CARLO SARZANA DI S. IPPOLITO

LE INIZIATIVE INTERNAZIONALI IN TEMA DI SISTEMI CRITTOGRAFICI CON RIFERIMENTO ALLA TUTELA DEI DATI PERSONALI

1. L'ATTIVITÀ DELL'OCSE NEL CAMPO DELLA CRITTOGRAFIA.

Il problema della sicurezza nel settore informatico è stato posto all'attenzione delle maggiori Organizzazioni internazionali sin dalla fine degli anni '80.

La presa di posizione più importante è stata quella dell'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico), il cui Consiglio il 26 novembre 1992 ha adottato la Raccomandazione concernente le linee direttrici in tema di sicurezza dei sistemi di informazione, rivolta ai 24 Paesi industrializzati aderenti all'Organizzazione.

Nello stesso 1992 l'OCSE, e per essa il Comitato PIIC[1], ha iniziato a convocare una serie di *meetings* sulla sicurezza, *privacy* e protezione dei diritti di proprietà intellettuale, creando poi un apposito gruppo di lavoro nel cui seno, un sottogruppo ha elaborato, nel gennaio 1997, un progetto di Raccomandazione sulle linee direttrici dell'OCSE in tema di politica della crittografia e sul quale si ritornerà più avanti.

Come risultato di tali *meetings*, *l'OCSE* alla riunione del G7 del febbraio 1995 presentò un rapporto dal titolo « *Infrastrutture mondiali dell'informazione - Società mondiale dell'informazione:*

* Relazione svolta alla giornata di studio indetta dall'ABI a Roma il 5 maggio 1997 sul tema « La tutela della riservatezza delle persone e di altri soggetti rispetto al trattamento dei dati personali. Adempimenti degli intermediari bancari e finanziari ».

[1] Comitato per la politica dell'informazione, dell'informatica e delle comunicazioni.

Raccomandazione per l'azione dei poteri pubblici». In tale documento si menzionava esplicitamente il problema della crittografia a proposito del commercio elettronico (paragrafi da 39 a 42) auspicandosi un'azione congiunta dei Governi e del settore privato, e raccomandandosi — tra l'altro — ai Paesi membri dell'Organizzazione di stabilire al più presto possibile delle linee direttrici comparabili a livello internazionale in materia di crittografia, ispirando i quadri nazionali alle linee direttrici che sarebbero state emanate in tema di politica della crittografia.

Il documento sottolineava, per inciso, che il successo della tecnologia crittografica dipendeva in modo totale dalla fiducia delle imprese e dei consumatori in tale settore e concludeva sul punto raccomandando ai vari Paesi di prevedere dei meccanismi di regolazione degli eventuali conflitti a livello internazionale.

Sempre nell'ambito dell'OCSE, il gruppo di esperti del settore privato sul commercio elettronico ha recentissimamente elaborato un progetto di rapporto sul tema, sottoposto poi nel febbraio di quest'anno al Comitato PIIC. In tale rapporto si esaminano, nell'ambito delle questioni di sicurezza, i problemi scaturenti dall'uso della crittografia, rilevando — tra l'altro — che i dibattiti relativi al settore, sollevano una questione critica e cioè il conflitto tra l'utilizzazione privata della crittografia a fini di riservatezza ed il timore dei Governi di vedere questa utilizzazione limitare le loro capacità di proteggere la sicurezza pubblica e la sicurezza nazionale.

2. In particolare, la Raccomandazione in ordine alle linee direttrici in tema di politica della crittografia.

Come anticipato più innanzi, un gruppo di esperti *ad hoc*, creato nell'ambito del gruppo di esperti sulle linee direttrici in tema di politica della crittografia, ha preparato un progetto, approvato con qualche modifica dal gruppo principale nel gennaio 1997 e trasmesso poi al Comitato PIIC che lo ha esaminato e lo ha approvato nella sua 31ª seduta del febbraio successivo. Il documento dopo il coordinamento effettuato dal Segretario è stato trasmesso al Consiglio con la proposta di approvazione come Raccomandazione dello stesso Consiglio ed approvato da quest'ultimo il 17 marzo 1997.

La Raccomandazione in questione considera anzitutto che gli utilizzatori delle tecnologie dell'informazione devono avere fiducia nella sicurezza delle infrastrutture, delle reti e dei sistemi d'informazione e di comunicazione ed inoltre nella riservatezza, integrità e disponibilità dei dati di questi sistemi così come nella possibilità di provare l'origine e la ricezione dei dati; rileva inoltre che il fatto di assicurare la sicurezza dei dati mediante l'opera della legislazione, della procedura e della tecnica riveste una importanza fondamentale per le infrastrutture nazionali ed internazionali dell'in-

formazione. Essa riconosce poi che la crittografia ha diverse applicazioni legate alla protezione della vita privata, della proprietà intellettuale, delle informazioni commerciali e finanziarie, della sicurezza pubblica e della sicurezza nazionale, così come nella pratica del commercio elettronico, specialmente per le transazioni ed i pagamenti anonimi sicuri, ed afferma che il fatto di non utilizzare i metodi crittografici può nuocere alla protezione della vita privata, della proprietà intellettuale e degli altri settori sopracitati. Esaminando poi il ruolo e la responsabilità dei Governi nella particolare materia, la Raccomandazione in questione rileva inoltre che esistono per i Governi stessi, le imprese ed i singoli individui, dei bisogni e degli usi legittimi della crittografia ma che la crittografia può essere anche utilizzata da persone fisiche o giuridiche per condurre delle attività illegali che possono mettere in pericolo la sicurezza pubblica, quella nazionale, il rispetto delle leggi, l'attività commerciale, la vita privata e la protezione del consumatore, per cui i Governi, in collaborazione con l'industria e con il settore pubblico, devono elaborare una politica che concili questi vari interessi.

La Raccomandazione conclude rivolgendosi agli Stati membri e raccomanda loro di adottare delle politiche, metodi, misure, e nuove procedure o di modificarle, se del caso, in modo da riflettere i principi relativi alla politica della crittografia, come indicati nelle linee direttrici annesse alla Raccomandazione, tenendo anche in considerazione, le altre Raccomandazioni del Consiglio in tema di protezione della vita privata e di sicurezza dei sistemi d'informazione.

I principi enunciati nelle linee direttrici sono otto e riguardano, rispettivamente: 1) la fiducia nei metodi crittografici; 2) la scelta dei metodi crittografici; 3) lo sviluppo dei metodi crittografici guidato dal mercato; 4) le norme tecniche applicate ai metodi crittografici; 5) la protezione della vita privata e dei dati di carattere penale; 6) l'accesso legale; 7) la responsabilità; 8) la cooperazione internazionale.

In questa relazione, tratterò brevemente, in quanto più vicini al tema della relazione stessa, i principi nn. 5, 6, 7 ed 8.

Il principio relativo alla protezione della vita privata e dei dati a carattere personale afferma che « *i diritti fondamentali degli individui al rispetto della loro vita privata, specialmente al segreto delle comunicazioni ed alla protezione dei dati di carattere personale, dovranno essere rispettati nelle politiche nazionali nei riguardi della crittografia e nella messa in opera e nelle utilizzazioni dei metodi crittografici* ».

Il principio relativo all'accesso legale, a sua volta, afferma che le politiche nazionali nei riguardi della crittografia possono autorizzare l'accesso legale ai testi in chiaro o alle chiavi crittografiche dei dati cifrati ma tali politiche devono rispettare nella misura del possibile gli altri principi enunciati nelle linee direttive. È da dire

che la questione dell'accesso legale è trattato nelle linee direttive con molta prudenza. Si dice anzitutto che il principio in questione non dovrà essere interpretato come implicante che i Governi dovranno o non dovranno promulgare una legislazione che autorizzi l'accesso legale ma soltanto che i Governi, nell'affrontare tale problema, devono valutare i vantaggi e gli svantaggi di eventuali decisioni al riguardo.

Le linee direttrici sul punto sono molto chiare in ordine alle autorizzazioni ed alle modalità dell'accesso, affermando, tra l'altro, che:

1) quando l'accesso legale è richiesto, la persona o l'organizzazione deve essere giuridicamente autorizzata ad entrare in possesso del testo in chiaro e che, una volta ottenuti i dati, questi devono essere utilizzati soltanto per scopi leciti;

2) le modalità di accesso legale dovranno essere enunciate chiaramente e pubblicate in modo che siano agevolmente disponibili per gli utilizzatori, detentori delle chiavi e fornitori di metodi crittografici;

3) le procedure di accesso legale alle chiavi crittografiche devono tener conto della distinzione tra le chiavi che possono essere utilizzate per proteggere la riservatezza e quelle che sono utilizzate esclusivamente per altri fini. Una chiave crittografica che fornisce unicamente l'identità o assicura l'integrità (per contrasto ad una chiave che unicamente *verifica* l'identità o l'integrità) non dovrà essere consegnata senza il consenso della persona o dell'entità che è in possesso legale di questa chiave.

Il principio della responsabilità afferma che le responsabilità delle persone e delle entità che offrono dei servizi crittografici o detengono delle chiavi crittografiche per conto di altri o hanno accesso a chiavi crittografiche altrui, devono essere chiaramente enunciate, sia che siano stabilite per contratto che in via normativa.

Ed infine, il principio della cooperazione internazionale stabilisce che i Governi dovranno cooperare allo scopo di coordinare le loro politiche nei riguardi della crittografia. Nel quadro di questo sforzo, i Governi dovranno vegliare allo scopo di evitare di creare, in nome di una politica della crittografia, degli ostacoli agli scambi.

Nel commento al principio si afferma, tra l'altro, che l'accesso legale al di là delle frontiere nazionali potrà essere realizzato mediante una cooperazione e degli accordi sul piano bilaterale e multilaterale.

3. Le iniziative della CEE e del Consiglio d'Europa.

A sua volta, la Comunità Economica Europea sta elaborando proprie regolamentazioni in materia di crittografia, impegnando

ben quattro Direzioni Generali della Commissione: in particolare, la Direzione XIII sta preparando uno schema di proposta sul ETPS (*European Trusted Party Services*) allo scopo di creare una infrastruttura per la gestione delle chiavi (pubbliche) crittografiche che permettano l'accesso alle informazioni nel settore privato.

Nell'ambito della Commissione agisce anche il Gruppo SOGIS (Gruppo degli Alti Funzionari per la Sicurezza delle Informazioni), che ha elaborato alla fine del 1993 il « *Green Book on the Security of International Systems* », nel quale vengono esaminati gli argomenti relativi all'uso della crittografia ed alla autentificazione dei documenti elettronici, nonché ai ruoli degli utenti e dei *managers* della sicurezza ed alla creazione di un organo denominato TTPS (*Trusted Third Parties*).

Anche il Consiglio d'Europa si è occupato in un recente passato di alcuni problemi giuridici relativi all'uso della crittografia nella Raccomandazione n. R(95)13, elaborata da un Comitato ristretto di esperti sui problemi della procedura penale legati alla tecnologia dell'informazione, approvata dal Comitato dei Ministri nel settembre 1995. Il Capitolo V della sopracitata Raccomandazione tratta della utilizzazione della crittografia enunciando il principio n. 14, secondo cui « *delle misure dovranno essere esaminate al fine di minimizzare gli effetti negativi della utilizzazione della crittografia sulle inchieste nel campo penale, senza tuttavia avere conseguenze non strettamente necessarie sulla sua utilizzazione legale* ». Nel commento che accompagna il citato principio si conclude affermando che « *il conflitto di interessi tra il bisogno degli utilizzatori ed il rispetto della legge deve essere convenientemente preso in considerazione e deve essere trovato un equilibrio* ».

L'argomento relativo all'uso della crittografia sarà, peraltro, nuovamente esaminato nel corso dei lavori del nuovo Comitato del Consiglio d'Europa incaricato di elaborare una Convenzione per combattere la criminalità nel « *cyberspace* ».

4. Le iniziative delle Organizzazioni internazionali del settore privato.

Anche il settore privato ha esaminato il problema, elaborando un certo numero di prese di posizione e di dichiarazioni sull'argomento.

Nel 1990 la Camera di Commercio Internazionale, che rappresenta gli interessi delle imprese in più di 110 Paesi del mondo, ha pubblicato una presa di posizione intitolata « *La sicurezza delle reti: il punto di vista dei settori privati internazionali* », nella quale, tra l'altro, si raccomandava l'adozione di accordi internazionali nel settore della legislazione, della giurisdizione e della nor-

malizzazione al fine di attuare un ambiente favorevole alla sicurezza delle comunicazioni informatiche.

Nel 1991 è stato creato l'IBAG (*Infosec Business Advisory Group*), che raggruppa le associazioni europee rappresentanti degli utilizzatori, dei venditori e degli organismi di normalizzazione, il cui scopo è quello di far sentire la sua voce in tema di tecnologia dell'informazione a livello della CEE e sul piano internazionale.

L'Organizzazione in questione ha pubblicato nel 1993 uno studio (*Framework for Commercial it Security*) col quale si raccomandava la semplificazione e l'armonizzazione delle regolamentazioni relative alla importazione, esportazione ed utilizzazione dei metodi di crittografia a fini commerciali.

La Camera di Commercio Internazionale nel maggio 1994 ha, infine, pubblicato una presa di posizione sulla politica internazionale della crittografia. A proposito della prevenzione dei delitti, la C.C.I. riconosce che l'industria è cosciente della necessità di combattere le attività delittuose o criminali ma afferma che tutte le procedure che autorizzano la decifratura da parte delle autorità devono essere chiaramente e strettamente definite dalla legge e devono essere gestite da un tribunale o da un altro organo giuridico equivalente.

Il documento della C.C.I. conclude facendo appello ai Governi affinché:

a) eliminino gli ostacoli al commercio e le restrizioni gravanti sulla utilizzazione dei metodi di crittografia disponibili sul mercato;

b) collaborino con l'industria nell'eliminare questi ostacoli elaborando una politica internazionale completa della crittografia.

Una decisa presa di posizione della predetta C.C.I. è quella contenuta nella dichiarazione della stessa C.C.I. sulla infrastruttura mondiale della informazione pubblicata in occasione della Conferenza mondiale del G7 sulla società dell'informazione (25-26 febbraio 1995) nella quale si chiede esplicitamente l'eliminazione delle barriere al commercio e degli ostacoli alla utilizzazione dei metodi di cifratura disponibili nel settore del commercio, eliminando i controlli — definiti inutili — all'esportazione ed alla importazione, in modo da assicurare al massimo la libertà di scelta da parte degli utenti.

Nell'ottobre del 1994 l'U.S. Council (*Council for International Business*), che rappresenta il punto di vista delle società multinazionali americane, ha pubblicato la sua posizione sui bisogni delle imprese in tema di crittografia. Tra l'altro, l'U.S. Council ha raccomandato la eliminazione dei controlli sulla crittografia commerciale e la creazione di una politica internazionalmente accettabile in tema di crittografia.

La necessità di adottare una politica internazionale nel settore in questione è stata inoltre sostenuta dalle tre maggiori associa-

zioni mondiali nel settore delle tecnologie dell'informazione e cioè l'Associazione Europea dei Costruttori di Macchine per Ufficio e per l'Informatica (EUROBIT), l'Industria della Information Technology (IIT) e l'Associazione Giapponese per lo Sviluppo dell'Industria Elettronica (JEIDA), rivolgendo apposite raccomandazioni al Summit del G7 del febbraio 1995 ed affermando, tra l'altro, « ... l'infrastruttura dell'informazione implica necessariamente il sostegno implicito generalizzato della tecnologia della crittografia. Senza una larga diffusione di questa tecnologia, la protezione della vita privata e la fiducia non potranno essere assicurate. La crittografia è indispensabile per la riservatezza e per integrità della informazione, specialmente allorché si tratta di confermare la sua esattezza e le firme elettroniche... ».

Infine, di recente (dicembre 1995), si è tenuto a Parigi, sotto l'egida dell'OCSE, un Forum « *Governi - Settore privato sulla politica mondiale della crittografia* », organizzato dalla CCI e dal BIAC, nel quale sono intervenuti rappresentanti del settore pubblico e rappresentanti del settore privato.

5. La situazione in alcuni Paesi esteri.

L'unico Paese europeo che allo stato ha regolamentato l'uso della crittografia è la Francia, paese nel quale la fornitura, l'esportazione e la utilizzazione dei sistemi crittografici sono previste all'art. 28 della legge n. 90.1170 del 29 dicembre 1990 e regolamenti connessi.

La legislazione citata prevede l'obbligo della semplice dichiarazione preventiva di fornitura o di utilizzazione allorché il sistema abbia per oggetto la sola autenticazione delle comunicazioni o l'integrità del messaggio trasmesso. Negli altri casi è richiesta, invece, una procedura di autorizzazione da rilasciarsi dal Primo Ministro.

È interessante notare che un *Arreté* del 28 dicembre 1992 ha previsto espressamente che il fornitore delle prestazioni è tenuto a dichiarare alla autorità di polizia giudiziaria territorialmente competente gli accessi illeciti al sistema di gestione o gli attentati alla sicurezza del sistema stesso dei quali ha avuto conoscenza e di informare anche il Servizio Centrale di Sicurezza dei Sistemi d'Informazione.

È da rilevare peraltro che il regime di cui sopra è stato in parte liberalizzato da una successiva legge, la n. 96-659 del 26 luglio 1996, che, tra l'altro, ha reso libero l'uso dei sistemi crittografici ai fini di autentificazione o di integrità del messaggio trasmesso o se il mezzo o la protezione di crittografia assicuri funzioni di riservatezza, ed utilizzi soltanto delle convenzioni segrete, gestite secondo le procedure e da un organismo autorizzato

in base a condizioni previste nella stessa legge, dal Primo Ministro.

È nota la situazione creatasi negli Stati Uniti a proposito della cosiddetta Direttiva Clinton. Com'è noto, tale direttiva prevedeva due punti e cioè una restrizione all'esportazione di sistemi crittografici che la *National Securiy Agency* non era in grado di intercettare e decodificare e la introduzione nei sistemi informatici crittografici di due particolari *chip* basati all'algorigmo SKIPJACK, denominati, rispettivamente, *Clipper* e *Capstone*, a seconda che riguardino sistemi vocali o di trasmissioni di dati, ideati dalla NSA, che contenevano un « *built-in electronic back-door* » in modo da consentire alle Agenzie governative, debitamente autorizzate dalle autorità giudiziarie, di intercettare qualsiasi comunicazione.

La codificazione e decodificazione doveva avvenire mediante due chiavi, una della quali avrebbe dovuto essere depositata presso il *National Institute of Technology and Standards* e l'altra presso il *Treasury Department*. Tali agenzie avrebbero dovuto consegnare le chiavi, detenute rispettivamente, alle Agenzie del *Law Enforcement* ma soltanto a seguito della esibizione di un ordine emesso da una Corte.

Va subito detto che la direttiva in questione ha suscitato vivaci proteste e ciò per moviti diversi da parte dell'industria informatica e da parte delle Associazioni per la tutela delle libertà civili, e per il momento sembra sia stata accantonata. Va detta ora che negli Stati Uniti l'esportazione di sistemi crittografici è sottoposto al controllo governativo in base all'*Arms Export Control Act* ed al *International Traffic in Arms Regulations*.

Coloro che pubblicano lavori che forniscono elementi per la elaborazione di sistemi crittografici relativi ai dati possono essere accusati di esportazione illegale di *armi* se i supporti relativi sono accessibili agli stranieri, come nel caso di pubblicazioni diffuse su reti informatiche. Vi sono state varie reazioni sul piano giudiziario anche da parte di comunità scientifiche che protestavano contro gli ostacoli all'insegnamento ed alla ricerca.

6. La situazione in Italia.

In Italia, a livello normativo, non sembrano esistere particolari disposizioni in ordine all'uso della crittografia, all'infuori di quelle riguardanti il particolare settore della tutela del segreto di Stato e delle informazioni di cui è vietata la divulgazione e di cui agli artt. 12 e 24 della legge 24 ottobre 1977, n. 801.

Altre disposizioni sono contenute nel complesso di norme che riguardano il controllo, l'esportazione, l'importazione ed il transito dei materiali di armamento nonché l'esportazione e transito di materiali di particolare interesse strategico (legge 8 luglio 1990, n. 185, legge 27 febbraio 1992, n. 222 ed i relativi decreti ministeriali

del 28 ottobre 1993, 18 novembre 1993, 5 maggio 1994, 1° settembre 1995)[2].

Un accenno all'uso delle tecniche crittografiche nel campo della Pubblica Amministrazione è contenuto in alcune deliberazioni (vedi quella del 28 luglio 1994, art. 1, n. 9) dell'AIPA (Autorità per l'Informatica della Pubblica Amministrazione), istituita con decreto legislativo del 12 febbraio 1993, n. 39. Tale deliberazione, all'art. 9, stabiliva che sarebbero stati regolati con successivi provvedimenti legislativi gli aspetti, tra gli altri, relativi all'uso della crittografia, alla protezione e alla conservazione delle relative chiavi, all'uso dei meccanismi di firma elettronica.

La Deliberazione di cui sopra prevede anche che per ogni *file* memorizzato sul disco ottico, dovranno tra l'altro, essere introdotte, con modalità che saranno di seguito precisate, eventuali informazioni in ordine alla crittografia.

Nelle note esplicative allegate alla sopracitata Deliberazione, relativa alle specifiche tecniche per l'uso dei supporti ottici, si dice, al paragrafo 3/I, relativamente all'aspetto della sicurezza, che « per ragioni di riservatezza deve essere ammesso l'uso della crittografia nella conservazione delle informazioni su disco: ma in tal caso occorre che l'algoritmo di crittografia sia normalizzato e che siano regolamentate anche le procedure di formazione e di conservazione delle parole-chiavi individuali e relative responsabilità[3].

---

[2] Rimando per questo al mio articolo dal titolo « Riflessi normativi sull'uso dei sistemi crittografici in Italia », pubblicato nella rivista « *Per aspera ad veritatem* » n. 4/1996, p. 55 e segg.

Vedi anche in argomento il D.L. 24 febbraio 1997 n. 89, emesso in attuazione del Regolamento CEE n. 3381/94 e della Decisione n. 94/942/PESC, sulla esportazione di beni a duplice uso.

[3] In realtà, un tentativo di regolamentare in generale l'uso di sistemi di criptofonia e crittografia venne compiuto in passato dal Ministro dell'Interno, il quale presentò al Senato, nella X legislatura, un disegno di legge (il n. 3232 dell'11 febbraio 1992) che prevedeva disposizioni (anche) in tema di apparecchiature criptofoniche ovvero destinate alla trasmissione in codice di comunicazioni telefoniche, radiofoniche o di altre forme di telecomunicazioni.

L'art. 1 del disegno subordinava a licenza del Questore la produzione, l'introduzione nello Stato, l'esportazione, la raccolta per ragioni di commercio o di industria e la messa in vendita, tra l'altro, di apparecchiature per la ricetrasmissione in codice e per la codificazione di telecomunicazioni. L'art. 3 disciplinava, in particolare, la materia degli apparecchi di comunicazione in codice prevedendo che il produttore o importatore di dette apparecchiature dovesse depositare presso il Ministero delle PP.TT. i dati e gli apparati necessari per la decodificazione delle comunicazioni: ciò ai fini dell'intercettazione investigativa. Veniva stabilito anche il divieto di vendita o di cessione, anche a tempo determinato, delle apparecchiature a soggetti privi del *nulla osta* all'acquisto ed all'uso rilasciato dal Questore, *nulla osta* soggetto a precisi limiti temporali; inoltre i detentori delle apparecchiature avrebbero immediatamente dovuto denunziare il possesso e le variazioni alle Forze di polizia: tutti i divieti e gli obblighi di cui sopra erano rafforzati da sanzioni penali.

Il disegno di legge in questione decadde con lo scioglimento delle Camere. Tuttavia, lo stesso Ministero dell'Interno, nel corso della successiva legislatura, preparò una versione lievemente modificata del testo precedente, che però non venne mai trasfuso in un disegno di legge.

Di crittografia si parla anche nello studio di fattibilità relativo alla rete unitaria della Pubblica Amministrazione, prevista dalla Direttiva del Presidente del Consiglio dei Ministri del 5 settembre 1995 (*G.U.* n. 272 del 21 novembre 1995).

In tale studio di ampio respiro si afferma, tra l'altro, che nella rete unitaria della P.A. la sicurezza sarà gestita per « domini » ... Per garantire origine, contenuto, riservatezza e non ripudio dei messaggi scambiati fra « domini » si adotteranno strumenti *software* a livello applicativo basati sull'impiego della crittografia a chiave simmetrica e/o a chiave pubblica. La gestione delle chiavi crittografiche sarà curata da un organismo da creare alle dirette dipendenze della Presidenza del Consiglio dei Ministri, composto da tre funzionari distinti per la:

1) creazione e distribuzione delle chiavi, ospitato dal Centro di Servizio;

2) gestione del notariato, ospitata dal Centro Operativo;

3) certificazione delle chiavi, ospitato dall'Autorità per l'Informatica.

In ogni caso — conclude lo studio sul punto — i mezzi tecnici necessari alla gestione delle chiavi crittografiche faranno parte della dotazione del Centro Tecnico di Assistenza che ne curerà anche la gestione dal punto di vista tecnico.

Richiami all'uso della firma elettronica (che assicura l'integrità dei dati e la sicurezza dell'origine del messaggio) ed alla crittografia a chiave (che garantisce la segretezza dei dati) sono contenuti in studi particolari allegati alla relazione generale.

Alla fine del 1995 l'AIPA ha esaminato una bozza di articolato concernente gli atti ed i documenti in forma elettronica in attuazione dell'art. 3 del D.L. n. 39 del 14 febbraio 1993, frutto delle riflessioni di un gruppo di studio, e ne ha disposto la diffusione sulla rete Internet al fine di acquisire ogni possibile contributo di riflessione.

Lo studio in questione esamina anche l'argomento relativo alle chiavi crittografiche (gestione, archivio, ecc.). Ed infine, sempre l'AIPA, ha elaborato, nel novembre 1996, un documento intitolato « Rete dei Gabinetti e dei Responsabili dei sistemi informativi automatizzati » che esamina anche il problema della sicurezza delle reti e dell'utilizzo della crittografia.

Va rilevato per inciso che un importante riconoscimento della legittimità dei documenti informatici è contenuto nella recentissima legge 15 marzo 1997, n. 52 (Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione aministrativa) il cui art. 15, secondo comma, prevede che « ... gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici e telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e tra-

smissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge »[4].

Ed infine, in tema di sicurezza, va ricordato l'art. 15 della legge 31 dicembre 1996, n. 675 (Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali) che tratta il problema della sicurezza dei dati. Il secondo comma dell'articolo in questione, prevede che le misure minime di sicurezza da adottare in via preventiva (tra cui evidentemente anche quelle crittografiche) verranno indicate con regolamento emanato con Decreto del Presidente della Repubblica, su proposto del Ministro di Grazia e Giustizia, sentiti l'AIPA ed il Garante.

Rilevo per inciso che il testo dell'art. 15 della legge n. 675 è in parte diverso da quello contenuto nell'originario disegno di legge che prevedeva per la proposta il concerto tra il Ministro della Giustizia ed i Ministri dell'Industria e delle PPTT, escludendo, quindi, sia l'AIPA che il Garante.

Tuttavia il testo dell'articolo pur così modificato, presta il fianco a varie critiche. Anzitutto non si vede quale competenza specifica abbia il Ministero della Giustizia in tema così tecnico come quello della individuazione delle misure di sicurezza e come mai sia stato escluso proprio l'organo tecnico costituito dal Ministero delle PPTT (ora delle comunicazioni).

A mio avviso, e ripeto ciò che ho detto più volte in questi anni, l'unico organo competente istituzionalmente ad individuare le misure di sicurezza era e rimane l'AIPA, alla quale spetta il compito esclusivo di dettare i criteri tecnici di sicurezza nell'ambito pubblico (art. 7, comma 1, lett. *a*) del D.L. n. 39 del 12 febbraio 1993: vedi anche l'art. 7, n. 1 del D.P.R. n. 680 dell'11 novembre 1994). Ribadisco quindi quanto da me dichiarato in varie occasioni e cioè che le indicazioni dei criteri tecnici di sicurezza dei dati, anche personali, contenuti nei sistemi informativi pubblici *non possono non spettare all'AIPA* quale organo indipendente, che, salve le eccezioni di cui all'art. 16, n. 2 del D.Lgs. n. 39 del 12 febbraio 1993, dovrebbe sovrintendere a tutta la materia della sicurezza informatica pubblica. È assolutamente indispensabile, a mio avviso, e risponde ad elementari criteri di razionalità, che vi sia una *unica autorità nazionale*, investita del compito di provvedere in tema di sicurezza dei sistemi informativi pubblici, eventualmente con qualche motivata esclusione per particolari sistemi.

---

[4] Il Regolamento previsto dal citato art. 15 comma 2 è stato approvato dal Consiglio dei Ministri nella seduta del 5 agosto 1997 ed è in corso di pubblicazione. Esso detta particolari norme in tema di documento elettrico, di uso della crittografia e di firma digitale.

7. Considerazioni conclusive.

In questo settore vi è indubbio conflitto tra la esigenza di tutela della collettività nei confronti nell'uso illecito delle tecniche crittografiche particolarmente da parte di organizzazioni criminali e quella della tutela della « privacy » degli individui. Come è stato rilevato dal dott. Meillan, consulente del Comitato Ristretto del Consiglio d'Europa sui problemi di diritto procedurale legati alla tecnologia dell'informazione, nel corso dei lavori del Comitato ristretto del Consiglio d'Europa per gli aspetti processuali della lotta alla criminalità informatica, l'uso dei sistemi crittografici restringe grandemente le possibilità di investigazione se la persona indagata è quella che detiene le chiavi della cifratura utilizzata, giacché essa non può essere costretta a rivelarle.

Esiste, occorre ricordarlo, una indubbia sotterranea riluttanza sia da parte dei Governi che da parte dei privati ad affrontare l'argomento della disciplina della crittografia. I problemi, quindi, sono numerosi sia sul piano nazionale che su quello internazionale ma potrebbero essere risolti con il ricorso a criteri tecnici adeguati, anche se i rischi rimarrebbero considerevoli.

In effetti, bisogna ricordare che, come rilevato dal Progetto di Rapporto preparato dall'OCSE in tema di infrastruttura globale dell'informazione (doc. DSTI-ICCP-(96)3-Rv3), queste questioni, come quelle relative alla sicurezza della vita privata ed alla protezione dei diritti di proprietà intellettuali, rischiano considerevolmente di rallentare o di perturbare l'apparizione della società mondiale dell'informazione. Le preoccupazioni del settore pubblico è di quello privato riguardano anche l'utilizzazione della crittografia a livello internazionale ...

Tuttavia bisogna riconoscere che la società della informazione è ormai una realtà ed essa ignora le frontiere ed i vincoli spaziali e temporali. In correlazione è aumentato il bisogno e la necessità da parte di singoli e delle organizzazioni sia pubbliche che private di proteggere la loro « privacy » ed i loro interessi, anche economici, mediante l'utilizzazione di tecniche crittografiche. Le esigenze del commercio elettronico, in particolare, e delle transazioni finanziarie e bancarie chiedono con urgenza l'eliminazione di restrizioni all'uso della critttografia.

Il compito di riportare tranquillità in questo delicato settore spetta, senza dubbio, ai Governi ed ai legislatori, in accordo, però, con le organizzazioni interessate. Probabilmente, a livello nazionale, occorrerebbe individuare una Autorità realmente indipendente, sia nel settore pubblico che in quello privato, alla quale affidare la creazione e la gestione delle chiavi crittografiche pubbliche e private, Autorità che però dovrebbe godere della fiducia illimitata da parte degli utenti ed essere al riparo dalle note lottizzazioni politiche... La legislazione dovrebbe poi prevedere e reprimere i possibili abusi quali, ad esempio, la rilevazione non auto-

rizzata delle *chiavi* affidate in deposito, l'uso non autorizzato delle stesse ed indicare, con la massima precisione, le condizioni nelle quali le chiavi depositate possono essere richieste ed acquisite nonché le relative rigorose cautele e le conseguenti responsabilità.

Restano comunque da risolvere i problemi di *standards* e di cooperazione internazionale ma questi potrebbero essere risolti mediante convenzioni bilaterali o multilaterali.

Per concludere, occorre comunque ricordare che l'adozione dei metodi o dei sistemi crittografici non rende assolutamente sicuro un sistema o una rete. È ancora vivo il ricordo tra gli specialisti del settore, del sistema gestito dalla macchina crittografica denominata ENIGMA, della quale si servivano le Forze dell'Asse durante il secondo conflitto mondiale e che, descrittato dagli alleati, consentì loro di compiere importanti operazioni militari.

La sicurezza assoluta è, quindi, soltanto un mito: non esiste!!!