutelare gli Stati parte non membri dell'Unione qualora, vertendosi in materie attribuite alle competenze comunitarie, gli Stati dell'U.E. votino attraverso la Commissione europea.

Sono inoltre proseguiti i lavori per la definizione del progetto di protocollo addizionale alla Convenzione, facoltativo per i Paesi che intendano accedere alla Convenzione, per gli aspetti relativi alle autorità di controllo ed ai flussi transfrontalieri. Come già ricordato, anche questo tema ha formato oggetto di previa concertazione comunitaria in seno al gruppo protezione dati dell'U.E.

È stata inoltre adottata la Raccomandazione 99 (5), predisposta dal Gruppo di progetto sulla protezione dei dati-CJ-PD e concernente *"linee-guida per la protezione della privacy in INTERNET"*.

Il CJ-PD, sotto-comitato istituito nell'ambito della cooperazione giudiziaria, che tratta dell'elaborazione di proposte e progetti di raccomandazioni rivolti ad integrare e specificare le disposizioni della Convenzione n. 108 con riguardo a settori determinati, nella sua riunione di ottobre

1999 ha completato l'esame della proposta di Raccomandazione sul trattamento dei dati personali raccolti e trattati a fini assicurativi e ne ha definitivamente messo a punto il testo, anche sulla scorta della posizione comunitaria ufficializzata in una nota della Commissione europea.

Altri argomenti all'esame del Gruppo sono stati il progetto di Raccomandazione n. 1402/1999 del Parlamento europeo concernente il "Controllo dei servizi di sicurezza negli Stati membri del Consiglio d'Europa" e l'elezione del nuovo presidente.

Gran parte del lavoro preparatorio delle riunioni del CJ-PD viene svolto dal bureau, composto dal Presidente e dai vice presidenti, che restano in carica per un biennio e possono essere rinnovati.

Il comitato ha inoltre istituito un Gruppo di lavoro, denominato Gruppo di lavoro nuove tecnologie, che in particolare affronta i temi della videosorveglianza e della criminalità nel cyber spazio. Il gruppo si riunisce in genere, a seconda delle compatibilità di bilancio, una o due volte l'anno, in autunno e/o in primavera.

Nel corso dell'ultima riunione si è svolta una discussione sui primi problemi riscontrati nell'applicazione delle linee guida per l'uso di Internet ed è stato esaminato il progetto di Raccomandazione sulla videosorveglianza.

5.11 O.C.S.E.

Il Garante partecipa anche ai lavori di alcuni gruppi in sede O.C.S.E. nei gruppi e comitati che hanno tra le loro attribuzioni la materia della protezione dei dati.

In particolare, le attività di interesse dell'Autorità sono demandate al Comitato per la politica dell'informazione (ICCP) istituito all'interno della Direzione scienza, tecnologia e industria dell'OCSE.

Il Comitato si riunisce due volte l'anno ed organizza seminari su temi specifici.

Il suo mandato, scaduto il 20 febbraio 1999, è stato prorogato fino al 1° marzo 2004 ed è stato ampliato, alla luce delle conclusioni della Conferenza ministeriale di Ottawa, per comprendere agli aspetti legati al "commercio elettronico, alla sicurezza dell'informazione, alla *protezione della privacy* e all'infrastruttura della società dell'informazione".

Il Comitato ICCP è articolato in quattro gruppi di lavoro:

- Gruppo di lavoro per la politica dei servizi di informazione e di telecomunicazione;
- Gruppo di lavoro sull'economia delle infrastrutture;
- " " sugli indicatori della società di informazione;
- " " sulla sicurezza dell'informazione e sulla privacy.

Il gruppo si riunisce di regola due volte l'anno, a maggio ed a ottobre e segue le tematiche connesse alla tutela della riservatezza, con specifico riferimento al mondo delle telecomunicazioni.

Ha elaborato in particolare le linee-guida per la politica in materia di crittografia, approvate dal Consiglio OCSE nel 1997 ed ha organizzato nel 1998 una Conferenza sulla *privacy* nelle comunicazioni *on-line*.

Le elaborazioni del gruppo WPISP sono sottoposte al Comitato ICCP per l'approvazione.

Il Garante, su richiesta di quel Ministero, ha partecipato alle riunioni di coordinamento interministeriali organizzate presso il Ministero degli affari esteri allo scopo di definire temi e

modalità e la composizione della delegazione italiana per la partecipazione al Forum organizzato dalla Direzione della scienza-tecnologia generale per approfondire i temi trattati nel corso della Conferenza di Ottawa sul commercio elettronico, che si è svolto il 12 e 13 ottobre 1999.

L'OCSE ha adottato infine il 9 dicembre alcune linee-guida sulla protezione del consumatore on-line, che contengono specifici principi in materia di rispetto della privacy.

### 5.12 Collaborazione con altre autorità di garanzia

Oltre agli obblighi di collaborazione con le altre autorità di controllo nascenti dalla Convenzione n. 108/1981 e da altri atti internazionali e comunitari, come ad esempio l'Accordo di Schengen e la convenzione Europol, il Garante ha continuato a mantenere nel corso dell'anno stretti contatti con tali istituzioni per favorire lo scambio di esperienze ed opinioni, anche al fine di raggiungere, ove possibile, interpretazioni convergenti o omogenee.

Il Garante ha inoltre partecipato con assiduità a numerose conferenze europee e mondiali che, per la loro rilevanza e la natura dei temi trattati, hanno rappresentato un importante foro di discussione ed hanno consentito un puntuale aggiornamento.

Sono state, in particolare seguite le Conferenze internazionali ed europee delle autorità garanti, che sono organizzate anche nel 1999 con criteri di periodicità, nella primavera e in autunno come in altri anni.

Nel corso del 1999 la conferenza europea si è tenuta a Helsinki dal 14 al 16 aprile 1999 e quella mondiale ad Hong Kong il 13- 15 settembre 1999.

Da segnalare la particolare attenzione rivolta dalle autorità europee agli strumenti elaborati od in corso di elaborazione nell'ambito della cooperazione affari interni e giustizia che prevedono l'istituzione di sistemi di scambi di dati personali e la necessità di armonizzare le varie disposizioni, sostanziali e procedurali.

L'incontro periodico dell'Autorità comune di controllo Schengen si è svolto a Firenze il 27 e 28 maggio 1999.

# 6. ALLEGATI

## Quadro sinottico dello stato di recepimento delle direttive comunitarie in materia di protezione dei dati personali

**Direttiva 95/46/CE (Situazione al gennaio 2000)**

**Paesi nei quali la direttiva è stata recepita con *legge***

*Austria* - Legge n. 165/99 del 17 agosto 1999
*Belgio* – Legge 3 febbraio 1999 sulla protezione dei dati personali
*Finlandia* – Legge 10 febbraio 1999
*Grecia* - Legge n. 2472 del 10 aprile 1997
*Italia* – Legge n. 675/1996 del 31 dicembre 1996
*Portogallo* - Legge n. 67/98 del 26 ottobre 1998
*Regno Unito* - Legge 16 luglio 1998 (Data Protection Act)
*Spagna* – Legge organica n. 15/99 (entrata in vigore il 14 gennaio 2000)
*Svezia* - Legge 204/98 del 29 aprile 1998 e regolamento attuativo 1191/98 del 03 settembre 1998

**Paesi nei quali *disegni di legge* di recepimento sono all'esame del Parlamento**

*Danimarca* - Progetto di legge L-44 (presentato al Parlamento per tre volte senza giungere alla discussione del testo);
*Lussemburgo* - Il Governo avrebbe dovuto presentare un disegno di legge nel mese di marzo 1999
*Paesi Bassi* – Il progetto di legge è stato discusso e approvato dalla Camera Alta e dalla Camera Bassa; si attende l'emanazione definitiva attraverso il decreto della Regina.

**Paesi nei quali *non* è stato ancora presentato in sede parlamentare un *disegno di legge* per il recepimento**

*Francia* - Il Governo deve presentare un disegno di legge in materia
*Germania* - L'esame in Parlamento del nuovo disegno di legge governativo (*Novellierung des Bundesdatenschutzgesetzes* - ripresentato dall'attuale Governo) deve ancora iniziare.
*Irlanda* - Il Governo ha elaborato un disegno di legge in materia che però non è stato ancora presentato al Parlamento.

**Direttiva 97/66/CE (Situazione al gennaio 2000)**

**Paesi nei quali la direttiva è stata recepita *"in misura sostanziale"***

*Austria* – Legge sulle telecomunicazioni (Telekommunikationsgesetz) del 19 agosto 1997
Finlandia – Legge sulla tutela della privacy e della sicurezza dei dati nelle telecomunicazioni (n. 565/1999); Regolamento sulla sicurezza informatica degli operatori di telecomunicazioni, del 1999; Regolamento sulla protezione fisica degli ambienti e delle reti degli operatori di telecomunicazioni, del 1999
Germania – Legge sulle telecomunicazioni (Telekommunikationsgesetz) del 25 luglio 1996 e Regolamento sulla protezione dei dati (Telekommunikationsdienstunternehmen-

Datenschutzverordnung) del 12 luglio 1996
**Italia** – Decreto legislativo n. 171 del 13 maggio 1998
Portogallo – Legge n. 69/98, relativa al trattamento dei dati personali e alla tutela della riservatezza nel settore delle telecomunicazioni
*Spagna* – Decreto reale n. 1736/98 (di attuazione del titolo III della legge generale sulle telecomunicazioni)
*Svezia* – Legge sulle telecomunicazioni; Regolamento sui servizi telefonici.

**Paesi nei quali la direttiva è stata recepita *"in misura parziale"***

***Belgio*** – Legge sulle telecomunicazioni del 21 marzo 1991; decreto reale del 22 giugno 1998 (servizi telefonici) – Mancano: fatturazione dettagliata; dati sul traffico; chiamate indesiderate
***Danimarca*** – Decreto sulla fornitura di reti e servizi di telecomunicazioni; Decreto sulle basi di dati dei servizi di ricerca abbonati – Mancano: chiamate indesiderate
***Francia*** – Legge sulle telecomunicazioni (96-659; 90-1170) – Mancano: informativa abbonati su rischi sicurezza; fatturazione dettagliata; chiamate indesiderate
***Paesi Bassi*** – Legge sulle telecomunicazioni; Regolamento sull'identificazione numerica del 1998 – Mancano: fatturazione; chiamate indesiderate
***Regno Unito*** – Regolamento sulle telecomunicazioni (protezione dati e privacy; marketing diretto) del 1998 – Mancano: fatturazione dettagliata; chiamate indesiderate; identificazione linea chiamante

***Paesi nei quali la direttiva non è stata sinora trasposta***

***Grecia***
***Irlanda***
***Lussemburgo***

## 6.1 DISPOSIZIONI NORMATIVE

### 6.1.1 Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali

CAPO I
PRINCIPI GENERALI

Art. 1.
*(Finalità e definizioni)*

1. La presente legge garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale; garantisce altresì i diritti delle persone giuridiche e di ogni altro ente o associazione.

2. Ai fini della presente legge si intende:

a) per "banca di dati", qualsiasi complesso di dati personali, ripartito in una o più unità dislocate in uno o più siti, organizzato secondo una pluralità di criteri determinati tali da facilitarne il trattamento;

b) per "trattamento", qualunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati;

c) per "dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

d) per "titolare", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono le decisioni in ordine alle finalità ed alle modalità del trattamento di dati personali, ivi compreso il profilo della sicurezza;

e) per "responsabile", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

f) per "interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

g) per "comunicazione", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

h) per "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

i) per "dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

l) per "blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

m) per "Garante", l'autorità istituita ai sensi dell'articolo 30.