Giovanni Ziccardi

Crittografia e diritto

Crittografia - suo utilizzo e disciplina giuridica - documento informatico e firma digitale - segretezza delle informazioni e sorveglianza globale

Introduzione di Andrea Monti

Giovanni Ziccardi

Crittografia e diritto

Crittografia - suo utilizzo e disciplina giuridica - documento informatico e firma digitale - segretezza delle informazioni e sorveglianza globale

Contributi di Valentina Apruzzi, Alessandro Arnone, Nicola Lucchi, Sarah Mosole, Alessandro Nori, Luciano Paglia, Pierluigi Perri, Elisa Tomasi.

Introduzione di Andrea Monti

Indice

8. Il valore giuridico del documento informatico.
9. La contestazione del documento informatico.

Capitolo Quarto

CRITTOGRAFIA E DIVIETI NELL'UTILIZZO DI PARTICOLARI TECNICHE DI SICUREZZA

1. Un primo inquadramento delle problematiche nel panorama mondiale.
2. Il COCOM, primi cenni.
3. Il *Wassenaar Arrangement*, primi cenni.
4. La situazione giuridica europea.
5. La situazione giuridica italiana.

Capitolo Quinto

CRITTOGRAFIA E QUADRO NORMATIVO

1. Le fonti sovranazionali: un'introduzione.
2. Aspetti giuridici del COCOM.
3. Aspetti giuridici del *Wassenar Arrangement*.
4. I principi fondamentali della Convenzione di Wassenaar.
5. Lo scambio delle informazioni.
6. I requisiti di ammissione.
7. L'Assemblea Plenaria del Dicembre 2001 e gli orientamenti attuali.
8. La *UN Security Council Resolution* n. 1373 del 2001.
9. La politica dell'OECD.
10. L'inventario dei controlli sulla crittografia messo a punto dall'OECD.

Capitolo Sesto

L'APPROCCIO NORMATIVO DEI SINGOLI ORDINAMENTI NAZIONALI

1. Gli Stati Uniti d'America.
2. Il caso Clipper.
3. La politica del *National Research Council*.
4. I tentativi di liberalizzazione.
5. L'*Electronic Data Security Act* del 1997.
6. L'attuale orientamento del governo americano.
7. Il *Computer Security Enhancement Act H.R. 1259*.
8. La politica dell'Unione Europea.
9. Il Regolamento del 1994.
10. La Decisione.
11. La Comunicazione del 1997.
12. L'attuale orientamento normativo comunitario.
13. La procedura per il rilascio dell'autorizzazione.

Capitolo Settimo

IL WASSENAAR ARRANGEMENT

Capitolo Ottavo

IL REGOLAMENTO N. 3381/94

Capitolo Nono

IL REGOLAMENTO N. 1334 DEL 2000

Capitolo Decimo

LA LEGGE 9 LUGLIO 1990, N. 185

Capitolo Undicesimo

CRITTOGRAFIA E FUNZIONI DELLA *NATIONAL SECURITY AGENCY*

Capitolo Dodicesimo

IL *CLIPPER CHIP*

PARTE TERZA - CRITTOGRAFIA E CASI GIUDIZIARI

Capitolo Tredicesimo

IL CASO DI DANIEL BERNSTEIN

Capitolo Quattrodicesimo

IL CASO DI PHIL ZIMMERMANN

Capitolo Quindicesimo

IL CASO DI DMITRY SKLYAROV

1. Il *Digital Millenium Copyright Act* e la crittografia
2. Il caso Sklyarov
3. Il DMCA in rapporto alla normativa europea: considerazioni.

Capitolo Sedicesimo

Il caso DeCSS

1. Introduzione.
2. I precedenti sulla legge sul diritto d'autore negli Stati Uniti d'America.
3. I recenti sviluppi nella vicenda Deccs: *DVD Copy Control Ass. v. Andrew Bunker*.
4. Conclusioni.

PARTE QUARTA - CRITTOGRAFIA, DIRITTI DI LIBERTA' E SORVEGLIANZA GLOBALE DELL'INDIVIDUO

Capitolo Diciassettesimo

CRITTOGRAFIA E SORVEGLIANZA GLOBALE

1. Il progetto *Platform*.
2. Le reazioni internazionali al caso Echelon: i rapporti del Parlamento Europeo.
3. Il Progetto P415.
4. Il sistema di intercettazione *Echelon*.
5. Echelon ed Internet: lo spionaggio della posta elettronica.
6. Dentro ad *Echelon*: il sistema dei 'dizionari'.
7. Il sistema dei 'dizionari' ed il controllo delle informazioni.
8. Il progetto Enfopol.

Capitolo Diciottesimo

CRITTOGRAFIA, SORVEGLIANZA GLOBALE E *PRIVACY*

1. Le accuse ad *Echelon*.
2. Echelon e *privacy* negli Stati Uniti d'America.
3. *Echelon* e l'Unione Europea.
4. La compatibilità tra *Echelon* e la legislazione dell'Unione Europea.
5. La Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali.

PARTE QUINTA - CRITTOGRAFIA, DIRITTO D'AUTORE E COMMERCIO ELETTRONICO

Capitolo Diciannovesimo

CRITTOGRAFIA E SISTEMI DI PROTEZIONE DEL DIRITTO D'AUTORE

Capitolo Ventesimo

CRITTOGRAFIA, DIRITTO D'AUTORE E COMMERCIO ELETTRONICO: I SISTEMI DI DIGITAL RIGHT MANAGEMENT

PARTE SESTA - CRITTOGRAFIA E SICUREZZA

Capitolo Ventunesimo

CRITTOGRAFIA E SICUREZZA

Capitolo Ventiduesimo

CRITTOGRAFIA E SICUREZZA DEI PROTOCOLLI DI RETE

1. Crittografia e protocolli di rete sicuri.
2. Protocollo IP (*Internet Protocol*) e sicurezza.
3. Crittografia e protocollo SSL (*Secure Socket Layer*).

Hanno contribuito alla redazione del Volume i dottori Valentina Apruzzi (Capitoli Quinto e Sesto), Alessandro Arnone (capitoli Trerdicesimo, Quattordicesimo e Quindicesimo), Nicola Lucchi (Capitolo Sedicesimo), Sarah Mosole (capitoli Diciannovesimo e Ventesimo), Alessandro Nori (capitoli Undicesimo, Dodicesimo, Diciassettesimo e Diciottesimo), Luciano Paglia (capitolo Ventunesimo), Pierluigi Perri (capitoli Quarto e Ventiduesimo), Elisa Tomasi (capitolo Terzo).

Giovanni Ziccardi è Professore Associato di Informatica Giuridica presso la Facoltà di Giurisprudenza dell'Università Statale di Milano. Avvocato, pubblicista e saggista, è Autore di decine di pubblicazioni in tema di diritto e nuove tecnologie e di un Romanzo, 'Occhi nella Rete' (Modena, 1999). Direttore della Rivista Scientifica 'Ciberspazio e Diritto', è Chairman della Italian Cyberspace Law Conference.

Alla piccola Sofia. Che la vita ti sorrida.

"Stella mi disse di aver capito in quel momento che in ciascuno di noi
c'è come l'anelito a gridare al mondo la verità, a qualsiasi costo.
O a distruggersi."

Patrick McGrath, *Follia*, Adelphi, Milano, 1998, p. 65.

Introduzione

Quando l'amico Giovanni Ziccardi mi ha chiesto di scrivere l'introduzione alla sua ultima fatica scientifica sono stato, nello stesso tempo, onorato per la scelta e preoccupato per l'impegno che mi si chiedeva di assumere.
L'oggetto della ricerca, lo studio dei rapporti fra crittografia e diritto è, infatti, un tema tanto 'gettonato', quanto 'maltrattato' dalla letteratura giuridica italiana, che se ne occupa spesso – non sempre, per la verità – in modo superficiale e tecnicamente poco avvertito (basti pensare al diffuso errore concettuale di chi, occupandosi di firma digitale, si ostina a pensare che il documento informatico sia cifrato). In breve: siamo di fronte a un esercito di archeologi che non ha mai visto uno scavo.
Non è questo il caso del Volume che avete fra le mani che, al contrario, si caratterizza per rigore scientifico e analisi delle fonti.
Invece di 'ispirarsi' ad autori che citano autori, Giovanni Ziccardi si rivolge direttamente a chi – a vario titolo – è stato effettivamente coinvolto nelle vicende documentate nel testo. Come dimostra la bibliografia che, pur tenendo conto di quanto pubblicato in Italia, evidenzia numerosissimi elementi di novità. Non stupirebbe, fra qualche tempo, trovare gli stessi titoli "citati autonomamente" a piene mani nelle prossime pubblicazioni.
Ciò premesso, parliamo dei contenuti.
La prima parte analizza sotto un profilo squisitamente politico la nascita e l'evoluzione della *quaestio* crittografica per poi passare alla disamina degli aspetti tecnici e definitori della materia. Segue l'analisi della (purtroppo prevedibilmente) confusa situazione normativa italiana sulla firma digitale e sul documento informatico, per poi "aprirsi" al panorama internazionale con il dotto *excursus* relativo al trattato di Wassenaar e alla struttura, ruolo e funzione politico giuridica della statunitense *National Security Agency* (di fatto, il controllore più o meno occulto dell'evoluzione normativa che coinvolge la crittografia).
Per non lasciare nel lettore una sensazione di astrattezza e, tutto sommato, di "alterità" della materia, la terza parte – forse la più interessante – è dedicata alla ricognizione di alcune vicende giudiziarie statunitensi che sono diventate dei veri e propri l*eading cases* e che affrontano, da varie angolazioni, il rapporto tra i diritti civili e il potere dello Stato.
Così, il caso del Dr. Bernestein, un matematico accusato di avere violato la normativa sulla esportazione di crittografia per avere discusso in Rete i contenuti di un sistema di cifratura elaborato dallo stesso, evidenzia il serio problema delle inaccettabili limitazioni alla libertà della ricerca scientifica da parte dello Stato
La vicenda di Phil Zimmermann, invece, prima tratto a giudizio per avere messo a disposizione dei cittadini un robusto *software* crittografico (PGP) e, poi, liberato da ogni accusa (grazie anche, si dice, al non indifferente peso politico del MIT), enuncia nitidamente il tema, di sicuro interesse per i cultori del

diritto costituzionale, del difficile bilanciamento fra il diritto dell'individuo a proteggere la propria riservatezza e quello dello Stato a tutelare gli interessi della collettività. Il nocciolo della questione è, in primo luogo, se al cittadino deva essere consentito l'impiego di strumenti crittografici (la risposta non è affatto scontata visto che in Francia, per molti anni, la crittografia era regolamentata in modo estremamente rigoroso e penalizzante per i "citoyen"). E in secondo luogo, decidere quanto robusti (cioè resistenti a tentativi di effrazione) questi sistemi dovrebbero essere. Orbene: PGP è un *software* tuttora considerato estremamente refrattario alla crittanalisi e l'averlo reso disponibile anche al di fuori dei confini statunitensi (questa l'accusa contro Zimmermann) metteva in pericolo gli interessi della nazione. Grazie a PGP, infatti, le attività di intercettazione e di indagine delle tante *law enforcement agency* americane sarebbero state grandemente pregiudicate. Ma è veramente accettabile una tesi del genere?

Sospesa la risposta, passiamo alla vicenda di Dmitry Sklyarov, accusato di avere elaborato un sistema per aggirare le protezioni crittografiche degli *e-book* (i libri elettronici) prodotti dalla Adobe (notissima azienda che opera nel settore della grafica computerizzata). Qui si discute se l'autore abbia o meno il diritto di limitare arbitrariamente le modalità di fruizione dell'opera tutelata (anche tramite strumenti crittografici) a chi ne abbia legittimamente acquistato l'uso. Come si vedrà, passando dalla teoria alla pratica la risposta è tutt'altro che scontata.

Chiude la rassegna il caso DeCSS (il sistema che consente la regionalizzazione dei DVD), veramente esemplare dell'ampiezza dei problemi giuridici legati all'uso della crittografia. Sotto accusa è un programmatore svedese colpevole – si dice - di avere aggirato queste protezioni per realizzare un *software* per la lettura dei DVD funzionante con il sistema operativo Linux. Le questioni sul tappeto (a parte quella sulla giurisdizione) riguardano innanzi tutto la protezione del diritto all'indipendenza della ricerca scientifica (che non è tale solo quando si svolge nei "santuari" istituzionali o aziendali) e, quindi il diritto (articolazione della libertà di espressione) di scambiare liberamente informazioni tecniche quando lo scopo non è delittuoso.

L'indagine casistica non si ferma, però, alle vicende giudiziarie e continua ricostruendo quelle che hanno caratterizzato la scoperta del sistema di intercettazione globale chiamato *Echelon* e la costituzione di un omologo europeo di nome *Enfopol*. Alla ricognizione fattuale si affianca – inoltre – quella normativa, con l'analisi della compatibilità di questi strumenti con l'ordinamento giuridico europeo e internazionale a salvaguardia dei diritti dell'uomo.

Chiudono il ponderoso lavoro i capitoli sul rapporto fra crittografia, diritto d'autore e commercio elettronico e quelli dedicati alla sicurezza informatica.

La vastità dei temi trattati – caso abbastanza raro nei libri di diritto - non inficia la fruizione e anche gli argomenti più eterogenei si reggono grazie a salde strutture d'assieme che guidano il lettore attraverso percorsi altrimenti capaci di disorientare.

Potranno giovarsi della consultazione di questo volume il cultore di diritto (non solo) costituzionale che troverà enunciati in termini rigorosi i problemi

più attuali legati alle molteplici applicazioni della crittografia. Gli operatori del diritto (avvocati o magistrati) che dovessero trattare, nella quotidianità del foro, casi giudiziari relativi a queste materie. E infine – *last but not least* – gli studenti che potranno mettere alla prova, leggendo questo volume, le cognizioni acquisite nel corso degli studi giuridici.
Il consiglio finale è di comprarne più di una copia. La continua consultazione, infatti, porterà velocemente alla consunzione delle pagine.

Pescara, 10 settembre 2002

Andrea Monti – amonti@unich.it

PARTE PRIMA

LE PROBLEMATICHE

Capitolo Primo

IL CONTROLLO DELLA TECNOLOGIA CRITTOGRAFICA E DELLA SUA ESPORTAZIONE

SOMMARIO: 1. Le problematiche. – 2. I settori d'impiego della crittografia e gli utilizzatori della stessa. – 3. La 'crypto controversy'. – 4. Il rapporto tra industria e Governo. – 5. La tutela della *privacy* delle comunicazioni e dei dati dell'individuo. – 6. Le fasi di sviluppo della politica crittografica. – 7. Il controllo delle esportazioni di tecnologia crittografica. – 8. L'evoluzione della qualificazione dei prodotti crittografici. – 9. L'alleggerimento dei controlli. – 10. Accordi sulla politica crittografica, azioni legislative e politiche. – 11. La politica crittografica in Italia e l'Aipa.

1. Le problematiche.

Uno degli effetti immediati della nascita della nuova società dell'informazione e della sua diffusione su scala mondiale – intendendo come 'nuova società dell'informazione' quell'insieme di tecnologie informatiche e telematiche, aziende e persone che le utilizzano – è stato quello di fare in modo che sempre più persone si affidassero all'*informazione* e, soprattutto, confidassero in questa in tutti i suoi aspetti.

L'informazione è diventata, allora, il centro dell'attività lavorativa, dell'*entertainment*, della vita quotidiana, ed è venuta a costituire un elemento essenziale ed imprescindibile per la vita della società stessa.

Questa centralità dell'informazione anche in settori 'delicati' da un punto di vista giuridico – si pensi al settore pubblico, non solo nei rapporti coi privati e col cittadino ma, anche, nel rapporto tra pubblico e pubblico - ha ben presto sollevato problemi di sicurezza.

Si parla, nel mondo tecnologico, di *information, computer and network security*: in poche parole, sicurezza (ovvero, in estrema sintesi: confidenzialità, integrità e disponibilità) dell'informazione, dei computer e delle reti che trasportano l'informazione stessa. Sicurezza intesa, soprattutto, come salvaguardia da

possibili effetti esterni che possano compromettere l'essenza dell'informazione stessa[1].
L'*information security* è diventata materia di studio anche per i giuristi: viene studiata nella *computer and network forensics*, nell'analisi della tutela della *privacy*, nel diritto penale dell'informatica, nella contrattualistica.
Di questa vasta area di studio che è l'*information security*, la crittografia – che possiamo definire, *in primis*, come "l'arte e la scienza delle scritture segrete", ha assunto un ruolo centrale, quasi vitale[2].
La crittografia, in sé, non è una scienza nuova, anzi. È antica come l'arte stessa di scrivere, è utilizzata da secoli come mezzo per tenere segrete le comunicazioni, ha visto grande fortuna nel settore dell'*intelligence*, nella diplomazia, in periodo di guerra.
Quello che però interessa, in questo Volume, è quella parte della 'vita' della crittografia che si è unita e fusa alle nuove tecnologie.
Sono molti gli studiosi che vedono l'inizio di una 'nuova era' nelle scritture segrete e nelle modalità per nascondere le comunicazioni nel momento esatto in cui la scienza crittografica si è incontrata con le macchine elettroniche. In sostanza, l'informatica ha fornito un *boost* – ha potenziato come non mai – l'utilizzo della crittografia stessa.
Oggi un utente comune, nemmeno troppo esperto, può utilizzare la tecnologia crittografica per autenticare utenti di computer e di reti, per proteggere la confidenzialità e l'integrità delle comunicazioni elettroniche e per mantenere informazioni sensibili sicure e archiviate.
Il passaggio è stato netto: da scienza per pochi, da tecnologia tenuta segreta, soprattutto in campo militare e governativo, grazie all'informatica la crittografia è diventata una tecnologia chiave per la società dell'informazione[3].
Volendo dare una indicazione temporale precisa, un giovane e valente studioso, Bert-Jaap Koops, in una sua opera, fa risalire l'inizio di un interesse su larga scala nei confronti della crittografia più o meno all'anno 1994, quando si registra un'espansione notevole dovuta a Internet, all'*electronic banking* e alla diffusione delle transazioni elettroniche.
Koops nota, poi, come, verso il 1998, la crittografia sia già diventata una tecnologia comune senza che la gente lo sappia, e gran parte della popolazione la utilizzi senza saperlo (come nella tecnologia telefonica cellulare GSM).
Accanto a questo utilizzo involontario della crittografia, una larga parte degli utilizzatori di computer inizia a servirsene volontariamente, soprattutto nel caso delle *e-mail*, o ordinando beni *on-line*. La crittografia si diffonde, poi, anche nella *information security* e nel mondo criminale[4].

---

[1] Questo rapporto tra evoluzione della nuova società dell'informazione e necessità di *security* è delineato con chiarezza da B.-J. KOOPS, *The Crypto Controversy – A Key Conflict in the Information Society*, Kluwer Law International, 1999, p. 13.
[2] Testo di riferimento, in Italia, sia da un punto di vista giuridico sia da un punto di vista politico e tecnologico-terminologico è C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *Segreti, spie e codici cifrati*, Apogeo, 1999.
[3] La 'democratizzazione' della crittografia e la sua diffusione su larga scala, ad apannaggio anche degli utenti comuni, è documentata da BERT-JAAP KOOPS, *The Crypto Controversy*, *cit.*, in esordio di Volume.
[4] Cfr. B.-J. KOOPS, *The Crypto Controversy*, *cit.*, p. 1.

2. I settori d'impiego della crittografia e gli utilizzatori della stessa.

I settori di utilizzo della crittografia sono diversi. Posto che la crittografia è soprattutto utilizzata, nell'area giuridica che ci interessa, per salvaguardare dati e per garantire che siano integri, non ripudiabili, autentici e confidenziali, sono molte le applicazioni possibili. In molti casi, inoltre, la crittografia è l'unico modo per salvaguardare effettivamente l'informazione.
Koops, nella suo Volume, divide tre soggetti che possono essere interessati nell'utilizzazione – e, *de facto*, utilizzano – la crittografia nella 'vita quotidiana'. Tali soggetti sono: 1. I *Providers*; 2. Il Governo; 3. Altri utenti.
I *network providers,* nota Koops, possono incorporare un utilizzo anche intenso della tecnologia crittografia nei loro *network* al fine di assicurare che tutte le informazioni trasferite su quelle reti, sia verso l'esterno, sia all'interno, siano sicure da intercettazione, furto o alterazione.
Una cifratura cosiddetta 'link by link' assicura infatti che, in tutti i nodi attraversati dalle informazioni, la massa di informazioni che passerà circola cifrata. Ad esempio, la nuova versione del protocollo Ip, Ipv6, prevede l'incorporazione dello standard crittografico DES nella struttura stessa del *network*. Con riferimento al trasporto dei dati, si può incorporare anche il *Secure Socket Layer*, SSL, per facilitare comunicazioni sicure tra le parti che comunicano attraverso Internet. Anche il protocollo ISDN, inoltre, ha la possibilità di incorporare la crittografia nella tecnologia di comunicazione stessa.
Koops ricorda, poi, come il più importante *network* ad incorporare la crittografia nella sua struttura sia stato SWIFT, il *network* finanziario internazionale che deve, per forza maggiore, essere protetto a causa del numero enorme di transazioni che avvengono e del loro ammontare.
I *provider*, fa notare ancora lo studioso, confidano nella tecnologia crittografica anche per aumentare la fiducia degli utenti: ecco perché, a volte, la crittografia viene incorporata nei *browsers*, con certificati e comunicazioni che vengono automaticamente criptate. I *provider* possono, poi, proteggere la *privacy* dei propri clienti grazie a sistemi crittografici e possono usare questa tecnologia anche per le comunicazioni mobili e per proteggere la proprietà intellettuale di determinati prodotti, così come per la *editoria on-line* e la gestione elettronica dei contenuti[5].
Accanto all'utilizzo da parte dei *provider*, l'Autorità governativa, per tradizione, è stata quella che più ha utilizzato la crittografia, ed è anche stata quella più interessata a 'rompere' i codici crittografici.
Il Governo, vedremo, la utilizza nei servizi diplomatici, nella *intelligence*, negli affari militari, nei *memoranda* interni, ma anche per gestire registri personali, per proteggere le comunicazioni *intra* governative, per cifrare linee di comunicazione critiche (ad esempio quella tra la CIA e l'Interpol). Viene anche

[5] Cfr. B.-J. Koops, *The Crypto Controversy*, *cit.*, p. 49 ss.

usata nel settore pubblico, nella comunicazione tra cittadini e Stato, anche per prevenire crimini, mantenendo il testo o il documento sicuro[6].
Infine, vi sono utilizzi vari, sia individuali sia in ambiente societario e commerciale. Ad esempio, nelle applicazioni finanziarie e nelle transazioni, che devono essere in ogni momento sicure. Si pensi all'*home banking*, attività che sta diventando sempre più popolare, ai pagamenti *on-line* con carta di credito, al tentativo di evitare la intercettazione di numeri di carta di credito.
La crittografia viene poi utilizzata per garantire la *privacy* dell'individuo. Può salvare la vita a persone coinvolte in attività correlate ai diritti umani, a membri di gruppi dissidenti, in Stati con Governi che monitorizzano illegalmente le comunicazioni. Senza contare che la crittografia è importante per la connessione con il mondo esterno, e per la connessione ai *network* pubblici, oltre che per difendersi da attacchi.[7]

3. La 'crypto controversy'.

Ben presto, nel panorama politico e giuridico che ruota attorno alla crittografia, nasce il problema della cosiddetta 'crypto controversy', ovvero di come bilanciare, a livello di regolamentazione statale, gli interessi confliggenti di *privacy* e di *information security* da un lato, e gli interessi di sicurezza nazionale e di applicazione delle leggi dall'altro.
Sono cinque, secondo Koops, gli studi nazionali sulla questione della crittografia che danno orgine alla *crypto controversy*, ovvero al dibattito politico, giuridico e sociale su larga scala su queste questioni.
Il primo studio ha origine in Australia, prende il nome di *Walsh Report*, e viene rilasciato e reso pubblico nei primi mesi del 1997 dopo una pressione notevole di *Electronic Frontier Australia*. Molte sezioni di questo documento non sono state pubblicate per motivi di sicurezza, ma la parte pubblicata si presenta come una analisi profonda di questi temi nel contesto Australiano.
In Canada, la *Task Force* sul commercio elettronico e le questioni correlate ha rilasciato un *paper* di discussione chiamato *A Cryptography Policy Framework for Electronic Commerce* nel febbraio del 1998, che elenca diverse opzioni con riferimento alla cifratura di dati archiviati, cifratura delle comunicazioni in tempo reale e controlli delle esportazioni.

---

[6] B.-J. KOOPS, *The Crypto Controversy*, *op. cit.*, p. 52. Nella stessa pagina Koops riporta un interessante esempio di utilizzo della tecnologia crittografica nel mondo giuridiario-criminale. La bozza di *Dutch Computer Crime Act II* prevedeva un uso della crittografia per sequestrare od attaccare informazioni che il giudice vuole togliere dalla disponibilità di qualcuno, ad esempio materiale pornografico con minori (uso che si può paragonare al tradizionale sequestro di proprietà). Se il sequestro del mezzo che trasporta l'informazione non è proporzionato, si può cifrare l'informazione sul disco del possessore, così che l'informazione diventa improvvisamente fuori portata della persona coinvolta, sempre che non ne abbia un'altra copia, e successivamente, ad esempio al termine della indagine, l'informazione può tornare al legittimo proprietario decifrandola.
[7] B.-J. KOOPS, *The Crypto Controversy*, *op. cit.*, p. 52-56.

In Danimarca uno dei primi *report* nazionali sulla crittografia è una collezione di articoli del 1995 del *Technology Council*, *A Danish Crypto Policy. How to keep digital information secret?*.
A questo ha fatto seguito un *report* più elaborato dal titolo *Report by the Expert Committee on Cryptography* rilasciato nell'aprile del 1997 dai rappresentanti di sette ministeri, che suggeriva di non introdurre regolamentazione della crittografia in Danimarca e la possibilità di introdurre, al contrario, incentivazioni all'utilizzo della stessa. Nel giugno del 1998 l'*expert committee* ha rilasciato un *report* che raccomandava di monitorare gli sviluppi internazionali e che non limitava l'uso della crittografia.
In Svezia, un *report* dell'ottobre 1997 del *Cabinet Office Reference Group for Cryptographic Issues* si intitola *Crypto Policy: possibile courses of action for Sweden* e si occupa di ampie parti delle problematiche sulla crittografia e sulla firma digitale. Questo studio raccomanda l'uso libero della crittografia e si occupa anche del problema del deposito delle chiavi.
Negli Stati Uniti d'America nel 1994 la *Association for Computer Machinery* pubblica *Codes, keys, and conflicts, Issues in U.S. Crypto Policy*, che è il primo studio approfondito pubblicato e contenente un'analisi del problema di grande valore tecnico e scientifico.
Nel 1996 il *National Research Council*, con membri del Governo, dell'industria e del mondo universitario, pubblica *Cryptography's role in securing the information society*, che viene considerato da molti il miglior *report* disponibile, e che contiene utili suggerimenti su come non vietare o limitare l'uso personale della crittografia e alleggerire, ma non eliminare, i controlli delle esportazioni[8].

4. Il rapporto tra industria e Governo.

Ripercorrendo la storia politica e giuridica delle tecnologie crittografiche, appare subito evidente un rapporto – non sempre lineare – tra mondo industriale (soprattutto, ovviamente, industria tecnologica) e Governo (intendendo come 'governo', in questo contesto, tutti quegli enti, quelle Autorità facenti capo al pubblico, che hanno il potere di regolamentare determinati aspetti tecnologici della società[9].
Quando è iniziata l'era della comunicazione elettronica, la situazione, per l'osservatore esterno, era molto semplice: la tecnologia crittografica (*encryption*), intesa come quella tecnica che permette di proteggere le informazioni rendendole non intelleggibili attraverso determinati procedimenti (di cui il più comune è lo *scrambling*), era appannaggio esclusivo del Governo.
I motivi di questo 'monopolio governativo di fatto' su questa tecnologia erano diversi, e si possono suddividere in: a) questione di costo; b) questione di

[8] B.-J. KOOPS, *The Crypto Controversy, op. cit.* p. 2.
[9] Tale evoluzione è magistralmente riassunta in W. DIFFIE, S. LANDAU, *The Export of Cryptography in the 20th Century and the 21st*, *technical report*, october 2001, report number TR-2001-102. Su Internet all'indirizzo http://research.sun.com/research/techrep/2001 (sito e documento consultati il 15 maggio 2002).

segretezza; c) questione di pericolo/identificazione della crittografia come arma[10].

In primo luogo, i costi per sviluppare e testare efficienti sistemi di *encryption* erano talmente elevati che solo enti o agenzie pubbliche – con fondi statali – o enti di ricerca correlati al settore pubblico e ai suoi finanziamenti, erano in grado di sostenere simili spese. Problemi di costi, nel caso anche società private fossero in grado di produrre simili prodotti, ci sarebbero stati anche nella fase finale, e sarebbero stati costi talmente elevati da impedire una diffusione su larga scala per scopi commerciali.

In secondo luogo, la scienza crittografica più avanzata era, in molti casi, portata avanti nella più assoluta segretezza, in ambito militare o, comunque, per un utilizzo ad esclusivo appannaggio del Governo, senza quindi la diffusione delle tecnologie stesse.

Infine, particolarità della materia *de quo*, la crittografia era equiparata ad un'arma nella lettera di Leggi che controllavano e limitavano l'esportazione delle armi.

Sino agli anni Ottanta e Novanta il quadro era questo: i sistemi crittografici erano chiusi in centro di ricerca, non potevano essere fatti circolare, men che meno per un uso commerciale, e venivano utilizzati segretamente.

L'industria si affianca al Governo, nel tentativo di 'spartirsi la torta' della crittografia, quando inizia la diffusione di Internet e appare, all'orizzonte, l'ombra del commercio elettronico. Si comprende in tale occasione come la crittografia possa essere – ed in molti casi già sia - una componente essenziale di tutto il sistema che circonda comunicazioni con fini commerciali.

Ecco, allora, più evidenti i fattori che portano la crittografia al di fuori dell'alveo segreto-governativo: 1) la diffusione del *personal computer*; 2) la diffusione di Internet; 3) le pressioni dell'industria nell'ottica della sicurezza del commercio elettronico[11].

Il primo fattore è la diffusione del *personal computer*, che permette grandi potenze di calcolo capaci, quindi, di gestire, dall'inizio alla fine, un sistema crittografico, anche da parte dell'utente comune.

Il secondo fattore è la diffusione di Internet, e l'aumento dei volumi di circolazione delle informazioni. L'aumento di circolazione delle informazioni ha portato con sé un aumento dell'esigenza di segretezza da parte di chi comunica.

Il terzo fattore è stato dato da una forte azione di pressione da parte del mondo industriale e accademico, che ha evidenziato quanto fosse dannosa una soluzione di monopolio simile. In questo senso, la velocità con cui le Autorità hanno aperto alla crittografia è stata molto differente da Paese e Paese. Il Governo statunitense, che era al centro dell'attenzione del mondo visto lo sviluppo tecnologico in corso, non è stato certamente, si vedrà, rapido in questa liberalizzazione.

Si esporrà, in seguito, che, accanto alla chiara intenzione di varie Autorità di tenere segreti i risultati delle ricerche in tema di crittografia, vi sono state anche vere e proprie azioni di ostacolo alla diffusione di crittografia nel mondo commerciale e, più in generale, dei privati.

---

[10] Cfr. W. DIFFIE, S. LANDAU, *The Export of Cryptography in the 20th Century and the 21st*, *op. cit.*

[11] Cfr. W. DIFFIE, S. LANDAU, *The Export of Cryptography in the 20th Century and the 21st*, *op. cit.*

L'azione più efficace ha toccato il controllo delle esportazioni: si delineerà, in seguito, come sino agli anni Novanta il governo degli Stati Uniti d'America abbia vietato l'esportazione di tecnologie crittografiche bloccando, di fatto, la circolazione nel mondo di simili prodotti.
Il nuovo rapporto tra industria e Governo, disegnato dalla normativa più recente, vede una distinzione alla base, comune al mondo statunitense, tra clienti e *partner* del Governo da una parte e mondo commerciale puro e semplice dall'altra, oltre ad una distinzione tra tecnologie a grande diffusione e soluzioni personalizzate.
In questo nuovo quadro, si è data una maggior libertà alla esportazione dagli Stati Uniti d'America di tecnologia crittografica, sia nei confronti di *partner* governativi sia per usi commerciali, verso tutti quei Paesi che non appoggiano i movimenti terroristici[12].
Un punto di svolta, negli Stati Uniti d'America, nel rapporto tra industria e governo si è avuto il 14 gennaio 2000, quando il *Bureau of Export Administration* – oggi *Bureau of Industry and Commerce*[13] – ha rilasciato le tanto attese revisioni alle regole sull'esportazione della crittografia, sia *hardware* sia *software*, dando inizio ad una nuova politica commerciale pensata anche per incentivare gli investimenti e la diffusione di simili tecnologie.
In seguito alla liberalizzazione delle esportazioni dell'Unione Europea, il 19 ottobre 2000, le regolamentazioni statunitensi sono state ulteriormente ritoccate, creando un quadro ancora più favorevole al mondo dell'industria.

5. La tutela della *privacy* delle comunicazioni e dei dati dell'individuo.

L'evoluzione del controllo dell'esportazione nel settore crittografico è molto interessante, soprattutto in considerazione del suo impatto con lo sviluppo delle tecnologie a protezione della *privacy*. Prima dell'era elettronica, tutte le interazioni in tempo reale tra gli individui dovevano avvenire di persona. La *privacy*, in simili interazioni, si dava per pacifica e garantita. Non era richiesto niente più di una attenzione minima al fine di assicurarsi che unicamente la persona cui ci si rivolgeva di persona – la persona che aveva tutti i diritto di essere presente in quel momento – poteva ascoltare l'informazione che veniva 'esternata'.
Le telecomunicazioni hanno cambiato radicalmente questo quadro comunicativo. La persona con cui si interagisce non deve più essere necessariamente nelle immediate vicinanze, ma può trovarsi anche dall'altra parte del mondo, rendendo ciò che una volta era impossibile come naturale ed economico.
Le telecomunicazioni, d'altro canto, rendono la protezione dell'individuo dalle intercettazioni molto più difficile. Si è allora diffusa la necessità impellente di altri meccanismi di sicurezza, divenuti indispensabili per sostituire il 'guardarsi

[12] Cfr. W. DIFFIE, S. LANDAU, *The Export of Cryptography in the 20th Century and the 21st*, cit.
[13] In Internet all'indirizzo http://www.bxa.doc.gov (sito consultato il 15 maggio 2002, di cui vedremo, nel corso del Volume, le funzioni).

attorno', per riuscire a vedere che non ci sia nessuno abbastanza vicino da ascoltare.
Nell'era delle telecomunicazioni si è scoperto che il meccanismo ideale in tal senso è la crittografia, il solo meccanismo di sicurezza che protegge direttamente le informazioni che passano dal controllo fisico del mittente al controllo fisico di chi le riceve.
La crittografia, ai giorni nostri, è diventata molto potente, affidabile e economica, anche se utilizzata su computer di uso comune. Ciononostante, la parte del mondo delle telecomunicazioni che è protetto dalla crittografia e, quindi, realmente sicuro, è esigua. Ciò è dovuto, in parte, alla difficoltà di integrare la crittografia nei sistemi di comunicazione attuali per dare sicurezza e, in parte, ad un problema di *marketing*.
Gli investimenti, in questo settore, da parte del privato, già si è visto in precedenza, non sono ingenti, soprattutto per il fatto che occorre una grande diffusione del prodotto per rientrare negli ingenti costi che si debbono sostenere per la creazione del prodotto stesso.
Contestualmente, la sorveglianza dei nuovi mezzi di comunicazione è aumentata, da parte delle Autorità e del Governo, e queste agenzie ora temono che una diffusione della crittografia nel mondo commerciale possa privare loro di informazioni che hanno, sino ad oggi, tranquillamente e senza troppa difficoltà intercettato.
Ecco, allora, il cuore del conflitto tra il mondo dell'industria, che ha bisogno della crittografia per il commercio elettronico, e dell'Autorità che teme di perdere, da un momento all'altro, la sua capacità di sorvegliare.
Il controllo delle esportazioni crea un *background* fondamentale in questa guerra di libertà e di tecnologia.

6. Le fasi di sviluppo della politica crittografica.

Negli anni Settanta, dopo tanti anni in cui la crittografia era stata appannaggio esclusivo e proprietà del mondo militare, questa tecnologia si presenta al grande pubbico in due diverse modalità che avranno un impatto sensazionale.
In primis fu reso pubblico il lavoro dello studioso Horst Feistel e dei suoi colleghi in IBM che portò alla produzione del *U.S. Data Encryption Standard* (DES).
Il DES, che fu adottato nel 1977 come *Federal Information Processing Standard* 46, fu implementato per la protezione di tutte le informazioni governative che richiedevano tutela legale, ma non previsto per le informazioni classificate (una categoria più tardi definita 'unclassified sensitive").
Il secondo sviluppo fu il lavoro certosino di diversi accademici che portò alla crittografia a chiave pubblica, la tecnologia che è alla base della sicurezza del commercio elettronico oggi.
La crittografia a chiave pubblica rese possibile per la prima volta a due persone, senza avere elaborato prima una chiave segreta, di comunicare con sicurezza attraverso un canale insicuro.

La crittografia a chiave pubblica fornì contestualmente un meccanismo di firma digitale molto simile, nel suo funzionamento, alla firma scritta.
Gli effetti di questi due nuovi sviluppi in distinte aree della crittografia furono di portare grande interesse nel campo, con una diffusione su larga scala, in pochissimi anni, di libri, conferenze e *paper* scientifici.
La risposta immediata del Governo fu quella di cercare di acquisire lo stesso potere di classificare le informazioni e di controllare legalmente la tecnologia crittografica simile a quello che il *Department of Energy* affermava nell'area della energia atomica. Lo sforzo, in tal senso, fu un completo fallimento.
La *National Security Agency* (NSA) si augurò pubblicamente che fosse attivato un comitato dell'*American Council of Education* al fine di studiare il problema e, soprattutto, al fine di 'raccomandare' vincoli legali sulla ricerca e pubblicazione di materiale crittografico.
Al contrario, tale comitato propose unicamente che gli autori di tali studi correlati alla crittografia inviassero volontariamente i *paper* alla NSA al fine di ottenere l'opinione dell'ente sulle possibili implicazioni, con i problemi di sicurezza nazionale, di tali pubblicazioni.
Il Governo comprese ben presto che era necessario un cambio di rotta, e che se non era materialmente possibile un controllo sulle menti, un vincolo legittimo alla ricerca e alle pubblicazioni, era invece possibile il controllo della diffusione della crittografia.
Leggi che regolamentassero direttamente l'uso della crittografia negli Stati Uniti d'America non furono, in quegli anni, adottate, anche perché a molti sembravano inutili. Fu invece molto più efficace puntare sulla limitazione delle esportazioni, che diminuì l'uso della crittografia non solo all'interno degli Stati Uniti d'America ma anche all'esterno.

7. Il controllo delle esportazioni di tecnologia crittografica.

Le leggi, in vigore oggi negli Stati Uniti d'America, che controllano le esportazioni sono radicate nel periodo della Guerra Fredda che seguì la seconda guerra mondiale.
Il sistema di regolamentazione delle esportazioni che è nato da questo ambiente non presentava un solo regime di controllo delle esportazioni, ma due.
Una autorità legale primaria venne demandata al *Department of State*, con l'obbiettivo di proteggere la sicurezza nazionale. Anche se i beni che devono essere regolati da tale normativa sono descritti come *munitions*, la Legge non limita la sua azione di controllo al significato comune di tali vocaboli e include molti prodotti che non sono né esplosivi né nocivi.
I prodotti che ricadono in questa limitazione sono determinati dal Dipartimento di Stato che agisce attraverso l'*Office of Defense Trade Controls*, ODTC (che in origine si chiamava *Munitions Control Board*) sull'avviso di altri elementi del braccio esecutivo e, specialmente nel caso di crittografia, della *National Security Agency*.

Le esportazioni che influenzano sia usi civili sia usi militari sono regolate invece dal *Department of Commerce*.
Questi prodotti sono indicati come *dual-use*, e presentano un problema completamente differente rispetto alle *munitions*.
Un vastissimo raggio di prodotti – veicoli, arerei, vestiti, macchine fotocopiatrici – sono vitali per le funzioni militari così come lo sono per le funzioni civili. Se questi prodotti venissero bloccati o limitati nel loro utilizzo e diffusione per il solo fatto che un loro potenziale utilizzo potrebbe beneficiare uno stato nemico, rimarrebbe ben poco dell'attività comune de commercio internazionale. Il controllo nella esportazione degli oggetti *dual-use* bilancia allora le esigenze delle applicazioni militari con le considerazioni della necessità di una loro disponibilità su scala nazionale.
I controlli sulle *munitions* sono molto più severi di quelli sui *dual use*, dal momento che richiedono una approvazione individuale delle licenze di esportazione, con specifica dettagliata del prodotto e dell'attuale acquirente, mentre gli altri beni sono semplicemente controllati su larga scala per categoria di prodotto o per nazione di destinazione. L'autorità legale che decide che regime debba essere applicato è il Dipartimento di Stato, che può autorizzare un trasferimento di giurisdizione al *Department of Commerce*, un procedimento che viene chiamato *commodities jurisdiction*.
Individuare se un bene è a uso civile o a uso militare non è sempre semplice e lineare. A parte ciò che è chiaramente militare, si incontrano beni che possono avere tutti e due gli usi o che possono passare da un uso a un altro senza particolari problemi. Il permesso delle esportazioni è sempre stato, allora, garantito sulla basi di come i beni *dual use* fossero configurati e in base a chi fossero gli acquirenti.
In generale, una tecnologia commerciale che non è esplicitamente adattata a una funzione unicamente militare può essere venduta a un acquirente non militare senza troppa burocrazia.
L'applicazione dei controlli alle esportazioni dipende, naturalmente, dalla destinazione dei beni stessi. Le applicazioni delle restrizioni alle esportazioni per gli alleati degli Stati Uniti d'America, come i Paesi europei, sono di più facile approvazione rispetto a quelle previste per Nazioni considerate ostili. Ovviamente ci deve essere anche un coordinamento delle *policy* di esportazione di tutte le nazioni, per garantire un effettivo controllo.
Durante la Guerra Fredda, il veicolo principale per questa cooperazione tra gli Stati Uniti d'America e i suoi alleati era il Cocom, il *Coordinating Committee on Multilateral Export Controls*, la cui *membership* combinava Australia, Nuova Zelanda, Giappone, Stati Uniti d'America e la maggior parte dei Paesi dell'europa occidentali. Nonostante il Cocom esistesse primariamente per prevenire esportazioni significative militari verso i paesi non-Cocom, ciò non significava comunque che i Paesi Cocom esportassero liberamente fra loro. Prodotti che non sarebbero stati permessi verso Paesi non–Cocom potevano essere venduti ad altri Paesi Cocom ma con un procedimento di approvazione denso di burocrazia.

8. L'evoluzione della qualificazione dei prodotti crittografici.

Nel periodo immediatamente successivo alla seconda guerra mondiale, la crittografia era, come la energia nucleare, una tecnologia quasi interamente militare.
Non è allora sorprendente il fatto che tutta la crittografia, indipendentemente dalle sue funzioni o dalle applicazioni per cui si intendeva utilizzare, venisse inserita nella categoria delle munizioni.
Il progresso, l'evoluzione dei mezzi di informazione e di comunicazione, la diffusione del computer e delle reti ha determinato una spinta per portare la crittografia tra i beni *dual-use*.
L'importanza della distinzione tra *munitions* e *dual-use* risiede nella differente procedura di licenza e nella differenza nei criteri applicabili per l'approvazione delle esportazioni.
Come *munitions*, i *devices* crittografici richiedono una approvazione individuale delle licenze di esportazione.
Due fattori rendono queste licenze in conflitto con un utilizzo commerciale serio della crittografia. Il primo è il tempo (le settimane o i mesi che di solito sono richiesti per approvarequeste licenze è sovente maggiore del tempo che le organizzazioni commerciali impiegano per sviluppare prodotti nuovi e più potenti). Il secondo è la necessità di identificare l'acquirente finale. A volte si può non conoscere l'identità di chi acquista, e per le *munitions* la regolamentazione della esportazione è molto più forte, e se una esportazione viene giudicata imprudente da un punto di vista militare, viene impedita senza pensare all'acquirente, alla sua qualità e alle sue esigenze.
Anche quando la crittografia si è spostata dall'uso militare come *munition* a bene *dual-use*, il problema della distinzione tra sistemi crittografici militari e civili è rimasto attuale. Alcuni casi si presentavano, all'interprete, particolarmente semplici (ad esempio sistemi adattati in maniera specifica per lavorare con protocolli di comunicazione militari quali il MK XII IFF (*Identification Friend or Foe*) che identifica gli aerei nei radar militari o altri sistemi appositi per il mondo militare). Tali prodotti potevano essere qualificati senza problemi come 'ad uso militare'.
Come occorreva comportarsi, d'altro canto, con sistemi crittografici che operavano in ambienti commerciali *standard* e in ambienti di ufficio ordinari, e che operavano in maniera molto simile sia che fossero in un uffico privato sia che fossero in una banca?.

9. L'alleggerimento dei controlli.

I controlli sulle esportazioni di sistemi crittografici hanno iniziato ad allegerirsi nel tardo 1980 con il trasferimento al mondo commerciale di tecnologie che non erano più usate per proteggere comunicazioni intercettabili sul lungo

raggio. I cambiamenti sono stati accelerati dalla fine della guerra fredda agli inizi degli anni 90.
Una mossa importante nella direzione dell'industria fu un accordo nel 1992 tra la *National Security Agency*, il Dipartimento del Commercio e i rappresentanti dell'industria che ha permesso una approvazione generalizzata della esportazione di prodotti che utilizzino determinati selzionati e specifici algoritmi con chiavi non più lunghe di 40 *bit*. Inizialmente, due algoritmi, tutti e due segreti commerciali di *RSA Data Security*, un *leader* nella progettazione di *software* crittografico, furono approvati, e altri furono aggiunti in seguito.
I tentativi del Governo di controllare la crittografia non erano unicamente limitati alla strategia correlata alla limitazione delle esportazioni.
In parallelo con la formula della lunghezza della chiave, il governo degli Stati Uniti d'America ha cercato di cambiare le regole per avere un vantaggio permanente nella possibilità di rompere in ogni momento il codice crittografico.
Nei primi mesi del 1993, il Governo si è mosso per sostituire il *Data Encryption Standard* a 56 *bit*, vecchio di 15 anni, con un algoritmo a 80 *bit* che forniva una speciale *trap door* – botola – per permettere un accesso dell'autorità ai dati. Nel progetto del *Clipper system* le chiavi erano divise e *escrowed* con le *federal agencies*. Nonostante il Clipper sia stato adottato, ebbe pochi acquirenti e fu considerato come un fallimento.
Il Clipper ha delineato però un fondamentale principio per cui il Governo avrebbe il diritto di controllare la tecnologia crittografica al fine di garantirsi il potere di leggere messaggi intercettati (in una mossa correlata, il governo ha segnato una grande vittoria. Il *Communications Assistance for Law Enforcement Act* del 1994 ha dato al governo la possibilità di richiedere ai *communications carriers* di installare sistemi di intercettazione nei loro *network*).
Nel 1996 fu dato al *Department of Commerce Bureau of Export Administration* autorità sulla maggior parte delle esportazioni crittografiche (questo fu permesso adottando regolamenti del Dipartimento di Stato che permettevano ai produttori di rivolgersi direttamente al Dipartimento del Commercio per determinate categorie di beni, invece di sottomettere le loro richieste prima al Dipartimento di Stato. Il personale che se ne occupava venne però trasferito da un ufficio all'altro, dando più il senso di un cambiamento di forma che di sostanza.
Nell'estate del 1996 il National Research Council rilasciò il suo studio sulla *cryptographic policy*, *Cryptography's role in securing the information society* (il CRISIS *report*), elaborato proprio in un periodo in cui su ventilavano proposte di *key-escrow*.
Agendo su mandato del Congresso, il NRC riunì un gruppo di 16 esperti dal governo, dall'industria e dal mondo della scienza. Il *report* concluse che, facendo un bilancio giuridico, politico e scientifico, i vantaggi di un utilizzo su larga scala della tecnologia crittografia superano di gran lunga gli svantaggi, e che la politica degli Stati Uniti d'America era inadeguata per i requisiti di sicurezza della società dell'informazione. Il *report* suggeriva di alleggerire le politiche di esportazione e di rendere i prodotti contenenti il DES facilmente esportabili.

Nel periodo tra il 1996 e il 1997 si torna poi a parlare di *key-escrow*, con possibilità di esportazione per società di prodotti basati su DES a patto che avessero preso accordi con il Governo per sviluppare sistemi con *key recovery*. In questo periodo l'espressione *key escrow* muta in *key recovery*.
Nel 1998 le restrizioni cadono ancora, e si permette l'esportazione libera di prodotti con DES o altri sistemi crittografici con chiavi non più lunghe di 56 *bit*.
Era però troppo poco, e troppo tardi: già nel mondo gli utenti avevano fiducia in sistemi con chiavi di almeno 128 *bit*. I sistemi più forti avevano lo stesso costo e le stesse funzioni di quelli deboli, quindi perché non usare quelli più forti?
Il 1996 ha visto anche un interesse del Congresso nella esportazione crittografica, e numerosi membri del Congresso introdussero delle *bills* che diminuivano la discrezionalità esecutiva nel controllo delle esportazioni crittografiche. Nelle loro ultime versioni queste *bills* furono chiamate SAFE (*Security and freedom through encryption*).

10. Accordi sulla politica crittografica, azioni legislative e politiche.

La fine della guerra fredda rese la struttura politica del Cocom inappropriata, e tale organizzazione, che esisteva sin dal 1949, fu sostituita da una nuova coalizione, il *Wassenaar Arrangement*, che includeva anche *ex* stati ostili dell'Unione Sovietica e del patto di Varsavia. Questa organizzazione più estesa prevedeva procedure meno formali. Nonostante le Nazioni membre si fossero accordate su una lista di controllo comune, ogni Paese mantiene poteri di deliberare anche proprie liste.
In Europa nel giugno del 2000 il *European Council of Ministers* ha annunciato la fine dei controlli sull'esportazione della crittografia nella Unione Europea e con i *partners* vicini e stretti, chiamata la EU + 10 . Oltre alla UE questo gruppo include Australia, Canada, Repubblica Ceca, Ungheria, Giappone, Nuova Zelanda, Norvegia, Polonia,. Svizzera e gli Stati Uniti. La liberalizzazione delle esportazioni del 14 gennaio ha mutato in Europa il quadro che il governo statunitense si aspettava.
Il 17 luglio la amministrazione Clinton, in risposta alla liberalizzazione europea, ha adottato regole simili. Licenze di esportazione non sarebbero più richieste per l'esportazione di prodotti crittografici ai 15 stati UE e ai paesi addizionali. Non ci sarebbe poi stata una distinzione tra governments e other customers nel paesi europei e negli altri dieci. Inoltre, nonostante le società debbano ugualmente fornire una technical review una volta sola al Governo degli Stati Uniti d'America prima di esportare, possono esportare immediatamente.
In dieci anni il Governo degli Stati Uniti d'America è passato da una intransigenza totale a una libertà assoluta, in neanche un decennio. Internet è stata una delle cause, sicuramente, dal momento che ha creato una richiesta di crittografia che non poteva essere ignorata e allo stesso tempo ha reso più difficile che mai il controllo del movimento delle informazioni.

11. La politica crittografica in Italia e l'Aipa.

In Italia si è iniziato a discutere intensamente di crittografia con riferimento alla riforma in chiave elettronica della Pubblica Amministrazione, riforma che ha avuto inizio con l'approvazione delle tre leggi Bassanini e che mira ad introdurre in maniera massiccia le nuove tecnologie dell'informazione negli uffici pubblici.
L'iter normativo può vantare diverse tappe. Nel 1990 c'è stata l'approvazione della legge sul diritto di accesso ai documenti amministrativi; nel 1993 è stata istituita l'Aipa (Autorità per l'Informatica nella Pubblica Amministrazione), poi 'soppressa' nel 2002; nel 1995 il Consiglio dei Ministri ha approvato una direttiva di Governo sulla realizzazione della rete unitaria della p.a; la disciplina dei documenti informatici equiparati ai documenti cartacei con la Legge n. 59/97 se muniti della cosiddetta firma digitale, e la disciplina del protocollo informatico[14].
Il d.lgs. 12 febbraio 1993, n. 39, che ha istituito l'Autorità per l'Informatica nella Pubblica Amministrazione (art.4), all' art. 7, comma 1, lett. a), dispone che ad essa spetta "dettare norme tecniche e criteri in tema di pianificazione, progettazione, realizzazione, gestione, mantenimento dei sistemi informativi automatizzati delle Amministrazioni e delle loro interconnessioni, nonché della loro qualità e relativi aspetti organizzativi; dettare criteri tecnici riguardanti la sicurezza dei sistemi"; dispone inoltre alla lett. g), che le compete, "nelle materie di propria competenza e per gli aspetti tecnico-operativi, curare i rapporti con gli organi delle Comunità europee e partecipare ad organismi comunitari ed internazionali, in base a designazione del Presidente del Consiglio dei Ministri".
Essa svolge, pertanto, una funzione di ente formatore per la Pubblica Amministrazione, ed in tale veste ha emanato, in ottemperanza a quanto previsto dall'art.15, comma 2, della legge 24 dicembre 1993, n. 537, le regole tecniche per l'uso dei supporti ottici ed, in base alla disposizione della Legge 20 aprile 1994, n. 367, quelle per il mandato informatico.
Per quanto riguarda le regole tecniche del 1993, alla luce della rapidissima evoluzione tecnologica del settore dei supporti ottici e tenuto conto del progressivo consolidamento delle tecniche crittografiche per la firma digitale, l'Autorità ha predisposto una sostanziale revisione.
La firma digitale basata sulla crittografia asimmetrica (a chiave pubblica) si è ormai affermata come principale strumento in grado, allo stato attuale della tecnologia, di assicurare l'integrità e la provenienza dei documenti informatici e, quindi, di svolgere per questi la funzione che nei documenti tradizionali è svolta dalla firma autografa, come si è precedentemente spiegato.
L'Autorità, in virtù del suo ruolo di consulente della Presidenza del Consiglio dei Ministri che il d.lgs. n. 39/1993 le ha conferito, ha assunto un ruolo

[14] Questa evoluzione è indicata da G. BUONOMO nella Prefazione a C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *Segreti, spie, codici cifrati*, Milano, 1999, p.XI – XIV.

trainante nella predisposizione della normativa del settore, svolgendo un'attività tanto intensa da portare uno studio iniziato nel 1996 sull'introduzione della crittografia al fine della realizzazione il dispositivo della firma digitale (che nella bozza del regolamento veniva chiamata "contrassegno elettronico"[15]), alla bozza di regolamento dell'estate 1997, dalla quale è poi stato elaborato il d.p.r. 10 novembre 1997, n. 513.
Già nel 1996 infatti l'Aipa aveva predisposto un rivoluzionario embrione legislativo che avrebbe condotto, come poi ha condotto, ad un aggiornamento all'interno del nostro ordinamento giuridico, di quella che è la nozione di documento, arrivando a definire la piena equiparazione di un documento formato su un supporto elettronico e firmato digitalmente, e un documento scritto "tradizionalmente" e valido *ex* art. 2702 c.c.[16]; tutto il progetto dell'Aipa si è basato sul sistema di crittografia a chiavi asimmetriche[17] ed ha conseguentemente individuato diverse (forse troppe) autorità preposte alla certificazione delle chiavi di codificazione.
In quel frangente la bozza del regolamento venne sottoposta anche al vaglio della comunità della Rete, e appare giusto ricordarlo in quanto tale condivisione costituì un palmare esempio di "democrazia legislativa telematica", cosa che potrebbe apparire nel mondo "reale" del tutto impraticabile, stante l'impossibilità fisica e logistica di poter assistere o addirittura partecipare alla nascita di un progetto normativo.
L'altro problema che *de iure condendo* l'Aipa si è premurata di risolvere *ab origine* è poi stato quello di stabilire come ottenere l'incontrovertibile certezza dell'identità del mittente di un documento crittografato e firmato; tale questione è stata risolta attraverso l'intervento all'interno del sistema delle Autorità di Certificazione che, all'interno della bozza del regolamento del 1996

---

15 Art. 7) dello "Schema di disegno di legge", pubblicato il 18 settembre 1996: "A ciascun documento elettronico o a un gruppo di documenti elettronici può essere associato un "Contrassegno elettronico", identificativo della persona o ente dal quale il documento è stato emanato o prodotto. Il Regolamento di cui all'art.2 definirà gli elementi che il contrassegno elettronico deve contenere, in modo che ciascun contrassegno possa essere riferito in maniera unica ed inequivocabile ad un solo soggetto e al documento o insieme di documenti cui è apposto. In particolare il citato regolamento indicherà le altre misure tecniche, organizzative e gestionali volte a garantire la sicurezza del contenuto documentale e la tutela della riservatezza delle persone e degli enti interessati.(…)".

16 Art.8) dello "Schema di disegno di legge": "L'applicazione del contrassegno elettronico equivale alla sottoscrizione, prevista per gli atti e documenti a forma scritta su supporto cartaceo, del documento elettronico cui esso è apposto. Il documento elettronico sottoscritto con contrassegno elettronico è opponibile al suo sottoscrittore, tranne che quest'ultimo non dimostri di aver segnalato all'Autorità Certificatrice, in un momento anteriore a quello della sottoscrizione, l'avvenuto uso fraudolento o l'avvenuta sottrazione o alterazione della propria chiave segreta di criptazione. L'uso del contrassegno elettronico revocato equivale a mancata sottoscrizione, tranne che il suo titolarenon ne confermi nel caso specifico l'autenticità e validità, fatti salvi i diritti dei terzi ed eventuali ipotesi di reato.

17 All'art. 4 dello "Schema di disegno di legge" si stabilisce che "è consentita la emanazione e/o la trasmissione per via telematica di documenti elettronici, siano essi direttamente intelligibili ovvero previamente codificati e resi intelligibili al solo destinatario mediante codificazione con sistema di criptazione a chiavi asimmetriche scelto tra quelli riconosciuti idonei dal Consiglio Superiore delle Autorità di Certificazione di cui al successivo art. 12 su parere conforme dell'Aipa".

venivano previste all'art. 12: "Il Governo della Repubblica è delegato per la creazione e regolamentazione delle seguenti istituzioni la cui attività si svolgerà nell'ambito e con gli strumenti tecnologici della Rete Unitaria della Pubblica Amministrazione: il Consiglio Superiore delle Autorità di Certificazione, l'Autorità Amministrativa di Certificazione, l'Autorità Notarile di Certificazione, il Registro Unico delle chiavi pubbliche di criptazione, gli Archivi delle chiavi di criptazione".
L'istituzione delle AA.CC. è una componente essenziale di tutto il sistema di validazione, ovvero di quel sistema informatico e crittografico in grado di verificare la validità a tutti gli effetti di una firma digitale.
Tale verifica avviene attraverso una catena di verifiche della correlazione di chiavi asimmetriche e di accesso alle informazioni contenute nei registri dei certificati e nell'elenco pubblico tenuto dall'Aipa[18]. Tutto ciò dovrebbe rientrare sotto la definizione di "sistema informatico e crittografico".
Preme far notare come già nel 1997 Aipa spiegasse le basi della crittografia nel documento dal titolo "Firma digitale Tecnologia e standard" (Approfondimenti - Luglio/Agosto 1997 - Numero 7/8 - Anno III)[19] nel quale si nota come "La diffusione degli strumenti informatici e la parallela crescita della comunicazione attraverso le reti di calcolatori hanno posto con pressante urgenza il problema della sostituzione del tradizionale documento cartaceo con un equivalente strumento informatico. Il meccanismo universalmente adottato per costruire tale strumento è la firma digitale basata sulla crittografia a chiavi pubbliche". Sempre nello stesso documento si evidenzia come "La base della firma digitale è la crittografia a chiavi pubbliche" e come "I meccanismi di firma digitale poggiano essenzialmente sopra gli algoritmi crittografici a chiavi pubbliche, che sono detti anche a chiavi asimmetriche poiché utilizzano chiavi diverse per le operazioni di cifratura e decifratura".

---

[18]Vedi articolo di G. Rognetta pubblicato in Interlex del 6/12/01, *La validazione della firma digitale: una verifica cartacea?*, precisamente dove dice "dopo aver verificato con l'applicazione della chiave pubblica certificata che il documento si riferisce al titolare della corrispondente chiave privata certificata con la quale ha firmato il documento, bisognerà poi verificare l'autenticità del certificato, pertanto consultare la lista dei certificati delle chiavi pubbliche di certficazione tenuta dall'AIPA (art. 15.1 del DPCM 8/2/1999-regole tecniche), lista che deve essere resa accessibile anche ai certificatori, sempre telematicamente (art. 17.4). I certificati delle delle chiavi di certificazione sono inoltre registrati nel dispositivo di firma durante la sua personalizzazione (art. 26.1). Se la informazioni così ottenute sono soddisfacenti, occorre verificarne l'autenticità: a ciò è preposta la firma digitale dell'AIPA: applicando la chiave pubblica corrispondente a quella privata utilizzata dal Presidente dell'AIPA per "sottoscrivere" detta lista. Se l'esito di tale verifica è positivo, si deve accertare l'autenticità del relativo certificato: le chiavi dell'AIPA, secondo quanto dispone l'art. 17.3, sono verificate da tutti i certificatori mediante propri certificati pubblicati nel registro tenuto dall'AIPA stessa. Ma poiché si potrebbe verificare anche di questi, è stata prevista una verifica di chiusura: i codici identificativi di ciascuna coppia di chiavi dell'AIPA che sono stati pubblicati con la Circolare AIPA n. 29 del 18/5/2001 (in G.U. n. 120 del 25/5/2001). Tali codici identificativi corrispondono all'impronta del certificato della chiave del Presidente dell'AIPA, emesso dal Centro Tecnico (art. 14 reg tecnico)."

[19] Consultabile nella sua versione integrale all'indirizzo http://www.aipa.it/servizi[3/pubblicazioni[5/bollettino[1/anno1997[3/numero78/approfir.asp (sito consultato il 15 luglio 2002).

Sempre nello stesso documento, in tema di standardizzazione, si rileva come "Sotto la spinta delle applicazioni commerciali, ed in particolare di quelle bancarie, sono stati sviluppati numerosi standard relativi all'uso delle tecniche crittografiche. Dal punto di vista della standardizzazione degli algoritmi crittografici asimmetrici non può essere ignorato lo sforzo dello IEEE americano, il quale sta sviluppando uno standard unico ed integrato comprendente tutti gli algoritmi attualmente disponibili, da quelli basati sulla fattorizzazione degli interi, a quelli che sfruttano la complessità del logaritmo discreto, a quelli che usano le proprietà delle curve ellittiche. Tale progetto di standard viene indicato con la sigla P1363."
L'Aipa si occupa di crittografia anche in fase di studio delle tecnologie alla base della rete unitaria della Pubblica Amministrazione, e in particolare nello studio di fattibilità[20], nel punto 5 dedicato alla sicurezza si legge: "Funzioni di sicurezza capaci di attenuare le vulnerabilità dei protocolli telnet e ftp sono offerte da alcuni pacchetti basati sul protocollo SSL (*Secure Sockets Layer*) che fornisce protezione crittografica dei dati, autenticazione dei server, salvaguardia di autenticità e integrità dei messaggi e opzionalmente autenticazione dei client per connessioni TCP/IP. In generale, l'approccio proposto consiste nel limitare l'impiego dei protocolli telnet e ftp all'interno di un dominio; invece per l'accesso a servizi di tipo pubblico (ad esempio a banche dati), che vengano forniti da sistemi che non contengono informazioni riservate, nel limitare il loro uso a livello del dominio della Rete. Con l'introduzione, nell'architettura della Rete, del concetto di Porta Applicativa e di Porta Delegata, il servizio di terminale virtuale tra amministrazioni, nel dominio della Rete unitaria, viene filtrato dalle due porte, che sono in grado di controllare l'accesso in conformità ai livelli di sicurezza richiesti".
Nello stesso documento, al punto 5.3 ("chiavi crittografiche") si rileva come: " Funzionalità di gestioni delle chiavi, certificazione e notarizzazione, indispensabili per implementare firma elettronica, non ripudio e confidenzialità, sono servizi a valore aggiunto forniti dalla Rete unitaria" e come "Uno degli aspetti fondamentali legati alla utilizzazione della crittografia è quello della gestione delle chiavi crittografiche. Possono essere individuate sei funzionalità: Generazione delle chiavi; Distribuzione delle chiavi; Conservazione delle chiavi; Aggiornamento delle chiavi; Archiviazione delle chiavi; Distruzione delle chiavi. La sicurezza sarà garantita al livello delle applicazioni con l'introduzione della crittografia a chiave simmetrica e/o a chiave pubblica. Nel dominio della Rete unitaria non si utilizzeranno contromisure a livello dei circuiti, quali ad esempio dispositivi hardware per la codifica di tutti i messaggi scambiati. Ogni amministrazione potrà, ove lo ritenga necessario, adottare contromisure a livello dei circuiti, nell'ambito del proprio dominio, per l'intera sua rete o per parte di essa. 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

[20] Consultabile integralmente all'indirizzo http://www.aipa.it/attivita[2/reteunitaria[1/fattib[1/studio5.asp (sito consultato il 15 luglio 2002).

crittografiche sarà curata da un organismo, da creare alle dirette dipendenze della Presidenza del Consiglio dei Ministri, composto da tre funzioni distinte per la: creazione e distribuzione delle chiavi, ospitato dal Centro di Servizio, gestione del notariato, ospitato dal Centro Operativo, certificazione delle chiavi, ospitato dall'Autorità per l'informatica. In ogni caso 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".

Cenni alla crittografia vengono fatti anche nel documento relativo al Mandato informatico di pagamento[21], e nei documenti alla base del progetto della rete G-net di Aipa[22] dove, nel punto 'sicurezza', si nota come "In linea con quanto proposto nello Studio di fattibilità della Rete unitaria si prevede di ottenere i livelli di sicurezza richiesti ricorrendo, oltre che ad una oculata progettazione delle reti locali, dei server e dei servizi di gestione della rete nel suo complesso, ai seguenti elementi di sicurezza: protezione attraverso firewall per la connessione ad Internet; utilizzo di crittografia; identificazione degli utenti tramite parole chiave ed eventuali meccanismi più sofisticati, a richiesta delle amministrazioni, quali "one time" password e badge personali; distribuzione e certificazione di chiavi crittografiche necessarie per la firma elettronica e la protezione crittografica delle informazioni. È prevista la disponibilità di prodotti software integrati con l'ambiente di automazione d'ufficio (in particolare per la gestione della posta elettronica e per l'archiviazione dei documenti). È richiesta la certificazione di livello C2, secondo gli standard del Dipartimento della Difesa americano e/o di livello E3 come previsto dall'Unione Europea, per le funzionalità di rete ed il software dei server e dei client".

---

[21] Consultabile all'indirizzo http://www.aipa.it/attivita[2/progettiintersettoriali[10/mandato[5/index.asp (sito consultato il 15 luglio 2002).

[22] Consultabile all'indirizzo http://www.aipa.it/servizi[3/pubblicazioni[5/bollettino[1/anno1996[2/numero11/gnetprog.asp (sito consultato il 20 luglio 2002)

Capitolo Secondo

CRITTOGRAFIA, *SMARTCARD*, CRITTOANALISI

Sommario: 1. Alcune considerazioni tecnico-giuridiche, introduttive e terminologiche in tema di crittografia. - 2. Le *smartcard*. - 3. La crittoanalisi.

1. Alcune considerazioni tecnico-giuridiche, introduttive e terminologiche in tema di crittografia.

Nell'area di studio della crittografia, rivestono un ruolo di particolare importanza le 'tecniche crittografiche': sono quelle tecniche che rendono i dati e i programmi inintelligibili a chi non conosca l'opportuna chiave e l'algoritmo di trasformazione (i due elementi dei sistemi di cifratura che permettono di ottenere questo risultato) e, quindi, assicurano determinate garanzie relative alla loro genuinità e sicurezza.
Nel corso degli anni Ottanta, durante il momento di massimo uso dell'informatica per l'attività di documentazione da parte degli operatori economici, la crittografia permetteva quindi, pur in presenza di una relativa 'fragilità' (cioè di una facile alterabilità) dei documenti prodotti e gestiti attraverso l'uso di elaboratori elettronici, di ottenere le necessarie garanzie per poter poi costruire una loro rilevanza giuridica[23], anche se minima (comunque documenti scritti e con il valore probatorio conseguente alla formazione del convincimento del giudice) e sulla base delle interpretazioni dottrinali in merito; si aggiungono, inoltre, i vantaggi e la soddisfazione di esigenze pratiche relative alla conservazione stessa delle informazioni, ottenuti attraverso l'archiviazione dei dati all'interno delle memorie dell'elaboratore elettronico.
Nel momento del passaggio dall'impiego del computer non più solo come *working station* ma come vero e proprio strumento di telecomunicazioni e telematica, la genuinità e la sicurezza, insieme alle nuove necessità di garanzia della provenienza e della non ripudiabilità dei messaggi, abbandonarono la dimensione statica del lavoro sul singolo sistema informatico ed entrarono in contatto con quella dinamica legata alla comunicazione delle informazioni elaborate. Problemi enormemente acuiti dall'avvento della rete Internet, nuovo media efficiente ed a basso costo, diffuso a livello mondiale, e del commercio elettronico da esso reso possibile.

---

[23] Insieme alle tecnologie di memorizzazione, dette 'ottiche' (perché basate sul raggio laser per la scrittura e la lettura dei *file*) e alla conservazione dei documenti elettronici su supporti di immagine (i dischi compatti di tipo *Cd-Rom* o *Cd-Worm*).

Anche in questo caso, comunque, è la tecnica, in un primo momento, a rispondere alle mutate esigenze e, sempre sulla base dei sistemi di crittografia, anche se più evoluti e fondati su presupposti diversi rispetto alle prime esperienze di gestione di sicurezza dei dati.
Così, da un iniziale sistema a chiavi simmetriche, idoneo a proteggere i dati nel momento della loro memorizzazione, nell'ambito di una determinata stazione di lavoro, si è passati ad un nuovo sistema di crittografia a chiavi asimmetriche, pensato per una gestione a distanza delle informazioni, quindi maggiormente soggetta a possibili interferenze da parte di estranei.
Questa tecnologia della crittografia a chiavi asimmetriche, permettendo, di fatto, di proteggere i documenti elettronici, e consentendo di ottenere la sicurezza circa la genuinità e la provenienza di un determinato documento, apportava un risultato determinante soprattutto alla luce dei requisiti richiesti dalle varie discipline giuridiche ai fini della realizzazione di specifici effetti giuridici.
Inizialmente, solo sulla base dell'interpretazione particolarmente aperta della dottrina, si poteva riconoscere al documento informatico una 'fisionomia' sua propria, successivamente anche grazie a produzioni normative apposite, come è avvenuto per il sistema della firma digitale.
La crittografia è la tecnica che permette, con l'aiuto di un algoritmo matematico, di trasformare un messaggio leggibile da tutti, in una forma illeggibile per quegli utenti che non possiedano una chiave segreta di decifrazione. La funzione è reciproca, per cui l'applicazione dello stesso algoritmo e della chiave segreta al testo cifrato restituisce il testo originale.
I procedimenti di cifratura esistono fin dall'antichità e, come l'etimologia del termine dimostra (*crypto* in greco, significa nascondo, celo), fin da allora venivano utilizzati per proteggere i documenti che maggiormente dovevano essere mantenuti segreti.
Le notizie relative alla crittografia più risalenti nel tempo sono, probabilmente, quelle connesse alla 'scitala lacedemonica', usata ai tempi di Lisandro, generale spartano che sconfisse gli Ateniesi nel 404 a.C. e impose loro il governo oligarchico dei Trenta Tiranni[24].
Tra il 390 e il 360 a. C. venne compilato da Enea il Tattico, generale della Lega Arcadica, il Primo trattato di cifre e messaggi segreti in cui viene descritto un disco su cui erano praticati ventiquattro fori nel bordo esterno, ciascuno corrispondente ad una lettera dell'alfabeto. Un filo di lana, partendo da un foro

---

[24] La *scitala* è uno dei pezzi di legno, presumibilmente un bastone, costituenti una coppia di dimensioni uguali, di cui si dotavano due soggetti che volevano scambiarsi messaggi riservati (in questo caso gli *efori* di Lisandro): il testo del messaggio veniva scritto su un nastro di cuoio avvolto intorno al bastone seguendo le spire di un'ipotetica elica; il contenuto, che doveva rimanere segreto, veniva riportato sul nastro, lettera per lettera, su colonne tra loro parallele rispetto all'asse del bastone. Nonostante tutto ciò costituisse uno stratagemma rudimentale, non appena srotolato il nastro dal bastone, accadeva che il testo iscrittovi risultasse illeggibile, se non tramite un altro bastone di legno delle stesse dimensioni e forma del primo. Questo è il primo esempio storico documentato da Plutarco nella sua opera *Vite parallele*. Per ulteriori approfondimenti vedi P. RIDOLFI, *Dalla 'scitala' di Plutarco alla firma digitale*, in *Media duemila*, ottobre 1998, p. 9; dello stesso Autore anche *Firma digitale e sicurezza informatica*, Franco Angeli, 1998, p. 128 ss.

centrale, veniva avvolto passando per i fori corrispondenti alle successive lettere componenti il testo del messaggio da inviare. Alla ricezione dello stesso messaggio cifrato, riportate le lettere sul disco, si svolgeva il disco segnando le lettere da esso indicate: il testo si doveva poi leggere a rovescio. Le vocali spesso erano sostituite da gruppi di puntini.
Il "libro di Geremia", nella Bibbia, usa un semplicissimo codice monoalfabetico per cifrare la parola "Babele": la prima lettera dell'alfabeto ebraico (*aleph*) viene cifrata con l'ultima (*tau*), la seconda (*beth*) viene cifrata con la penultima (*shin*) e così via.
Lo storico greco Polibio descrive il più antico esempio di codice poligrafico: ogni lettera viene cifrata con una coppia di numeri compresi tra '1' e '5', riferendosi ad una matrice '5 x 5', che a quel tempo veniva chiamata 'scacchiera'. La scacchiera di Polibio permette di scomporre il messaggio nelle singole lettere e quindi è in grado di trasmettere qualsiasi testo. L'alfabeto greco è composto da ventiquattro lettere e, rispetto alla griglia "5 x 5", manca un carattere, carattere che veniva sostituito da un simbolo usato come segnale di sincronizzazione (inizio e fine trasmissione). La scacchiera di Polibio ha alcune importanti caratteristiche, ovvero la riduzione del numero di simboli utilizzati per la cifratura (soltanto le cifre 1, 2, 3, 4, 5) e la trasformazione di un carattere 'chiaro' in due parti cifrate, utilizzabili separatamente. Tali caratteristiche furono importanti nella storia della crittografia e vennero impiegate e rielaborate in altri cifrari (*Playfair Cipher*, Cifrario Campale Germanico).
Svetonio, nella Vita dei dodici Cesari, racconta come Giulio Cesare utilizzasse, per la corrispondenza privata, durante il tempo delle campagne di conquista nelle Gallie, la tecnica di sostituzione di ogni lettera costituente la parola, con altra lettera posticipata nel suo ordine alfabetico.
Le tecniche crittografiche col tempo vennero impiegate oltre che in campo militare anche in quello economico, come testimoniano gli storici medievali a proposito dell'uso dei banchieri fiorentini e fiamminghi, oltre ai commercianti, vicari e ambasciatori della Repubblica Serenissima di Venezia, di proteggere in questo modo le loro lettere (*in primis* le proprie lettere di cambio da inviare alle rispettive filiali)[25].
Un esempio di elaborazione tecnologica della crittografia è fornito dall'invenzione delle macchine Enigma, utilizzate dai tedeschi durante la seconda guerra mondiale, fondate sull'uso congiunto di una chiave di codifica e di un apposito macchinario a tre (esercito e aviazione) o a quattro (*U-boot* e unità speciali della Marina) cilindri sequenziali rotanti[26].
Gli esempi indicati, in particolare l'ultimo, mostrano come le tecniche di crittografia siano state applicate soprattutto nell'ambito delle esigenze di segretezza delle informazioni dell'esercito e di quelle diplomatiche: tanto che

---

[25] Per una appassionante ed esauriente trattazione del tema della crittografia nella storia, dagli antichi Egizi alla firma digitale, vedi S. SINGH, *Enigmi e segreti*, Rizzoli. Interessante e debitamente documentato anche l'articolo di G. CARCHESIO, *Crittografia: passato, presente, futuro,* pubblicato sul sito Internet www.geocities.com/Athens/Crete/2958/articolo2.html (sito Web consultato il 15 luglio 2002).
[26] Cfr. G. CIACCI, *La firma digitale*, ed. Il sole 24 ore, Milano, 2000.

sono in genere assimilate , per le loro caratteristiche e per l'uso che ne viene fatto, al materiale militare.
Anche in questo caso, però, con l'avvento e lo sviluppo di Internet, quale nuovo media di informazione e comunicazione, la crittografia è definitivamente uscita dall'oscurità per essere messa a disposizione di un pubblico sempre più vasto: quello dei milioni di utenti della rete.
In particolare, una delle conseguenze della struttura "aperta" della rete consiste nel problema della sicurezza e della riservatezza dei vari servizi offerti ed utilizzati. Tenuto conto del numero sempre maggiore di operazioni commerciali e di trasmissione di informazioni delicate, quali i dati finanziari o quelli sottoposti a segreti professionali, gli utenti, gli autori e le imprese desiderano vedere garantite proprio la sicurezza e la riservatezza delle informazioni nell'ambito della loro attività svolta su Internet.
È possibile operare una distinzione fra le varie tecniche di crittografia esistenti, basandosi sul tipo di chiave utilizzato: si individuano, così, due categorie di sistemi crittografici, quelli a repertorio, che sostituiscono a ciascuna parola una determinata serie di lettere e numeri; quelli a cifratura letterale, che provvedono alla sostituzione di lettere (sistemi a sostituzione monoalfabetica), di gruppi di lettere (sistemi a sostituzione poligrammica), o di frazioni di lettere (sistemi tomogrammici).
Sempre sulla base del tipo di chiave utilizzato, discriminante questa volta la modalità stessa di funzionamento del sistema di crittografia, si distinguono due diversi tipi di tecniche crittografiche: quelle che richiedono l'uso di una sola chiave segreta per criptare e decriptare il messaggio, e perciò dette "simmetriche" , e quelle che utilizzano una coppia di chiavi, diverse per chiudere ed aprire il documento, di cui una viene resa pubblica, e dette allora "asimmetriche".
I sistemi di crittografia simmetrica[27] funzionano partendo da una medesima chiave, detta "segreta" (perché per la riuscita del sistema tale chiave deve essere conosciuta solo dai suoi due utilizzatori), posseduta dall'emittente e dal destinatario di un messaggio, e che serve allo stesso tempo per la cifratura e la decifrazione del messaggio elettronico. Tale metodo, adatto soprattutto per soddisfare l'esigenza di genuinità del documento nel momento della sua conservazione nelle memorie del computer, e quindi in un momento 'statico', implica una serie di conseguenze negative che giungono a comprometterne l'efficienza.
Il problema più rilevante sorge quando si rende necessario trasmettere a distanza il documento e, quindi, nel momento in cui l'attività relativa al documento informatico passa ad essere 'dinamica', dovendo le parti scambiarsi la chiave di criptazione, la cui trasmissione implica tutelarne la sicurezza: questa infatti potrebbe perdersi, o essere intercettata da un terzo. Inoltre, in caso di comunicazione con diversi soggetti, si ha la necessità di adottare chiavi diverse per ognuno di essi.
Un altro aspetto negativo, rispetto allo scopo di assicurare l'integrità del documento, è che tale fine si otterrebbe nei confronti di terzi, ma non fra le

[27] Il sistema si dice simmetrico, perché, noti il procedimento e la chiave di codifica, per simmetria, si ricavano quelli di decodifica (così P. RIDOLFI, *op. cit.*, p. 10)

parti che, essendo dotate della stessa chiave, possono entrambe modificare, o alterare, il documento originario.
Esempi di questo genere di crittografia sono quelli storici già illustrati (come quello adottato dalle macchine ENIGMA durante la seconda guerra mondiale, mentre più di recente si deve segnalare il *Data Encryption Standard* (D. E. S.) , creato dal Governo americano sulla base di una procedura realizzata dall'IBM, riconosciuto come standard internazionale dal *National Bureau of Standards*, il 15 luglio 1975[28].
Altro importante esempio di crittografia simmetrica è rappresentato dal progetto chiamato *Escrowed-Enscription Standard* (E.E.S.), conosciuto anche sotto il nome di 'Clipper' o di 'Clipper Chip', sviluppato nel 1993 dall'Amministrazione presidenziale americana, probabilmente per rispondere alla rilevante diffusione del software di crittografia asimmetrica PGP (*Pretty Good Privacy*): questo sistema, che potrebbe essere definito di 'crittografia fiduciaria', utilizza un algoritmo simmetrico classificato come segreto, elaborato dalla *National Security Agency* (NSA). Poiché in caso di necessità, con autorizzazione proveniente da un mandato del giudice, un funzionario di pubblica sicurezza potrebbe ottenere una delle chiavi depositate presso le agenzie governative autorizzate (il *National Institute of Standards and Technology* e il *Department of Treasury*), nel 1994 il *Department of Commerce* ha dichiarato l'irregolarità dello standard federale 'Clipper', per mancanza dei requisiti di sicurezza necessari; in seguito, nonostante la sua diffusione immediata, venne fortemente osteggiato, seguendo la tendenza predominante di adottare sistemi asimmetrici e di utilizzare *software* che non implichino alcun accesso esterno di autorità governative che possono minare la riservatezza del sistema, rendendolo di fatto inutile.
Come si è detto, la crittografia a chiave segreta, appena esaminata, presentava diversi problemi di gestione e di efficienza. Per questo motivo, e proprio al fine di risolvere tali problemi, nel 1976, vennero inventati da Whitfield Diffie e Martin Hellman i sistemi asimmetrici di criptazione[29], detti anche sistemi a chiave pubblica: resi poi operativi nel 1977, attraverso la scoperta di uno specifico algoritmo, sviluppato sulla base del teorema di Fermat-Eulero, che

---

[28] Dopo più di vent'anni il D.E.S. sembra destinato ad essere sostituito da sistemi più recenti: infatti il N.I.S.T. (*National Institute of Standard and Technology*) ha avviato una selezione del metodo più affidabile fra quindici algoritmi crittografici, che diventerà il nuovo A.E.S. (*Advanced Encryption Standard).*

[29] "Nel 1976 Diffie ed Hellman hanno descritto un protocollo per lo scambio di una chiave segreta sopra un canale insicuro; tale meccanismo era stato inteso essenzialmente per risolvere il problema dell'avvio di un normale sistema di cifratura a chiavi simmetriche, per esempio l'E.E.S., ma in realtà ha posto le basi per la crittografia a chiavi pubbliche. Il protocollo, utilizzato da due interlocutori A e B, permette loro di utilizzare una chiave K, comune ad entrambi, calcolata utilizzando un numero di elementi superiore a quello che passerà sopra il canale insicuro, rendendo quasi impossibile la ricostruzione di K sulla base degli elementi noti trasferiti, il problema richiede la soluzione di un logaritmo discreto, che consiste nella determinazione dell'intero corrispondente al logaritmo di una base intera di un intero. Tale problema è computazionalmente difficile". Spiegazione tratta da un articolo di M. TERRANOVA, *Firma digitale: tecnologia e standard*, pubblicato nel *sito Internet* www.aipa.it/news/ottica/firmaweb.htm (sito consultato il 10 luglio 2002).

prese il nome di RSA (acronimo delle iniziali dei suoi inventori, Rivest, Shamir e Adleman, tre scienziati del *Massachussets Institute of Technology* di Boston)[30].
In tale ipotesi ciascuna persona risulta in possesso di due chiavi, una pubblica e l'altra privata, necessarie per applicare l'algoritmo matematico che permette la cifratura del documento e utilizzabili con finalità diverse, ora per criptare, ora per decriptare[31].
Orbene, ogni utente ha a disposizione due chiavi per proteggere il contenuto del documento che intende trasmettere: una chiave segreta, che custodisce e che gli permettere di procedere alla cifratura, seguendo dei criteri esclusivi (grazie ai quali è possibile identificare l'autore), e una chiave pubblica che egli distribuisce a tutti coloro ai quali desidera comunicare i propri messaggi cifrati[32].
Non è necessario che le parti si scambino informazioni riservate relative al metodo di protezione del documento (e quindi la chiave simmetrica che permette l'operazione): la chiave privata infatti è destinata a rimanere segreta ed è utilizzabile dal solo legittimo titolare; l'altra chiave deve invece essere resa pubblica, con i mezzi più diversi (mediante l'inserimento in archivi consultabili anche *on-line*), associandola al nome di un titolare (associazione che sarà garantita da un apposito soggetto, il cosiddetto certificatore).
La crittografia asimmetrica è suscettibile di due distinte utilizzazioni, potendo essere impiegata a fini di segretezza ovvero a scopo di autenticazione[33].
Presentati gli aspetti positivi dei sistemi asimmetrici, bisogna sottolineare però, che la criptazione a chiave simmetrica risulta essere più rapida e veloce, soprattutto nel caso di documenti particolarmente lunghi, che solitamente sono i più esposti ad una possibile violazione.
Allo scopo di risolvere tale inconveniente, nei sistemi a criptazione asimmetrica è stato ideato un ulteriore stratagemma, per la protezione dei documenti informatici: la chiave privata, non viene applicata di regola sull'intero messaggio, ma solo su di un estratto di esso che viene automaticamente ricavata dal documento originale, applicando una funzione di *hash*[34].

---

[30] È il primo sistema di crittografia a chiavi pubbliche e attualmente il più utilizzato e diffuso. Il metodo si basa sulla fattorizzazione di interi di grandi dimensioni (fino a duecento cifre); la sicurezza del RSA è affidata alla complessità, che è di tipo esponenziale, del problema della fattorizzazione dei numeri interi. È possibile rinvenire un interessante approfondimento della teoria matematica alla base della crittografia asimmetrica in P. RIDOLFI, *Firma digitale e sicurezza informatica, op. cit.*

[31] Vedi L. BERARDI - A. BEUTELSPACHER, *Crittologia*, in *Collana di quaderni di informatica*, Milano, 1996.

[32] Come si vedrà in seguito, attraverso l'uso della chiave pubblica di un utente, i terzi possono inoltre cifrare un messaggio che quell'utente sarà poi il solo a poter decifrare, ottenendo così la massima riservatezza durante la trasmissione.

[33] Per autenticazione si intende il processo in forza del quale il destinatario di un messaggio digitale ha la certezza dell'identità del mittente e/o dell'integrità e non ripudiabilità del messaggio stesso.

[34] Una dottrina considera poi *l'hash* un terzo tipo di funzione crittografica, oltre a quella simmetrica e a quella asimmetrica, sul tema vedi M. FAGNANI, la *Firma digitale: soluzioni e strumenti per realizzazione, problematiche gestionali*, intervento al Convegno *I regolamenti di attuazione in materia di firma elettronica e archiviazione ottica dei documenti*, Roma, 25 e 26 novembre 1998.

Tale tecnica rende possibile, partendo da un determinato documento di lunghezza variabile, ottenere una sequenza di caratteri alfanumerici a lunghezza prefissata e standard (normalmente 128 o 160 *bit*), una stringa definita 'impronta' (o *hash code*): questo tramite l'applicazione al testo del documento di un algoritmo matematico (la cosiddetta 'funzione di hash') che, sulla base del numero e del tipo di caratteri, permette di generare tale estratto. È importante sottolineare che l'impronta è unica per ogni documento, e che basta cambiare anche un solo carattere del testo dello stesso (anche solo uno spazio), per avere un'impronta diversa[35].
Queste caratteristiche rendono tale modalità fondamentale ai fini dell'apposizione della firma digitale ad un documento: è, infatti, l'uso incrociato di una funzione matematica (la funzione di *hash*) e della crittografia asimmetrica a realizzare un ottimale livello di efficienza. Questo il motivo per cui viene utilizzata nei più recenti sistemi di firma digitale.

2. Le *smartcard*.

In un sistema di certificazione e di autenticazione supportato dal metodo di cifratura a chiavi asimmetriche, si è visto che la provenienza del documento trasmesso è fondamentalmente ricollegata alla semplice presunzione che la paternità di quel documento sia imputabile al titolare della relativa chiave pubblica.
Per tutelare al massimo il soggetto titolare, il quale deve necessariamente essere l'unico a poter conoscere ed utilizzare la propria chiave privata, il Legislatore del 1997 ha ritenuto essenziale dare una definizione di chiave privata quale "elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare" (art. 1 lett. e)del Regolamento).
È stato peraltro necessario individuare un supporto informatico idoneo[36] a memorizzare e conservare i dati relativi alle chiavi private, anche per il fatto che esse sono piuttosto lunghe (più di 4000 *bit*): esse consistono infatti di sequenze di caratteri privi di un senso compiuto e perciò impossibili da ricordare a mente.
Per quanto riguarda la conservazione delle chiavi private, le Regole Tecniche prescritte nel DPCM 8 febbraio 1999 stabiliscono che "le chiavi private sono conservate e custodite all'interno di un dispositivo di firma", che è "un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno firme digitali".

---

[35] Anche in tal caso, basta solo modificare un carattere affinchè cambi l'impronta, e di conseguenza, la firma digitale: nell'indicato sistema non si avrà dunque una sottoscrizione unica per tutti i documenti di un autore, ma tante firme digitali, tutte validi criteri di imputazione, quanti sono i diversi documenti sottoposti alla funzione di *hash* e crittografia mediante chiave privata.
[36] Supporti come *hard disk*, *floppy disk*, *microchip*, carte a microprocessore o *smart card* o *chip card*, *cripto-card*, *cripto-box*, ecc…

Nella fase di definizione del cosiddetto dispositivo di firma, non era ancora chiaro in cosa dovesse esattamente consistere, ma la scelta si è concentrata sull'uso di una *smartcard*, dalle caratteristiche standard, strutturata cioè, al suo interno, in una memoria digitale ed un microprocessore, connessi ad un sistema operativo miniaturizzato in grado di supportare le applicazioni e le operazioni di cifratura.
La *smartcard*, naturalmente, viene corredata del supporto fisico che ne permette l'utilizzazione (e precisamente un lettore di *smartcard* da collegare al *personal computer*) e di un programma informatico apposito che, nella maggior parte dei casi, è scaricabile gratuitamente direttamente dal sito dell'ente certificatore prescelto per ottenere l'assegnazione della propria coppia di chiavi per la firma digitale.
Oltre la capacità di memorizzare e di calcolare al suo interno la chiave privata, il dispositivo di firma, al fine di garantire l'identità del titolare legittimo deve gioco-forza avere la capacità di procedere a tale identificazione prima di passare alla fase di generazione della chiave, escludendo altresì qualsiasi forma di comunicazione della chiave segreta verso l'esterno[37].
Soccorrono, in questo senso, le tecniche di identificazione per l'accesso ai sistemi informatici, stante la loro applicabilità anche per l'accesso alle chiavi private, ed essenzialmente si basano su una strategia semplice ed ormai collaudata: il soggetto titolare-utente deve conoscere personalmente un dato (*password*, *pin*, *passphrase*), deve possedere uno strumento (ad esempio una *smartcard*[38]), ma potrebbe anche usare un dispositivo tarato attraverso la misurazione di una o più delle sue caratteristiche fisiche o comportamentali (chiavi biometriche[39]).
Il metodo di riconoscimento biometrico, in effetti, offre una maggiore sicurezza contro gli abusi, in quanto basato sulle caratteristiche fisiche (impronte digitali, timbro vocale, mappa dei vasi sanguigni della retina, impronta delle labbra, geometria della mano, mappa del DNA) o su caratteristiche comportamentali (analisi grafologica, schemi di digitazione), caratteristiche che comparate o opportunamente combinate sono idonee ad identificare un individuo in maniera unica ed univoca.
Il Regolamento n. 513/1997 intende come chiave biometria "la sequenza di codici informatici utilizzati nell'ambito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente" (art. 1, lett. g); le regole tecniche emanate con il d.p.c.m. 8 febbraio 1999, però, non contengono precisi ed espliciti riferimenti circa l'impiego di tecniche biometriche di identificazione del titolare della chiave.
L'eventuale impiego dei dati biometrici come strumento idoneo all'accesso alla chiave privata, pur costituendo un sistema di sicurezza di grado elevato, non

---

[37] Un programma informatico, infine, gestisce la procedura di validazione, sia nell'apposizione della firma che nella verifica della firma altrui, limitandosi a richiedere all'utente un 'clic' per apporre la firma, mentre invierà un messaggio del tenore 'firma valida', una volta effettuata la verifica
[38] Sui vari tipi di carte, vedi E. GIANNANTONIO, *Manuale di diritto dell'informatica,* p. 311 ss..
[39] Vedi R. ZAGAMI, *Firme "digitali", crittografia e validità del documento elettronico*, *op.cit.*

rende in ogni caso 'personale' la firma digitale, così come nell'accezione classica si intende una sottoscrizione autografa; la firma digitale, infatti, non è direttamente collegata al dato biometrico, il quale, esattamente come un *pin* o una *password*, costituisce solo il mezzo tecnico per accedere all'uso del dispositivo di firma, dove effettivamente è custodita la chiave segreta[40].
In definitiva, il riconoscimento dei dati biometrici (o la digitazione del *pin* o della *password*) è funzionale ad una prima fase di identificazione dell'utente legittimo del sistema informatico (*access control*), corrispondente al normale accertamento dell'identità personale (corrispondenza biunivoca fra un soggetto e i suoi dati identificativi), che viene svolto con i mezzi più diversi (documento di riconoscimento, ricognizione da parte di persone conosciute).
Non sarebbe una firma elettronica 'avanzata', dunque, se effettuata con l'apposizione del solo dato biometrico, dato inevitabilmente legato alla persona cui si riferisce, senza alcun collegamento con il documento informatico firmato; tale documento infatti potrebbe essere modificato senza che ciò possa comportare alcuna variazione della 'firma biometrica' che potrebbe, peraltro, essere duplicata e riutilizzata.

3. La crittoanalisi.

Ne *I Pensieri* di Leonardo si legge che "Nessuna umana investigazione si po' dimandare vera scienza, s'essa non passa per le matematiche dimostrazioni", e tra tutte le scienze nessuna meglio della crittografia e della crittoanalisi rientrano nella definizione leonardesca.
Entrambe le summenzionate scienze, però, hanno risentito, e risentono tuttora, della forte matrice militare che le ha sempre connotate, per cui raccogliere informazioni esaustive sugli strumenti utilizzati per cifrare messaggi o sui cifrari più utilizzati non è un'impresa facile. Le difficoltà si moltiplicano poi quando si va a trattare della sorella gemella della crittografia, ovvero la crittoanalisi.
La crittoanalisi è quella scienza che si preoccupa di studiare i messaggi cifrati e di riportare, mediante complesse operazioni matematiche, il testo in chiaro ed intellegibile.
La moderna crittoanalisi si basa sul cosiddetto principio di Kerckhoffs, contenuto all'interno del libro scritto da lui stesso *La criptographie militaire* del 1883. Per questo principio la sicurezza di un sistema crittografico non deve dipendere dalla segretezza dell'algoritmo usato ma solo dalla segretezza della chiave.
Fondamentalmente non si può riporre la sicurezza di un sistema crittografico solo sulla convinzione che nessuno scoprirà l'algoritmo, ma paradossalmente se un sistema crittografico è veramente sicuro si potrà anche pubblicare

[40] Ad esempio, il servizio Bancomat, nel subordinare le operazioni all'inserimento della tessera magnetica e di un *pin*, compie solo l'identificazione dell'utente, verificando unicamente la legittimità al compimento dell'atto (il prelievo di denaro), senza creare alcun documento che lo rappresenti in modo sicuro.

l'algoritmo (ad esempio come è avvenuto per il DES) visto che la sicurezza del sistema verterà esclusivamente sulla segretezza della chiave di cifratura.
Oltre al già citato principio di Kerckhoffs, per individuare la robustezza del sistema crittografico devono anche essere rispettati i principi di Bacon, ovvero: 1) Le funzioni di cifratura e decifratura devono essere facili da calcolare; 2) nota la funzione di cifratura deve essere impossibile calcolare la funzione di decifratura; 3) il messaggio cifrato deve apparire come un qualsiasi messaggio in chiaro.
Ovviamente, la crittoanalisi come scienza ha seguito pari pari l'evoluzione della crittografia, riuscendo man mano a elaborare tecniche sempre più complesse per rompere i vari sistemi crittografici nel frattempo elaborati.
In particolare, la crittoanalisi ha tristemente conosciuto la sua massima espressione in uno dei periodi più bui della storia dell'uomo, ovvero intorno alla seconda guerra mondiale, quando riuscire a decifrare le informazioni del nemico era un'esigenza primaria.
La storia di questo periodo ruota intorno ad ENIGMA, la notissima macchina per cifrare utilizzata dai tedeschi e più volte protagonista di film di spionaggio.
Gli attacchi sistematici verso questa macchina ed il suo sistema di cifratura vennero prevalentemente da due direzioni: dalla Polonia prima della guerra e, successivamente allo scoppio del conflitto, dal gruppo di decrittatori di Betchley Park in Inghilterra.
I maggiori ringraziamenti, tra tutti i matematici inglesi che parteciparono al lavoro di crittoanalisi, vanno ad Alan M. Turing, che oggi viene considerato a pieno titolo uno dei fondatori dell'informatica moderna. Grazie al suo validissimo apporto, infatti, non solo si riuscì a decrittare il complesso sistema crittografico che stava dietro ad ENIGMA, per quanto si riuscì a tener segreta la cosa per tutta la durata della guerra, così che i messaggi intercettati provenienti da postazioni tedesche riuscivano ad essere tranquillamente decifrati. Giusto per una maggiore completezza storica è a dirsi che, mentre la vicenda di ENIGMA ha visto vittoriosi i crittanalisti inglesi, vi furono però macchine crittografiche che non furono mai violate, come la Geheimschreiber T-52, utilizzata sempre dai tedeschi.
Sempre nello stesso periodo si registrò anche una considerevole produzione di macchine *hardware* appositamente studiate per agevolare la decifratura dei sistemi crittografici utilizzati dai tedeschi, e la più famosa di esse, ovvero il COLOSSUS, può essere fondatamente considerato un precursore dei moderni computer digitali.
Del resto, il legame tra crittoanalisi ed informatica è evidente, visto che per testare un sistema crittografico spesso bisogna lavorare con stringhe di lettere e di numeri molto grandi, confrontare dati e compiere varie operazioni che un computer riesce a effettuare in modo sicuramente più veloce ed efficiente che non la mente umana.
Gli attacchi che i crittoanalisti compiono nei confronti dei sistemi di cifratura sono stati bene o male canonizzati, e qui di seguito si analizzeranno i più rilevanti:
1) *Ciphertext-only attack*. L'*attacker* non è a conoscenza assolutamente di cosa contenga il messaggio cifrato, e quindi deve lavorare solo sul messaggio cifrato,

sperando di riuscire ad intuire la chiave. Se questo sistema poteva anche essere valido per i vecchi sistemi di cifratura, ora è praticamente inutile contro i moderni algoritmi.
2) *Known-plaintext attack*. L'*attacker* conosce una parte del testo in chiaro ed ha di fronte il testo cifrato. Deve riuscire a capire dove collocare la parte in chiaro di sua conoscenza e, sulla base delle informazioni raccolte, decifrare il resto. Uno dei più moderni sistemi di attacco *known-plaintext* è la crittoanalisi lineare contro i cifrari a blocchi.
3) *Chosen-plaintext attack*. Il crittanalista può, in questo caso, avere un testo di sua scelta cifrato secondo una chiave a lui ignota. Lo scopo è determinare la chiave usata per la cifratura. Questo procedimento viene utilizzato nella crittanalisi differenziale contro cifrari a blocchi.
4) *Man-in-the-middle attack*. Si verifica questa situazione quando un soggetto si frappone nello scambio di chiavi necessarie per decifrare il messaggio (ad esempio nel sistema denominato 'Diffie-Hellman'). Ci si può cautelare usando un sistema di crittografia pubblica firmato digitalmente.
5) *Correlation*. Questa tecnica studia le correlazioni tra la chiave segreta e le risultanze del sistema di cifratura. Si può dire che sia il sistema migliore per 'rompere' un algoritmo crittografico, tant'è che questa tecnica è stata utilizzata per il *cracking* del DES.
6) *Attack against or using the underlying hardware*. Consiste in tutti gli attacchi portati a livello *hardware* contro sistemi di cifratura. Qui la differenza è che bisogna decifrare l'implementazione dell'algoritmo all'interno dell'*hardware*, oltre che l'algoritmo matematico in sé e per sé.
7) *Faults in cryptosystems*. Si ha in caso di piccoli errori nella computazione interna che, però, possono portare il crittoanalista alla scoperta della chiave segreta.
8) *Quantum cryptography*. Utilizza macchine costruite secondo i dettami della meccanica quantistica e, quindi, molto più potenti rispetto a quelle attualmente conosciute, per cui dovrebbero riuscire a decifrare un messaggio in minor tempo. A detta di molti, l'informatica quantistica rappresenta il futuro sia della crittografia sia della crittoanalisi, ma le implementazioni finora sperimentate di crittografia quantistica ci mostrano ancora una certa inadeguatezza di fondo.

PARTE SECONDA

CRITTOGRAFIA, POLITICA, NORMATIVA E DIRITTO

Capitolo Terzo

CRITTOGRAFIA, FIRMA DIGITALE E DOCUMENTO INFORMATICO

SOMMARIO: 1. Crittografia e firma digitale come garanzia di validità del documento informatico. – 2. La firma digitale: la certificazione. – 3. I soggetti certificatori: requisiti, obblighi e responsabilità. – 4. La mancata garanzia di interoperabilità tra certificatori. – 5. Firma digitale e sottoscrizione autografa. – 6. La firma digitale autenticata e la marcatura temporale. – 7. Il documento informatico. – 8. Il valore giuridico del documento informatico. – 9. La contestazione del documento informatico.

1. Crittografia e firma digitale come garanzia di validità del documento informatico.

Le tecniche di cifratura (in particolare ci si riferisce ai metodi di crittografia a chiavi asimmetriche), elaborate e sviluppate per proteggere i documenti informatici durante la fase di trasmissione attraverso reti telematiche (per definizione 'aperte ed insicure'), si sono rivelate, *de iure condendo*, un supporto necessario alla teorizzazione della validità giuridica dei documenti formati attraverso un elaboratore elettronico, ed ora, *de iure condito*, l'unica possibile e percorribile via attraverso la quale si è giunti a definire il documento elettronico e la sua entrata a tutti gli effetti nel *corpus* normativo del nostro ordinamento giuridico.
Soffermandoci sull'importanza data dal nostro sistema, sia dal punto di vista sostanziale sia da quello processuale, alla sottoscrizione quale criterio di imputazione delle dichiarazioni provenienti da un soggetto determinato e quale fondamento del valore probatorio conferito ad alcune specie di documenti (la scrittura privata o l'atto pubblico, detti documenti 'dichiarativi'[41], proprio in ragione della funzione che svolgono), non si può non riconoscere come l'intervento sulla materia , attraverso tutta l'attività normativa 'a cascata'[42], fino

[41] Vedi sul punto A. GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico*, in *Riv. Trim. dir. Proc. Civ.,* 1998, p. 491.
[42] Si è indicato infatti, come ciò sia avvenuto attraverso una specie di 'fattispecie a formazione progressiva', rappresentata dall'emanazione successiva dell'art. 15, comma 2, della Legge 15 marzo 1997, n. 59, in materia di riforma della Pubblica Amministrazione e di semplificazione amministrativa; del d.p.r. 20 novembre 1997, n. 513 (il "Regolamento contenente i criteri e le

al recente d.lgs. 23 gennaio 2002 n. 10, in attuazione della Direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche, abbia segnato un momento di enorme portata innovativa all'interno del sistema, tanto da poterne definire gli effetti 'rivoluzionari'.
Il Legislatore italiano ha introdotto nel nostro Paese un'articolata disciplina, come appena accennato, in materia di valore giuridico del documento elettronico, che tuttavia è andata sviluppandosi attraverso una serie di rinvii in bianco ai regolamenti, senza passare al vaglio del dibattito parlamentare, costituzionalmente sede eletta per il 'giudizio' sulle leggi: in altri termini, è stato conferito al Governo un potere normativo eccezionale nella materia di cui si tratta.
Certamente è innegabile il fatto che attualmente si registra la tendenza, negli ordinamenti cosiddetti 'evoluti', ad alleggerire le incombenze normative del Parlamento, attribuendo le stesse ad organi con competenze tecniche, ma è anche vero che l'art. 17, comma 2, della Legge. 400 del 1988 presuppone la determinazione con legge delle "norme generali regolatrici della materia", norme che non si ravvisano *ictu oculi* nel testo dell'art. 15, comma 2, della Legge. 59 del 1997[43].
Con il puntuale intervento del 1997 sopracitato, il Legislatore ha statuito la validità, ai sensi e per gli effetti dell'art. 2702 c.c., di una dichiarazione contenuta in un documento formato e firmato digitalmente attraverso l'uso di un *software ad hoc* (sistemi crittografici asimmetrici); si è raggiunta così la certezza nel poter attribuire la paternità del documento stesso al soggetto titolare della chiave privata certificata, certezza che tradizionalmente si è sempre e solo concretizzata a mezzo di sottoscrizione autografa da parte del soggetto dichiarante; solo l'intervento legislativo pertanto ha potuto fare assurgere la sottoscrizione digitale a valida tecnica di sottoscrizione, tanto da essere equiparata a tutti gli effetti a quella autografa[44].
La definizione di firma digitale[45], così come contemplata dall'art. 1, lett.b), del d.p.r. n. 513/1997[46], rimane sempre valida, nonostante la sovrapposizione di

---

modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'art. 15, comma 2, della Legge 15 marzo 1997, n. 59") e delle Regole tecniche in esecuzione dell'art. 3 del d.p.r. 513/1997, approvate dalla Presidenza del Consiglio dei Ministri il 13 febbraio 1999; infine il Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, d.p.r. 28 dicembre 2000, n. 445.

[43] Ci si allinea così con il pensiero di L. ALBERTINI, *Sul documento informatico e sulla firma digitale (novità legislative)*, in *Giust. Civ.,* 1998, p. 267, soprattutto dove annota il fatto che la soluzione migliore sarebbe stata una delega legislativa "con opportuni principi e criteri direttivi".

[44] La Corte di Cassazione infatti, ha sempre escluso che la sottoscrizione con nome e cognome potesse essere sostituita da attività equipollenti, anche se astrattamente idonee ad assicurare la provenienza della dichiarazione da un determinato soggetto, come , per esempio, l'apposizione di crocesegno da parte di un analfabeta in presenza di due testimoni. Per tutte Cass. 10 maggio 1950 n. 1205, in *Foro It.*, 1950, I, p.1307.

[45] Non è più possibile oggi parlare *solo* di firma digitale. A seguito del recente intervento legislativo di attuazione della normativa europea, esiste allo stato un *sistema di firme elettroniche*, al cui interno si possono distinguere *tre tipologie di firme*: 1) la firma elettronica *debole*, vale a dire *l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica* (art. 2, lett. a, d.lgs. 10/2002); 2) la firma elettronica *avanzata*, definita come *la firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca identificazione, creata con mezzi sui quali il*

successivi contributi normativi sia nazionali che sovranazionali, in quanto i requisiti previsti dal nostro Legislatore ai fini della sua validità coincidono con quelli del legislatore comunitario ove definisce la tipologia della "firma elettronica avanzata": è facile rilevare come la caratteristica peculiare della firma digitale, rispetto a quella tradizionale o alle firme "elettroniche" (di cui si parlerà più oltre, in una breve scorsa alla direttiva 1999/93/CE), sia costituita dal sistema di validazione, intendendosi come tale un sistema informatico e crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità[47].

Fondamentalmente la firma digitale è un'informazione che viene aggiunta ad un documento redatto per mezzo di un elaboratore elettronico al fine di garantirne integrità e provenienza.

Sebbene l'uso per la sottoscrizione dei documenti formati su supporti informatici sia quello più frequente e per così dire, 'fisiologico' alla firma digitale, essa invero può essere utilizzata per autenticare una qualunque sequenza di simboli binari, indipendentemente dal loro significato[48].

Da sottolineare, per inciso, che un'altra caratteristica innovativa della firma digitale consiste nel fatto che essa è intrinsecamente legata al documento cui è applicata: la firma e il corpo del testo possono essere separati effettivamente

---

firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 2, lett. g, d.lgs. 10/2002); 3) la firma elettronica *avanzata basata su un certificato qualificato e generata attraverso un dispositivo di firma sicura* (art. 10, comma 3, d.p.r. 445/2000, così come introdotto dall'art. 6 d.lgs. 10/2002). A tale ultimo tipo di firma elettronica (*firma elettronica sicura*) appartiene la firma digitale adottata in Italia con il d.p.r. 513/1997. L'art. 11, d.lgs. 10/2002 stabilisce d'altra parte espressamente che i documenti sottoscritti con firma digitale basata sui certificati rilasciati da certificatori iscritti nell'elenco pubblico tenuto dall'AIPA ai sensi dell'art. 27, comma 3, d.p.r. 445/2000 producono gli effetti della firma elettronica avanzata basata su certificato qualificato e generata mediante un dispositivo per la creazione di una firma sicura. Inoltre, i certificatori che (alla data di entrata in vigore del regolamento di cui all'art. 13 d.lgs. 10/2002) risulteranno iscritti nell'elenco pubblico tenuto dall'AIPA saranno iscritti d'ufficio nell'elenco pubblico dei certificatori accreditati, di cui all'art. 5 d.lgs. 10/2002 (art. 11, comma 2, d.lgs. 10/2002). Il sistema di firma digitale adottato con il d.p.r. 513/1997 (confluito poi nel d.p.r. 445/2000) sopravvive dunque oggi nell'ambito del più vasto sistema di firme elettroniche adottato con il d.lgs. 10/2002 in attuazione della normativa europea. Vedi commento di F. DELFINI alla *La recente direttiva sulle firme elettroniche: prime considerazioni,* in *I Contratti,* n.4/2000, p. 425 e l'articolo di G. BRIGANTI, *Le firme elettroniche, Forma ed efficacia del documento informatico dopo il D.L.vo 23 gennaio 2002, n. 10, "Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche"* pubblicato all'url http://www.iusreporter.it (sito Internet consultato il 20 luglio 2002).

[46] S'intende "per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

[47] Cfr. art. 2, comma 1, dell'allegato tecnico al d.p.c.m. 8 febbraio 199: per la generazione e la verifica delle firme digitali possono essere usati i seguenti algoritmi: a) RSA (*Rivest-Shamir-Adleman algorithm*). b) DSA (*Digital Signature Algorithm*).

[48] Un esempio sempre più comune di questo uso generalizzato è l'apposizione di firme digitali ai *database* contenuti nelle memorie di massa di un sistema i elaborazione, al fine di bloccare, o per lo meno contrastare, gli attacchi di *virus*, *worms* o l'attività dei *crakers*.

senza perdere il vincolo funzionale che li lega; a documenti diversi corrispondono firme diverse[49].

Attraverso la predisposizione da parte della Presidenza del Consiglio dei Ministri, delle "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, del d.p.r. 513/1997" (13 febbraio 1999)[50] , si comprende bene quale sia il sistema di firma digitale scelto dal legislatore italiano: la crittografia a chiavi asimmetriche unita alla funzione di *hash*[51].

Vengono inoltre introdotti sia il concetto di "impronta", sia quello di "funzione di hash"[52], e, per meglio identificare le modalità pratiche di

---

[49] "Nonostante la sua perfetta replicabilità, è impossibile trasferirla (la firma digitale) da un testo ad un altro", così spiega M. TERRANOVA, *Firma digitale:tecnologie e standard,* pubblicato in http://www.aipa.it/news/ottica/firmaweb.htm (sito Internet consultato il 15 luglio 2002); sull'argomento cfr anche R. MONTANARI, *Il documento informatico: profili tecnici sulla riconoscibilità della provenienza e della firma*, in http://www.interlex.com (sito Internet consultato il 15 luglio 2002) (Relazione del Convegno Nazionale su "Informatica e riservatezza" del CNUCE di Pisa, 26 settembre 1998).

[50] La forma legislativa impiegata è quella di un decreto della Presidenza del Consiglio dei Ministri, costituito da tre articoli, con un "Allegato tecnico" di 63 articoli, suddivisi in cinque titoli, che contiene il vero e proprio Regolamento.

[51] Si è introdotta una distinzione tra due possibilità: da una parte la criptazione mediante il solo uso della propria chiave privata; dall'altra la generazione dell'impronta e, successivamente, la criptazione unicamente di questa con la chiave privata: secondo i sistemi che adottano questo tipo di distinzione, unicamente nel secondo caso si sarebbe in presenza di una firma digitale. Bisogna inoltre rilevare che, almeno con riferimento al d.p.r. 513/1997, non si capisce bene quale delle due modalità di crittografia asimmetrica indicate venga effettivamente scelta (con o senza l'uso della funzione di *hash*), e se devono essere considerate alternative o cumulabili: tutto ciò nonostante la dizione "firma digitale" sia riportata ripetutamente nell'intero Capo II del Regolamento. Vedi anche G. CIACCI, *La firma digitale*, 1999, Il sole 24 Ore. Tale difficoltà di comprensione è probabilmente dovuta all'incomprensione o alla confusione fatta fra l'uso della chiave privata e la sottoscrizione digitale ed è stata segalata anche da MARTINO, il quale rileva come ciò sia "grave, contrario agli orientamenti della UE e giuridicamente sbagliato: è tanto grave da essere una delle ragioni del ritardo nella pubblicazione dopo la firma del decreto", A. MARTINO (a cura di), *Nuovo regime giuridico del documento informatico,* Franco Angeli, 1998, p. 24. Aggiungasi infine che tale confusione non viene chiarita nemmeno dal Regolamento Tecnico (nella versione approvata dalla Presidenza del Consiglio dei Ministri il 13 febbraio 1999) emanato allo scopo di precisare le modalità pratiche del sistema (ai sensi dell'art. 3 del d.p.r. 513/1997 (anche se in conclusione, sembra più sicuro l'accoglimento della tecnica che usa sia la chiave privata, sia la funzione di *hash* (come si può evincere dalla lettura dell'art. 1, lett. *b*, *d, e* ed *f* del d.p.r. 513/1997) che riporta le definizioni dei termini usati nel Regolamento, dove si parla di "sistema di chiavi asimmetriche a coppia". In mancanza di una norma che espressamente distingua tra la cifratura mediante l'uso della chiave privata e la sottoscrizione digitale, sembrerebbe accolta la seconda modalità, quella attraverso la funzione di *hash*, sulla base dell'interpretazione degli articoli in cui si usa l'espressione "apposizione" di firma digitale.

[52] Per "funzione di hash", si intende una funzione matematica che genera, a partire da una sequenza di caratteri binari, un'impronta, una compressione della sequenza originaria, in modo tale che risulti impossibile risalire reversibilmente alla stringa di origine; stante la proprietà di detta funzione, consistente nell'unidirezionalità, è definita anche "hash irreversibile"; un'altra peculiarità della funzione di *hash* sta nella resistenza alle collisioni, nell'impossibilità pratica di determinare una coppia di documenti con lo stesso valore dell'impronta. Per firmare un documento, si ricorre alla funzione matematica di *hash* che genera l'impronta del documento stesso, impronta che viene poi, a sua volta, cifrata con la chiave privata del firmatario: in questo

svolgimento dell'attività di sottoscrizione digitale, ad essi si accompagnano i termini "dispositivo di firma" e di "evidenza informatica".
Ne consegue allora che i documenti prodotti e gestiti mediante elaboratore elettronico, sui quali sia stata applicata la chiave segreta di un soggetto, ai fini dell'autenticazione, possono essere considerati alla stregua di quelli cartacei tradizionali: documenti scritti, scritture private, atti pubblici o riproduzioni meccaniche, a seconda di come siano redatti [53].
Il semplice utilizzo delle chiavi crittografiche però, realizza perfettamente solo due dei requisiti essenziali al documento per poter produrre i propri effetti giuridici rappresentativi e dichiarativi, cioè la sicurezza e l'integrità dei dati in esso contenuti; manca un terzo requisito essenziale, quello della paternità, della possibilità di ricondurre il documento formato ad un soggetto determinato che lo riconosca come proprio.
Il Legislatore del 1997, all'art. 1 lett. m), ha previsto la creazione di un'Autorità *ad hoc*, l' Autorità di Certificazione, il cui compito è quello di stabilire, garantire e pubblicare la corrispondenza tra ogni chiave disponibile al pubblico nei registri telematici consultabili *on-line*, ed il soggetto che usa la complementare chiave segreta.
Tale associazione viene realizzata attraverso il procedimento di certificazione.

2. La firma digitale: la certificazione.

La certificazione[54], consiste nella possibilità di verifica della firma presso un soggetto pubblico o privato (soggetti che svolgono la funzione di certificatori

---

modo si è ottenuta la firma che viene accodata al documento. Chiunque può accertare sia l'origine del documento, sia l'integrità dello stesso, attraverso una procedura a ritroso: dopo aver applicato lo stesso algoritmo di *hash* del firmatario al documento cifrato (cosiddetto "hash fresco"), recupera la chiave pubblica del firmatario, decifra l'*hash* allegato al documento e verifica che sia identico a quello "fresco"; se i due *hash* corrispondono, sono garantite l'identificazione della chiave di cifratura e l'identità del documento: il documento non ha subito alcuna alterazione dal momento della sua generazione. Per la descrizione dettagliata della funzione di *hash* cfr. R. GRANATO CORIGLIANO, *Firma digitale e forma elettronica,* in Riv. Di Dir. Privato, n.4, 2000.

[53] È chiaro che un risultato così importante non poteva essere raggiunto se non attraverso un riconoscimento legislativo, essendo stati necessari sì, ma non sufficienti gli sforzi interpretativi della migliore dottrina (*ex plurimis* CARNELUTTI, MONTESANO, VERDE, ANGELICI, RICCI, GIANNANTONIO, PATTI, CLARIZIA, IRTI, ZAGAMI, DE SANTIS. La novità risiede proprio in questo, in una nuova consapevolezza, acquisita dal Legislatore, dell'indispensabile apporto delle nuove tecnologie in relazione alle modalità di documentazione e di trasmissione dei dati che lo ha condotto ad elaborare la disciplina già adottata a livello internazionale.

[54] La certificazione è definita come il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato, in ogni caso non superiore a tre anni (art. 22, lett. f, D.P.R. 445/2000). Ai fini del d.lgs. 10/2002: per certificati elettronici devono intendersi gli *attestati elettronici che collegano i dati utilizzati per verificare le firme elettroniche ai titolari e confermano l'identità dei titolari stessi* (art. 2, lett. d); per certificati qualificati *i certificati elettronici conformi ai requisiti di cui all'allegato I della direttiva*

delle chiavi pubbliche, iscritti nell'elenco tenuto a cura dell'AIPA) che custodisce la chiave pubblica[55].
Tale procedura di pubblicazione della seconda chiave garantisce l'assenza di alterazioni sul documento informatico sottoscritto, ma l'ulteriore ed indispensabile funzione identificativa del soggetto dichiarante e sottoscrittore è data dalla "certificazione" della firma digitale.
I soggetti certificatori, rispondenti tassativamente ai requisiti fissati dal Regolamento, hanno il compito di rilasciare il certificato (che dovrà essere allegato ogni volta in cui l'utente appone la propria firma digitale) e di pubblicarlo insieme alla chiave pubblica nell'elenco delle chiavi di sua gestione: elenco che viene posto *on-line*, a disposizione di chiunque.
Tali enti hanno appunto il compito di garantire la corrispondenza tra chiavi e identità personale dei soggetti ai quali esse si riferiscono.
Essi sono definiti come il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati (art. 22, lett. i, d.p.r. 445/2000)[56].
Il fatto che una chiave pubblica decifri una firma digitale, non ha di per sé alcun significato, se non che due chiavi (pubblica e privata) sono matematicamente correlate; *rebus sic stantibus*, però, non esisterebbe alcun collegamento intrinseco tra una chiave pubblica ed una persona.
È necessario ed essenziale l'intervento di una terza parte fidata ed imparziale, detta appunto "certificatore" (art. 1 lett.k) del Regolamento)[57], la quale emetta i

---

1999/93/CE, rilasciati da certificatori che rispondono ai requisiti fissati dall'allegato II della medesima direttiva (art. 2, lett. e). Per accreditamento facoltativo deve intendersi *il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e sicurezza* (art. 2, lett. h).

[55] Il dispositivo di firma è definito come un apparato elettronico programmabile solo all'origine in grado (almeno) di conservare in modo protetto le chiavi private e generare al suo interno firme digitali (art. 1, lett. d, allegato tecnico d.p.c.m. 8 febbraio 1999). Ai fini del d.lgs. 10/2002, per dispositivo per la creazione di una firma sicura deve intendersi l'apparato strumentale, usato per la creazione di una firma elettronica, rispondente ai requisiti di cui all'art. 10 del medesimo decreto (art. 2, lett. f).

[56] L'art. 27 d.p.r. 445/2000 prevede che chiunque intenda utilizzare un sistema di chiavi asimmetriche di cifratura deve munirsi di una idonea coppia di chiavi e rendere pubblica una di esse mediante la procedura di certificazione. La medesima disposizione stabilisce che le attività di certificazione sono effettuate da certificatori inclusi, sulla base di una dichiarazione anteriore all'inizio dell'attività, in un apposito elenco pubblico, consultabile in via telematica, predisposto tenuto ed aggiornato a cura dell'Autorità per l'informatica nella pubblica amministrazione (AIPA) e dotato dei prescritti requisiti (art. 27, comma 3, d.p.r. 445/2000). Il sistema di validazione è definito come *il sistema informatico o crittografico in grado di generare ed apporre la firma digitale o di verificarne la validità* (art. 22, lett. a, d.p.r. 445/2000). Le chiavi asimmetriche sono definite come la coppia di chiavi crittografiche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici (art. 22, lett. b, d.p.r. 445/2000). La chiave privata è definita come l'elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico o si decifra il documento informatico in precedenza cifrato mediante la corrispondente chiave pubblica (art. 22, lett. c, d.p.r. 445/2000).

[57] Si parla anche, indifferentemente, di Autorità di Certificazione (A.C.) o *Certification Authority* e di *Trusted Third Party* (T.T.P.). In realtà le A.C. si distinguerebbero dalle T.T.P. perché queste ultime hanno anche compiti di archiviazione delle chiavi private, preclusi invece alle prime.

certificati, cioè i documenti digitali che attestano essenzialmente che una certa chiave pubblica[58] è di proprietà di un certo soggetto (art. 1 lett. h) del Regolamento).
In sede di emissione del certificato, il certificatore, "previo accertamento dell'identità personale del richiedente", "garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto" (art. 1 lett. h), art. 9, comma 2, lett. a)del Regolamento)[59].
Considerando poi che si tratta di una tecnologia ancora relativamente nuova, il certificatore è tenuto ad informare i richiedenti sugli aspetti tecnici della procedura di certificazione (art. 9, comma 2, lett. e).
Il rapporto tra il titolare della chiave e l'ente certificatore può essere ricostruito in termini contrattuali, in quanto soggetti privati e operanti in regime di libera concorrenza come imprese commerciali[60].
Sembra che nessun ruolo sia affidato al notaio in sede di emissione dei certificati; le procedure e le attività di certificazione, anche riguardo alla fase di accertamento dell'identità personale e della dichiarazione di corrispondenza tra chiave e soggetto, sono riservate ai certificatori autorizzati (art. 1 lett. h e lett. k, art. 8, art. 9, comma 2, lett. a)[61].

Così *European Commission*, *Ensuring Security and Trust in Electronic Communication - Towards a European Framework for Digital Signatures and Encryption,* 8 ottobre 1997, COM (97) 503, che pone l'obiettivo di armonizzare le differenti legislazioni entro l'anno 2000, allo scopo di assicurare il mutuo riconoscimento delle firme digitali (per una lettura integrale delle modificazioni della direttiva sopra menzionata vedi sito web http://europa.eu.int/eur-lex/it/register2.htlm e http://www2.echo.lu oppure http://www2.cordis.lu (siti consultati il 20 luglio 2002) .

58 La chiave pubblica è definita come l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche o si cifrano i documenti informatici da trasmettere al titolare delle predette chiavi (art. 22, lett. d, d.p.r. 445/2000).

59 È imprescindibile anche un accertamento dello stato di capacità legale e naturale del richiedente (ad esempio: interdizione, fallimento, ecc.) (art. 9, comma 2, lett *b*).

60 Nel contratto l'utente accetta il certificato, e si definiscono quegli aspetti che possono essere diversi tra i vari certificatori e che vanno oltre le varie prescrizioni legislative ed i requisiti minimi comuni (ad esempio costi, qualità del servizio, limiti di responsabilità, livelli di sicurezza). Il contratto in questione dovrebbe essere concluso in forma scritta su carta (a meno che il richiedente non possieda già altra valida chiave privata con cui sottoscrivere) e contenuto nel relativo certificato oppure da questo richiamabile mediante *link* ipertestuale alle condizioni generali contrattuali del certificatore (*certification practice statement*).

61 Nelle leggi e progetti di certi stati americani, i 'public notaries' agiscono come autorità certificanti subordinate, o come loro supporto. Nel *Notaries Public Reform Act* dello stato dello Utah, promulgato l'11 marzo 1998, si stabilisce che il riconoscimento di un messaggio o di un documento in forma elettronica da parte di un notaio, è considerato valido a tutti gli effetti, nonostante la mancanza di stampa sullo stesso di un "notary seal" (sigillo o timbro notarile) se: a) il messaggio o documento elettronico è stato firmato digitalmente in modo conforme alla sezione 46-3-401 dello *Utah Digital Signature Act* alla presenza del notaio; b) il notaio ha confermato che la firma digitale sul messaggio o documento elettronico è verificabile mediante l'uso della chiave pubblica certificata e pubblicata secondo quanto disposto dalla sezione 46-3-403 dello *Utah Digital Signature Act;* c) il notaio firma elettronicamente il riconoscimento con firma digitale conforme alla sezione 46-3-401 dello *Utah Digital Signature Act* ; e d) la seguente informazione appare elettronicamente all'interno del messaggio firmato digitalmente dal notaio: (I) il nome per esteso del notaio e il numero corrispondente al mandato (a certificare, da parte dell'autorità di certificazione sovraordinata) esattamente come indicato nel loro mandato; e (II) le parole "Notary Public", "Stato dello Utah" e "il mio mandato scade il -data- "; e (III) il

Il contenuto dei certificati, secondo il Regolamento, deve essere tale da potersene ricavare le generalità dell'utente, della corrispondente chiave pubblica e del termine di scadenza, l'indicazione, inoltre, di un numero seriale identificativo, dell'algoritmo di cifratura da utilizzare, del periodo di validità (*operational period*) (o dell'eventuale revoca), del certificatore e, infine, la firma digitale di quest'ultimo applicata su tutti gli elementi precedenti.
Altre informazioni indicabili (le cosiddette *certificate extensions*) sono eventuali poteri di rappresentanza volontaria, legale od organica (ad esempio l'amministratore delegato di una società, oppure l'indicazione che le chiavi sono da usare con "firma congiunta", o con "firma disgiunta"), titoli e cariche professionali (art. 9, comma 2, lett. c)[62]; non è previsto che siano indicati limiti di utilizzo entro valori prestabiliti o per tipi di atti.
Il Regolamento Tecnico del 13 febbraio 1999 inoltre introduce, senza evidenziarla particolarmente, una novità importante agli effetti della sottoscrizione, anzi della certificazione, dato che all'art. 23 statuisce che nei certificati relativi alle chiavi, i dati di cui all'art. 11, comma 1, lett. d), cioè nome, cognome, data di nascita, ovvero ragione o denominazione sociale del titolare del certificato, possono essere sostituiti da uno pseudonimo, sul presupposto che i dati effettivi del titolare siano poi reperibili negli elenchi tenuti dal certificatore.
Lo pseudonimo per avere autonoma rilevanza dovrà naturalmente rispondere ai requisiti stabiliti dalle norme coordinate degli artt. 9 c.c. e 8 della Legge sul diritto d'autore n. 633 del 1941 che ne sanciscono la rilevanza e l'equiparazione al nome vero solo in ragione di parametri oggettivi (notoria conoscenza dell'equivalenza fra nome e pseudonimo) che portino ad identificare con certezza l'identità del titolare.
Il ricorso all'uso dello pseudonimo come alternativa all'indicazione di dati reali nell'ambito della sottoscrizione non era mai stata oggetto di alcuna previsione legislativa, ma piuttosto frutto di elaborazione giurisprudenziale[63]: il

---

domicilio o la residenza del notaio, esattamente come indicato nel loro mandato. (vedi sito web http://www.mbc.com/ecommerce/legis, sito consultato il 10 luglio 2002).

[62] Le chiavi con le quali agiscono gli enti sono intestate a persone fisiche, la cui autorizzazione ad agire e i cui poteri di rappresentanza organica risultano dai certificati, in cui andrebbero incorporate le disposizioni rilevanti degli statuti; eventuali discordanze tra le risultanze dei certificati e quelle dei registri tradizionali (ad esempio con riguardo alla sussistenza e ai limiti di poteri di rappresentanza) andrebbero risolte con la prevalenza dei secondi (Registro delle Imprese), almeno fino a quando non si stabilisca un collegamento diretto fra gli archivi dei certificati ed i registri già esistenti, per cui, una modifica degli amministratori nel registro delle imprese, porta ad un automatico aggiornamento dei primi. In caso di rappresentanza volontaria, la procura andrebbe incorporata al certificato; per l'efficacia delle modificazioni o della revoca della procura *ex* art. 1396 c.c. occorrerà anche intervenire sul relativo certificato; la revoca del certificato non comporta revoca tacita della procura (art. 1724 c.c.); in caso di discordanza tra contenuto del certificato e procura, sarà quest'ultima a prevalere. In caso di rappresentanza legale, rispetto al contenuto dei certificati, saranno prevalenti le risultanze del registro delle tutele e di quello delle curatele (artt. 47-51 att. C.c.).

[63] Cfr. F. SARZANA DI SANT'IPPOLITO, *Considerazioni in tema di documento informatico, firma digitale e regole tecniche,* in Il Corriere Giuridico, 1999, n.7, p. 807 dove annota Cass. 11 ottobre 1956, n. 3513 "Non può essere negata la validità di una scrittura privata, la quale sia stata sottoscritta con l'indicazione di un prenome e di un cognome, che quantunque non corrispondenti a quelli che risultano dai registri dello stato civile, siano tuttavia sostanzialmente idonei, anche per

regolamento tecnico sopracitato invece riconosce valore giuridico pieno alla sottoscrizione effettuata mediante pseudonimo, a condizione che i dati reali di identificazione del titolare del certificato siano conservati dal certificatore almeno per dieci anni dalla scadenza del certificato stesso.
Il Regolamento non specifica gli obblighi informativi accessori da parte del certificatore nei confronti di terzi, si limita a stabilire l'onere di conservazione, facendo perciò supporre che le reali informazioni sull'identità del titolare possano o debbano addirittura rimanere segrete anche nei confronti di un terzo che le volesse verificare, con tutte le conseguenze aberranti che ne scaturirebbero in un campo come ad esempio quello contrattualistico, in cui è essenziale la conoscibilità dell'identità dei contraenti al fine della valida stipulazione negoziale.
Il certificatore pertanto, può, stante il tenore letterale del regolamento tecnico, legittimamente rifiutare, senza incorrere in sanzioni, di fornire le informazioni sulla reale identità del titolare, consolidando così a livello normativo quello che è stato definito come "anonimato protetto"[64].
Lo stesso certificatore che ha certificato la chiave (pubblica) pertanto, provvede alla sua conservazione per un periodo non inferiore a dieci anni dall'inizio di validità (art. 8, comma 2), mediante l'istituzione e il mantenimento di un archivio telematico dei certificati (*key repository*): sarà in questo modo possibile la consultazione telematica dei certificati e delle liste dei certificati revocati, condizione essenziale per la funzionalità dell'intero sistema, data la normale esigenza di una verifica rapida (in tempo reale al momento della loro apposizione) delle firme digitali, per accertare la sussistenza di eventuali revoche o scadenze[65].
Per la diffusione delle chiavi pubbliche delle autorità certificatrici di vertice, occorrerebbe prevedere una divulgazione con mezzi diversi e più sicuri (ad esempio, tramite la pubblicazione in Gazzetta Ufficiale o mediante CD-WORM appositamente stampigliati) per scongiurare i rischi di diffusione di chiavi false, dato che tali chiavi non possono essere verificate, perché non certificabili, se non da autorità di pari grado[66].

---

concorso di altri elementi contestuali, ad indicare la persona del sottoscrittore, dalla quale provenga in effetti la dichiarazione". Secondo CARAMAZZA, voce *Documentazione e documento,* in *Enc. Giur. Treccani,* vol. XI, 6, la sottoscrizione con un nome diverso dal proprio può implicare l'attribuzione di una responsabilità, come avviene nel caso degli artt. 7, 8, 11, l. camb..

[64] Vedasi sempre F. SARZANA DI SANT'IPPOLITO, *op. cit.* , dove aggiunge anche che il registro del certificatore non può essere considerato un pubblico registro, "a meno che il certificatore stesso non sia una P.A., nel qual caso, al di là della definizione giuridica del registro, trattandosi di esercizio di attività pubblica, potrebbe forse applicarsi la disciplina dell'esercizio del diritto di accesso prevista dalla Legge 241 del 1990".

[65] Nel caso di comunicazioni in reti aperte ed insicure (come Internet) vi è comunque il rischio che un terzo si possa inserire nella comunicazione e sostituire il certificato inviato dal certificatore con un altro certificato verificabile con la stessa chiave pubblica del certificatore, però emesso in un periodo anteriore alla sua perdita di validità.

[66] Le chiavi delle autorità di vertice non possono essere fornite telematicamente, a meno che il sistema di trasmissione dei dati non sia assolutamente sicuro da intrusioni (situazione normalmente improbabile nelle reti aperte, come Internet).

3. I soggetti certificatori: requisiti, obblighi, e responsabilità.

Con riferimento al settore privato (per la pubblica amministrazione vige un autonomo sistema *ex* art. 17), per svolgere l'attività di certificatore[67] occorre l'inclusione in un apposito elenco pubblico tenuto dall'AIPA (art. 8, comma 3)[68].
I requisiti per l'iscrizione sono in parte mutuati da quelli richiesti per l'esercizio dell'attività bancaria (artt. 14 e 26 del d.lgs. 385/1993):
- forma di società per azioni[69], con un capitale sociale adeguato[70] (a garanzia del corretto funzionamento del certificatore e dell'adempimento degli eventuali obblighi di risarcimento);
- requisiti di onorabilità da parte dei rappresentanti legali e degli amministratori;
- affidamento per competenza ed esperienza al fine del rispetto delle norme del regolamento e delle regole tecniche;
- adozione di processi informatici e prodotti conformi a standards internazionali[71].

---

[67] Il certificatore, è definito come il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati (art. 22. lett. i, d.p.r. 445/2000). Ai fini del d.lgs. 10/2002: per certificatori devono intendersi *coloro che prestano servizi di certificazione delle firme elettroniche o che forniscono altri servizi connessi alle firme elettroniche* (art. 2, lett. b). In ossequio alla Direttiva europea, l'art. 3, comma 1, d.lgs. 10/2002 prevede espressamente che l'attività dei certificatori stabiliti in Italia o in un altro Stato membro dell'Unione europea è libera e non necessita di autorizzazione preventiva; per certificatori accreditati *i certificatori accreditati in Italia ovvero in altri Stati membri dell'Unione europea, ai sensi dell'articolo 3, paragrafo 2, della direttiva 1999/93/CE* (art. 2, lett. c);

[68] Vedi anche il commento di G. FINOCCHIARO alla *Circolare Aipa sull'utilizzo della firma digitale nelle PP.AA. del 16 febbraio 2001 n. AIPA/CR/27*, dove si ribadisce anche che "le PP.AA. possono certificare solo le chiavi dei propri organi ed uffici, escludendo quindi che le PP.AA. possano certificare le chiavi pubbliche degli utenti: ad esempio il Comune non può certificare le chiavi pubbliche del cittadino o l'Università le chiavi pubbliche degli studenti. Continua precisando che le PP.AA. che intendano certificare direttamente le chiavi pubbliche dei propri organi o uffici devono iscriversi nell'elenco pubblico dei certificatori", *Firma digitale: per i documenti "esterni" serve l'iscrizione all'elenco dei certificatori,* in *Guida al Diritto,* n.10, p.114.

[69] L'inciso "se soggetti privati", contenuto nell'art. 8, comma 3, lett. *a*, fa pensare che anche nel settore privato (dato che l'art. 8 fa salvo l'art. 17, relativo alla certificazione nell'ambito della p.a.) possono svolgere il ruolo di certificatori dei soggetti non privati. In numerose leggi e progetti di legge stranieri e sovranazionali sulla materia, la struttura e il quadro di funzionamento delle autorità di certificazione (*public key infrastructure*) sono puntualmente disciplinati su un piano legislativo e non regolamentare, prevedendo in generale una struttura gerarchizzata a due livelli, con il livello subordinato (*root authority*) di emanazione statale o pubblica che certifica le autorità subordinate, normalmente private[69]. *Rebus sic stantibus*, con la scelta della forma di società per azioni, si è inteso istituire un sistema di certificazione con soggetti imprenditori, operanti in libera concorrenza. Essenziale al ruolo di certificatore è la sua indipendenza e terzietà rispetto a interessi coinvolti nelle transazioni. Un sistema di certificatori privati con scopo di lucro, potrebbe non garantire sufficientemente questa esigenza, potendosi prospettare delle ipotesi di conflitto di interessi. È però irrealizzabile un obbligo di astensione, una volta che una firma digitale è stata apposta, in relazione ad un certificato già emesso; rimane allora la responsabilità per i danni (art. 9) che il certificatore può avere causato violando la sua posizione di terzietà.

[70] Capitale sociale di 12,5 miliardi.

L'accertamento del possesso dei suddetti requisiti, avviene attraverso la valutazione dell'AIPA, in un regime di tipo autorizzatorio (licenza) e non concessorio (art. 8, comma 4)[72].
L'AIPA, inoltre, deve monitorare l'attività dei certificatori in particolare, per quanto riguarda l'adempimento degli obblighi cui sono tenuti e puntualmente previsti dal regolamento:
- identificare con certezza la persona che fa richiesta della certificazione;
- rilasciare e rendere pubblico il certificato (le cui caratteristiche tecniche sono stabilite da un apposito decreto del Presidente del Consiglio dei Ministri);
- specificare, su richiesta dell'istante, e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite;
- attenersi alle regole tecniche stabilite con l'apposito decreto indicato sopra;
- informare i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici necessari per accedervi;
- attenersi alle norme sulla sicurezza dei sistemi informatici e a quelle sul trattamento dei dati personali;
- non rendersi depositario di chiavi private;
- procedere tempestivamente alla revoca o alla sospensione del certificato in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione di conoscenze di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni;
- dare immediata pubblicazione della revoca o della sospensione delle chiavi;
- dare immediata comunicazione all'Autorità per l'Informatica nella Pubblica Amministrazione ed agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività e della conseguente rilevazione della documentazione da parte di altro certificatore o del suo annullamento[73].
Il certificatore inoltre è tenuto a rispettare le misure minime di sicurezza per il trattamento dei dati personali adottate ai sensi dell'art. 15, comma 2, della Legge 31 dicembre 1996, n. 675; a non esercitare il ruolo di depositario di chiavi private; a sospendere e revocare il certificato qualora si verifichino le seguenti ipotesi:

---

[71] È previsto il riconoscimento delle firme verificabili con certificati rilasciati da certificatori stranieri (*cross certification*) operanti sulla base di licenza rilasciata da altro stato membro dell'Unione Europea o dello spazio economico europeo, subordinando tale riconoscimento alla dimostrazione di "equivalenti requisiti" di sicurezza (art. 8, comma 4).

[72] Il regolamento non impedisce l'impiego di firme digitali certificate da parte di soggetti non autorizzati, e l'utilizzo di sistemi di cifratura (algoritmi) diversi da quelli che verranno riconosciuti dalle emanande regole tecniche. In queste ipotesi, poiché il Regolamento (artt. 5, comma 1, 8, comma 1, 2, 3), non permette di attribuire al documento informatico l'efficacia di scrittura privata *ex* art. 2702 c.c., si dovrebbe rientrare, pertanto, nella generale categoria del semplice documento informatico, con il valore di riproduzione meccanica *ex* art. 2712 c.c. (art. 5, comma 2). Effetti probatori maggiori potranno derivare dall'esistenza di sottostanti accordi contrattuali, eventualmente rafforzati dal deposito della chiave pubblica presso un notaio. Vedi R. ZAGAMI, *Firme "digitali", crittografia e validità del documento elettronico*, in *Diritto dell'informazione e dell'informatica*, 1996, p.163 e p. 159 ss..

[73] Vedi l'articolo di G. BUONOMO, *Atti e documenti in forma digitale,* pubblicato sul sito Web www.interlex.com/docdigit/buonomo6.htm (sito consultato il 15 luglio 2002).

- apposita richiesta da parte del titolare o del terzo dal quale derivino i poteri di quest'ultimo (cosiddette cause volontarie o soggettive);
- perdita del possesso della chiave o provvedimento dell'autorità ovvero acquisizione della conoscenza di cause limitative della capacità del titolare (cosiddette cause oggettive);
- sospetti abusi o falsificazioni (cosiddette cause derivanti da supposizioni del certificatore).

La revoca o la sospensione della coppia di chiavi asimmetriche devono essere immediatamente pubblicate, così come deve essere prontamente data comunicazione all'AIPA e agli utenti, con un preavviso di almeno sei mesi, della cessazione dell'attività, indicando se alla cessazione conseguirà la rilevazione dell'attività da parte di un altro certificatore o il mero annullamento delle certificazioni.

Nel caso invece di cessazione involontaria, conseguente ad esempio al fallimento o ad altra procedura concorsuale nei confronti della società, è necessario comunque, che la comunicazione sia data al più presto possibile, anche se sembra difficile il rispetto del termine di preavviso[74].

L'art. 28, comma 1, del Testo Unico (d.p.r. n. 445/2000) stabilisce il criterio di imputazione della responsabilità civile connessa all'attività di certificazione: chiunque intenda utilizzare un sistema di chiavi asimmetriche per firmare digitalmente ha l'onere di adottare "tutte le misure tecniche ed organizzative idonee per evitare danno ad altri[75].

Non è di facile interpretazione il comma 1 nel punto in cui richiama "tutte le misure…idonee", poiché non si dice quale livello di efficienza sia richiesto, anzi, letteralmente, il soggetto responsabile deve avvalersi di "tutte" le misure suggerite come idonee sia dalla scienza informatica, che dall'organizzazione aziendale (sembrerebbe però, in questo modo, obbligato ad adottare anche le misure di sicurezza solo "astrattamente idonee")[76].

Altri Autori[77], rilevando che la Direttiva 1999/93/CE detta una norma minimale (nel senso che gli Stati membri potranno eventualmente optare per forme di responsabilità più severe), sottolineano peraltro come la stessa direttiva preveda una regola, in materia di prova, che tende a favorire il danneggiato: si dipone infatti l'inversione dell'onere della prova circa la

---

74 V. FEDELI, *Documento informatico e firma digitale: valore giuridico ed efficacia probatoria alla luce del decreto del Presidente della Repubblica 10 novembre 1997, N. 513,* in *Riv. Di Dir. Comm*., 1998, I, p. 828.

75 Si rileva facilmente come riecheggia in questa previsione il precetto dell'art. 2050 c.c. in materia di esercizio di attività pericolose: assimilare la certificazione ad attività pericolosa ha come conseguenza rilevante l'inversione dell'onere della prova. All'attore sta di dimostrare il nesso di causalità fra l'attività e il danno subito, mentre al convenuto incombe l'onere di provare di avere adottato tutte le misure idonee ad evitare il danno. In realtà il Legislatore non ha disposto esplicitamente in tal senso e una tale interpretazione è forse eccessiva, se non altro nei confronti degli utenti. Sembra opportuno quindi, ritenere che nei loro confronti si possa continuare ad applicare la normativa generale relativa ai fatti illeciti.

76 Ritengono corretto qualificare l'attività di trasmissione di atti giuridici elettronici come pericolosa ai sensi dell'art. 2050 c.c. G. FINOCCHIARO, *I Contratti informatici,* op.cit., p. 193 e ALBERINI, *Sul documento informatico e sulla firma digitale (novità legislative),* op.cit., p. 284-285.

77 Per tutti vedi F. SORRENTINO, *Firma digitale e firma elettronica: stato attuale e prospettive di riforma*, in Diritto dell'informazione e dell'informatica, n.3, 2000.

valutazione della colpa del certificatore in ordine alle riscontrate inesattezze del certificato qualificato che siano fonti di danno. Il prestatore del servizio è esonerato da tale responsabilità solo se prova di aver agito senza negligenza[78].
A carico del privato invece sorge l'obbligo di custodire la chiave privata per evitare che i terzi inviino dichiarazioni a nome del soggetto titolare, ma senza il suo consenso, ed altresì l'obbligo di comunicare immediatamente al certificatore l'eventuale smarrimento della chiave medesima.
Il certificatore dovrà invece verificare sempre la corrispondenza fra la chiave pubblica e il relativo titolare, curandosi anche di controllare i poteri rappresentativi in capo a colui che chieda la certificazione, nonché la verifica della tempestività di pubblicazione degli atti di revoca o di sospensione delle chiavi.

4. La mancata garanzia di interoperabilità tra certificatori.

Nonostante la predisposizione e la precoce entrata in vigore di una dettagliata e "pionieristica" disciplina normativa sulla firma digitale, il problema principale incontrato dagli operatori giuridici e non, è stato sicuramente quello di giustificare la mancanza di interoperabilità, cioè di incompatibilità fra tecnologie e strutture dei certificati utilizzati che hanno reso impossibile in molti casi la trasmissione e lo scambio dei documenti informatici firmati fra soggetti che possiedono firme digitali certificate da differenti certificatori.
Il problema sorge poiché i vari standard adottati per la rappresentazione dei dati e la loro realizzazione nei prodotti commerciali[79], allo stato dell'allegato tecnico dell'8 febbraio 1999, non garantiscono una completa interazione tra i vari prodotti.
L'AIPA ha fissato in due Circolari (19 giugno 2000 n. AIPA/CR/24 e n. AIPA/CR/25, n. 151) dei citeri per la risoluzione di alcuni dei problemi che si erano prefigurati già in sede di introduzione della firma digitale.
Nelle citate circolari si è cercato di fissare, *in primis*, la tipologia di certificati cui applicare le linee guida, in secondo luogo, il contenuto e la loro rappresentazione, pur sempre avvertendo che "l'aderenza agli standards internazionali sulla certificazione delle chiavi pubbliche non è sufficiente a garantire la corretta rappresentazione delle informazioni relative all'identificazione del titolare".
Si ricorda, per inciso, che il Regolamento del 1997 (non modificato in sostanza dalla successiva normativa), precisava che il titolare ha tre tipologie di coppie di chiavi: chiavi di sottoscrizione, chiavi di certificazione, chiavi di marcatura temporale, ed è chiaro che in ragione del processo di generazione delle stesse,

---

[78] Nell'ordinamento nazionale tale disposizione è sostanzialmente conforme alla regola generale in tema di inadempimento delle obbligazioni (art. 1218 c.c.), mentre costituisce un'eccezione rispetto alla regola generale di responsabilità aquiliana (art. 2043 c.c.) nella quale il danneggiato deve provare anche la colpa di chi ha provocato il danno.
[79] Ogni certificatore ha scelto di sviluppare un software proprietario, con tutti i costi ad esso connessi.

era quanto mai necessario individuare un sistema idoneo a realizzare uno scambio dei documenti che garantisse la certezza dell'identificazione del titolare.
Scopo delle circolari pertanto era di rendere agevole, anzi di standardizzare il più possibile il sistema di circolazione dei documenti informatici[80].
Innegabile è però il fatto che quanto opinato dalle predette circolari è non ha avuto seguito, preso atto che i diversi certificatori già operanti hanno già reso disponibili i *kit* per generare la coppia di chiavi asimmetriche necessarie per la firma, ma che tali software non sono perfettamente compatibili, tanto da costringere gli utenti, al fine di poter verificare una determinata firma, ad aderire all'offerta di certificatori diversi.
Si deve sottolineare come la scelta di sviluppare diversi *software*, oltre che essere discutibile a fronte dell'obiettivo comune di rendere compatibili i sistemi, è soprattutto discutibile dal punto di vista della sicurezza.
Non ultima una riflessione sul fatto che la maggior parte dei crimini informatici infatti, viene perpetrato all'interno delle istituzioni pubbliche o private o all'interno delle aziende, ad opera di dipendenti infedeli, e che pertanto non è da sottovalutare il pericolo di un uso a rischio della firma digitale in ambienti resi inaffidabili dalle incompatibilità tecnologiche.
Se fosse possibile, ad esempio per il fatto del dipendente infedele, inserire un procedimento di *key recovery* all'interno dei programmi sviluppati dai certificatori, recuperare o rigenerare la chiave privata, gli utenti si troverebbero completamente inermi di fronte alla certa usurpazione della loro chiave privata, con l'aggravante della prova diabolica a proprio carico di dimostrare in un eventuale giudizio che la chiave è stata loro sottratta o crackata e quindi disconoscerne l'utilizzo su di un documento che risulta "firmato".
L'intero sistema della firma digitale appare, allo stato, garantito unicamente dall'affidamento alla correttezza dei certificatori e, quest'ultima, in ogni caso, alla fedeltà dei dipendenti coinvolti nel processo di studio, sviluppo e controllo dei programmi di generazione e di validazione delle chiavi asimmetriche.

5. Firma digitale e sottoscrizione autografa.

Soffermando l'attenzione, in particolare, sulla sottoscrizione, un punto di riferimento obbligato sono gli studi di Francesco Carnelutti[81], in quanto hanno conservato intatta, malgrado il tempo trascorso e l'emanazione dei nuovi codici, tutta la loro validità ed efficacia[82].

---

[80] Cfr. A. MONTONESE, *Interoperabilità della firma digitale*, in Diritto e pratica commerciale, n. 7-8, 2000, p. 1143.
[81] Vedi in particolare, CARNELUTTI, *Studi sulla sottoscrizione,* in *Riv. dir. comm.,* 1929, p. 513.
[82] In essi sono adombrati i requisiti essenziali e le funzioni della sottoscrizione: - una funzione indicativa, consiste nell'identificare l'autore del documento; - una funzione dichiarativa, consistente nell'assunzione di paternità del documento da parte dell'autore dello stesso; una funzione probatoria, in quanto mezzo per provare l'autenticità del documento.

In connessione con le peculiari funzioni attribuite alla sottoscrizione, la dottrina ha attribuito alla stessa determinati requisiti, ritenendo, cioè, che debba essere autografa (scritta di pugno dall'autore), nominativa (riportare il prenome e il cognome dell'autore), leggibile (in modo quindi da consentire l'identificazione dell'autore), non riproducibile (in quanto garanzia di autenticità della provenienza)[83].
La legislazione speciale disciplina peraltro, come già visto al paragrafo precedente, alcune fattispecie in cui il requisito dell'autografia della sottoscrizione può mancare, basti ricordare, per tutti: l'art. 807 c.p.c. nel testo novellato dalla Legge 5 gennaio 1994 n.25, sul compromesso in arbitri; l'art. 15-*quinquies* della Legge 28 febbraio 1990 n. 38, sulle certificazioni d'anagrafe e di stato civile da parte di amministratori comunali; l'art. 6-*quater* del d.l. 12 gennaio 1991 n. 6, convertito in Legge 15 marzo 1991 n. 80 che prevede l'emanazione di atti amministrativi mediante sistemi informatici; infine l'art. 3 d.lgs. 3 febbraio 1993 n. 39 sulla predisposizione di tutti gli atti amministrativi tramite sistemi informativi automatizzati.
Altre norme derogano, ad esempio, al requisito di nominatività della sottoscrizione: così l'art. 602, comma 2, c.c., in tema di sottoscrizione del testamento olografo; l'art. 8 della legge cambiaria (R.D. 14 dicembre 1933 n. 1669, per cui "è valida la sottoscrizione nella quale il nome sia abbreviato o indicato con la sola iniziale"); l'art. 51 n. 12 della legge notarile in tema di firme marginali dell'atto pubblico; la Legge 3 febbraio 1975 n. 18 in tema crocesegno del cieco che non sa apporre la propria sottoscrizione.
L'art. 2705 c.c., riconosce al telegramma, anche non sottoscritto, l'efficacia probatoria della scrittura privata, se l'originale è consegnato o fatto consegnare dal mittente (questo ha fatto supporre addirittura l'eventualità dell'applicazione al telex dell'efficacia probatoria prevista per il telegramma[84]); allo stesso modo,

---

[83] Sui requisiti della sottoscrizione, vedi R. ZAGAMI, "*Firme digitali", op. cit.*. Per una critica alla dottrina tradizionale in tema di requisiti di autografia, nominatività e leggibilità della sottoscrizione, vedi ORLANDI, *La paternità delle scritture,* Milano, 1997, p. 82 ss.. L'autore rileva innanzitutto che i sopraindicati requisiti, non sono prescritti da alcuna norma di legge, e tanto meno dalle norme in tema di validità del contratto e del negozio giuridico. Per quanto attiene specificatamente all'autografia, l'autore rileva come, in realtà, il documento scritto possa dirsi perfetto anche soltanto in presenza della chirografia della sottoscrizione. Quanto alla nominatività e leggibilità, l'autore rileva (a p. 95) come dottrina e giurisprudenza oscillino tra chi considera sottoscrizione soltanto la firma chirografa, con prenome e nome leggibili, e chi invece reputa sufficiente il simbolo, comunque identificabile, e quindi anche lo pseudonimo o la sigla abbreviata, concludendo nel senso che la sottoscrizione debba necessariamente riportare prenome e cognome leggibili "soltanto quando si presenti come unico segno indicativo dell'autore, cioè quando questi non venga espresso in nessun'altra parte del testo", salve le norme di legge (come l'art. 51 della legge notarile) che espressamente prevedono la nominatività in termini rigorosi. La necessità che la sottoscrizione sia comunque non riproducibile in serie (il che sarebbe possibile sia su supporti magnetici che supporti ottici) comporta in ogni caso, la non idoneità delle tecniche informatiche di sottoscrizione mediante "penne magnetiche" o "lavagne elettroniche", su cui vedi ORLANDI, *op. ult. cit.*, p. 100.
[84] In dottrina questa posizione è avallata da C. MANZINI, *Il telex come mezzo di prova*, in Giur. comm., 1978, I, p. 890; e comunque guardata con simpatia da PARISI, *Il contratto concluso mediante computer*, Padova, 1987, p. 56 ss., che pur ritiene l'impostazione errata.; S. PATTI, *Sull'efficacia probatoria del telefax,* in Banca, borsa e titoli di credito, 1990, p. 432; MONTESANO, *Sul documento informatico come rappresentazione meccanica nella prova civile e nella forma negoziale,* in Riv Dir. Proc.,

l'efficacia probatoria del documento prescinde dalla sottoscrizione nelle ipotesi disciplinate dagli artt. 2707, 2708, 2709 c.c..
L'art. 2354 c.c., dichiara "valida la sottoscrizione mediante riproduzione meccanica della firma" sui titoli azionari, purchè l'originale sia depositato presso l'ufficio del registro delle imprese dove è iscritta la società.
Parallelamente, la giurisprudenza, con indirizzo costante, ritiene valida la scrittura privata, in assenza di sottoscrizione (ed anche ove la forma sia richiesta "ad substantiam"), in caso di produzione della scrittura in giudizio dalla parte che non l'ha sottoscritta.[85]
Quanto sopra non toglie, peraltro, che, al di fuori delle eccezioni e delle situazioni particolari, mantenga il proprio vigore il principio generale, in base al quale la sottoscrizione autografa e nominativa è, nell'attuale situazione normativa (e fatto salvo quanto successivamente specificato in ordine al documento elettronico), requisito essenziale della scrittura privata redatta su supporto cartaceo (ed a maggior ragione dell'atto pubblico).
Ciò non significa, peraltro, che la sottoscrizione sia un requisito logico indispensabile della scrittura privata: ciò è comprovato sia dalle eccezioni normative al principio, sia dalla possibilità teorica che sussistano meccanismi alternativi in grado di assolvere con uguale efficacia alle funzioni "indicativa", "dichiarativa" e "probatoria" sopra indicate.
La dottrina ha avuto modo già da tempo, quindi prima della Legge n. 59 del 1997, di approfondire le tematiche del documento elettronico e dei problemi ad esso connessi[86].
Per documento elettronico "in senso stretto"[87]si intende il documento formato dall'elaboratore elettronico, memorizzato in forma digitale e contenuto nella sua memoria centrale o su supporti ottici o magnetici.

1987, p. 5. Anche la giurisprudenza di merito ha più volte dimostrato di voler aderire a tale opinione, ritengono applicabile analogamente l'art. 2705 c.c. Trib. Ascoli Piceno 7 settembre 1980, in *Foro it.* 1980, I, 3090 con osservazioni di PARDOLESI; Trib. Taranto 11 maggio 1981, in *Arch. Civ.* 1982, p. 158 ss. con nota di LUPO; Trib. Trieste 30 settembre 1975, in *Dir Maritt.*, 1976, p. 219. Ritiene applicabile l'art. 2712 Trib. Casale Monferrato 20 luglio 1977, in *Dir. maritt*. 1978, p. 106.

85 Si tratta di giurisprudenza costante: Cass. 23 dicembre 1995 n. 13103, in Mass. Foro It.,1995; Cass. 17 giugno 1994 n. 5868, in Mass. Foro It. 1994; Cass. 7 agosto 1992 n. 9374, in Giust. Civ. 1993, I, p. 2197; Cass. 21 maggio n. 6133, in Giur It. 1993, I, p. 1550, con nota di CIMEI, *In tema di scrittura privata: "crocesegno"; gli "equipollenti" della sottoscrizione.*

86 Esiste già una corposa letteratura sul tema: G. PETRELLI, *op. cit.,* p. 567; GALLIZIA, *Il documento informatico e la sicurezza giuridica,* in Rivista del notariato*,* 1992, I, p. 63; ORLANDI, *La paternità , op. cit.;* GIAQUINTO-RAGOZZO, *Il sigillo informatico,* in Notariato*,* 1997, p. 80; M. MICCOLI, *Cybernotary*, in Notariato*,* 1996, p. 105; R. ZAGAMI, *Firme "digitali", op. cit*, p. 151 ss.; E. GIANNANTONIO, *Manuale di diritto dell'informatica,* Padova, 1994; G. FINOCCHIARO, *op. cit.,* p. 433 ss.; VERDE, *Per la chiarezza di idee in tema di documentazione informatica,* in *Riv. dir. proc.,* 1990, p. 715 ss.; E. GIANNANTONIO, *op. cit.,* p. 261 ss.; V. FRANCESCHELLI, *Computer, documento elettronico e prova civile,* in *Giur. it.,* 1988, IV, p. 314; R. BORRUSO, *Computer e diritto,* Milano 1988.

87 In dottrina si contrappone il documento elettronico in senso stretto, al documento elettronico in senso ampio, inteso quest'ultimo come quel documento, formato con l'ausilio dell'elaboratore, ma successivamente stampato su supporto tradizionale (quindi cartaceo), come i tabulati meccanografici. Vedi in particolare per tale distinzione E. GIANNANTONIO, *op. ult. cit.,* p. 265 ss..

In esso, "il linguaggio elettronico non costituisce semplice documentazione di una volontà già espressa nelle forme tradizionali, ma ne costituisce la forma, intesa come mezzo espressivo necessario di tale volontà"[88]: unico mezzo espressivo, a prescindere da un'eventuale riproduzione su supporto diverso da quello informatico.
La conclusione universalmente condivisa dalla dottrina è quella per cui il documento elettronico è documento in senso giuridico, possiede cioè, non meno del documento cartaceo, tutte le caratteristiche idonee a ricevere e conservare i segni che manifestano una determinata realtà giuridicamente rilevante.
Nel nostro sistema giuridico c'è una sostanziale indifferenza normativa per quanto riguarda il tipo di supporto materiale, così come per il tipo di alfabeto o di linguaggio da utilizzare per la produzione di un documento giuridicamente rilevante. Da ciò si è ricavata, da tempo, la conseguenza dell'ammissibilità di deposito di *software* presso il notaio, facendo leva sull'ampio significato del termine "documenti", che il notaio può ricevere in deposito ai sensi dell'art. 1 del R.D. 14 luglio 1937 n. 1666.
Altro risultato acquisito da parte della dottrina prevalente è "l'identificazione della cosiddetta forma elettronica con la forma scritta"[89].
Un'opinione piuttosto diffusa ha incisivamente affermato che con il computer, l'energia elettrica (o più precisamente, il flusso di elettroni tramite il quale si registrano dati in forma numerica binaria (*bit*) su un supporto idoneo, come un floppy disk, o un cd-rom), è diventato il nuovo mezzo di scrittura dell'umanità: il "nuovo inchiostro" di cui l'uomo si serve.

---

88 E. GIANNANTONIO, *op. ult. cit.,* pp. 262-263.

89 La dottrina dominante afferma l'identità tra forma scritta e documentazione su supporto elettronico: GIANNANTONIO, *Manuale di diritto dell'informatica,* op. cit., p. 347; PARISI, *op. cit.,* p. 64; nel senso invece che la forma elettronica costituirebbe un 'tertium genus' rispetto alla forma scritta ed alla forma verbale, CLARIZIA, *op. cit.,* p. 100 (secondo il quale la forma elettronica è una forma dematerializzata, né scritta, né orale, pur partecipando maggiormente dei caratteri dello scritto). Le obiezioni effettuate alla ricomprensione della forma elettronica in quella scritta, sembrano peraltro facilmente superabili, in quanto: non appare decisivo il requisito della "leggibilità a occhio nudo", perché diversamente dovrebbe negarsi carattere di scrittura al documento redatto in caratteri microscopici o in un linguaggio cifrato o comunque non immediatamente comprensibile, ma decifrabile; il fatto che risulti necessario tradurre i segnali elettrici e/o magnetici in segnali visibili, attraverso il monitor o la stampante, non toglie che sia comunque soddisfatta l'esigenza di conoscibilità del messaggio contenuto sul supporto elettronico, al pari di quello incorporato in un supporto cartaceo. Nel senso che l'esigenza di riconoscibilità ed accessibilità, propria della forma, è soddisfatta anche dal documento elettronico, ORLANDI, *La paternità delle scritture,* op. cit. p. 501 ("La memoria elettronica conserva i segnali delle digitazioni sotto forma di impulsi magnetici, ridotti in unità informatiche (i *bit*): questi impulsi non sono di per sé percepibili direttamente dai sensi dell'uomo, ma si offrono alla decodificazione della macchina attraverso il codice binario, il quale consente di convertire le lettere ed i simboli di un alfabeto corrente, in unità di senso, proprie del sistema binario, e viceversa. La memoria elettronica, dunque, è già in sé un testo intelligibile, poiché può essere letto attraverso la decodificazione binaria: che il nudo senso umano sia insufficiente alla lettura del testo non muta punto la natura del fenomeno, dato che non esiste una modalità tipica ed esclusiva della percezione sensoriale. L'osservante sarà chiamato ad utilizzare la macchina informatica, alla stregua di una lente di ingrandimento").

Nasce così un nuovo tipo di documento, rispetto al quale le memorie elettriche o elettroniche non sono altro che la "nuova carta", il nuovo supporto e i *bit* (nella combinazione necessaria per rappresentare ogni carattere alfanumerico) non sono altro che il "nuovo alfabeto"[90], universale e internazionale.
Nel campo dei rapporti civili è indubbio che le norme sulla "forma" dei contratti e quelle sulle prove documentali hanno avuto per presupposto la convinzione che di solito lo scrivere consiste nell'apporre "nero su bianco".
Nell'ambito civilistico, però, non vi è alcuna disposizione che escluda altri modi di scrivere e di documentare[91], né prescrive quali debbano essere i mezzi tecnici di registrazione dei segni, i supporti e gli alfabeti, né che i segni costituenti lo scritto debbano poter essere letti in qualunque momento ad occhio nudo, né che i segni attraverso i quali si estrinseca la scrittura debbano essere indelebili, né, infine, che il supporto debba essere indistruttibile[92].
Prima dell'emanazione della Legge 59/1997, la dottrina più attenta segnalava, in assenza di un apposito intervento normativo che prevedesse un equipollente della firma autografa, l'impossibilità di formare con lo strumento informatico una scrittura privata ai sensi degli artt. 2702 ss. c.c., non potendosi apporre alla fine del documento elettronico la sottoscrizione di pugno dell'autore (questa considerata come essenziale requisito della scrittura privata).
Ciò portava a ridurre di molto la rilevanza giuridica del documento elettronico (essenzialmente a quelle fattispecie, e per quegli effetti per i quali la legge non prevede la sottoscrizione).
Può tuttavia affermarsi che il documento elettronico avrebbe sempre potuto costituire principio di prova per iscritto ai sensi dell'art. 2724 c.c.[93], infatti, come ha più volte sottolineato la giurisprudenza, non è necessario che il principio di prova scritta sia sottoscritto da colui contro il quale viene richiesta la prova testimoniale[94], né che la sottoscrizione sia riconosciuta[95].

---

[90] VERDE, *Per la chiarezza delle idee in tema di documentazione informatica*, *op. cit.,* p. 719. In senso contrario, CIAN*, Forma solenne e interpretazione del negozio*, Padova, 1969, almeno in relazione ai negozi in forma vincolata, rispetto ai quali sarebbe impossibile ammettere l'uso di segni e di suoni che "nulla dicono a un possibile lettore senza la mediazione di una ulteriore manifestazione di linguaggio, la quale peraltro rimarrebbe esterna alla dichiarazione stessa, anche se con essa funzionalmente collegata" (p. 165).

[91] E. GIANNANTONIO, *op. cit.,* p. 276.

[92] Ciò a prescindere dal fatto che, con l'attuale evoluzione tecnologica, alcuni tipi di supporto informatico (in particolare, i supporti ottici, non riscrivibili, e le memorie ROM e WORM) offrono garanzie di affidabilità, di durata e di inalterabilità di gran lunga maggiori dei supporti cartacei; d'altra parte, esistono tecniche di formazione e trasmissione dei documenti elettronici che offrono garanzie di sicurezza (ad esempio contro i rischi di falsificazione) sicuramente maggiori rispetto ad analoghi documenti redatti su supporto cartaceo.

[93] Articolo rubricato "Eccezioni al divieto della prova testimoniale".

[94] Un esempio è il caso in cui l'uso dei mezzi elettronici sia diventato una pratica comune e consuetudinaria, come nel caso dei trasferimenti elettronici di fondi, il giudice potrebbe, ai sensi del capoverso dell'art. 2721 c.c., ammettere la prova per testimoni dei contratti anche quando il valore dell'oggetto ecceda le lire cinquemila. In questi casi, anzi, il giudice potrebbe forse giungere a considerare il documento elettronico come sottoscritto, qualora non ne sia contestata la provenienza.

[95] Cass. 64/461; 75/1047. Occorre, naturalmente, che dal documento risulti la provenienza dalla persona contro la quale è diretta la domanda ovvero dal suo rappresentante.

6. La firma digitale autenticata e la marcatura temporale.

La firma digitale, dunque, apposta con il sistema delle doppie chiavi a crittografia asimmetrica, ha il vantaggio di assolvere a tutte le funzioni che, secondo la dottrina dominante[96], vengono attuate dalla firma autografa, e precisamente la funzione dichiarativa, quella indicativa e quella probatoria: ne consegue che anche la firma digitale è passibile di autenticazione.
L'autentica di una firma digitale può apparire superflua se ad essa si assegna solo la funzione di accertamento della provenienza soggettiva del documento informatico. Una tale certezza è raggiungibile mediante la verifica del certificato, già emesso previo accertamento dell'identità personale del richiedente; l'autenticazione di una firma digitale si giustifica però, qualora si riconosca che la funzione dell'autentica non si esaurisce nella sola certificazione della provenienza soggettiva, quando cioè comporta anche un controllo di legalità da parte del notaio sul contenuto del documento informatico sottoscritto[97].
In questo frangente, l'art. 16 prevede che il pubblico ufficiale autenticante attesti, oltre il fatto che "la firma digitale è stata apposta in sua presenza" (artt. 2703, comma 2, c.c. e 72 l. not.)[98], che "il documento sottoscritto corrisponde alla volontà della parte (art. 47, comma 3, l. not.) e non è in contrasto con

---

96 A titolo esemplificativo vedi R. ZAGAMI, *Firme "digitali", crittografia e validità del documento elettronico,* in Diritto dell'informazione e dell'informatica*,* 1996, p. 153 ss.; Id., *La firma digitale tra soggetti privati nel regolamento concernente "atti, documenti e contratti in forma elettronica",* in Diritto dell'informazione e dell'informatica, 1997, p. 905 ss.; S. Patti, *Informatica e nuovi documenti,* in *Dir. banc.,* 1997, p. 203-206; F. Orlandi, *Il regolamento sul documento elettronico: profili ed effetti,* in Rivista di diritto commerciale*,* 1998, p. 748-750. F. Ferrari, *op.cit.,* p. 140-142.

97 Per l'applicabilità dell'art. 28 l. not. alle scritture private autenticate è la maggioranza della dottrina notarile (vedi, tra i tanti, P. BOERO, *La legge notarile commentata*, Torino, 1993, p. 169 ss.; G. CASU, *L'atto notarile tra forma e sostanza*, Milano, 1996, p. 389 ss.; P. TONALINI, *La sottoscrizione elettronica dei documenti*, in Studium Iuris, 1997, p.442 ss.) e la giurisprudenza, (in Massimario del Foro Italiano, vol. LXIII, 1994 , voce *Notaio, compravendita immobiliare, scrittura privata autenticata, obblighi del notaio:* "L'obbligo di procedere al preventivo accertamento della libertà del bene con le visure ipotecarie e catastali sussiste unicamente quando al notaio venga conferito l'incarico di preparare e redigere un atto pubblico di vendita, cioè nei casi, in cui egli dirige personalmente la compilazione integrale dell'atto previa indagine della volontà delle parti, in modo da tradurre la volontà stessa in uno strumento negoziale idoneo a conseguire i risultati voluti, e non anche quando - salvo che al notaio sia stato conferito quello specifico incarico - egli si limiti all'autentica delle firme delle parti contraenti poste in calce ad una scrittura privata, già predisposta dagli stessi contraenti", Cass. Civ. n. 2699/1994) ; *contra* Cass. Pen. n. 2720/1990. Nel codice deontologico approvato dal Consiglio Nazionale del Notariato il 24 febbraio 1994, è stabilito che il notaio "deve controllare la legalità del contenuto della scrittura e la sua rispondenza alla volontà delle parti". Un disegno di legge approvato dal Consiglio dei Ministri il 29 novembre 1997, prevede l'espressa estensione dell'art. 28 l. not. alle scritture private.

98 Nel rispetto della *ratio* della norma che prescrive la "presenza", questa in futuro potrebbe ritenersi ugualmente soddisfatta da una "presenza virtuale", realizzata mediante sofisticati sistemi di videoconferenza, in modo che il notaio possa, anche a distanza, indagare la volontà del "comparente", accertarsi della sua identità personale e del fatto che la firma digitale sia stata effettivamente apposta da lui stesso e non da altri.

l'ordinamento giuridico, ai sensi dell'art. 28, n.1, della l. 16 febbraio 1913, n. 89 (legge notarile)".
Il notaio o altro pubblico ufficiale sottoscrive l'autentica apponendo la propria firma digitale (art. 16, comma 3), la quale sostituisce "l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi comunque previsti" (anche art. 10, comma 6)[99].
In considerazione del loro superiore grado di importanza, è stabilito che la certificazione e la pubblicazione delle chiavi pubbliche dei notai e degli altri pubblici ufficiali non appartenenti alla pubblica amministrazione, è compiuta in modo autonomo dai soggetti diversi dai certificatori ex art. 8, comma 3, e con modalità che verranno indicate da successive leggi e regolamenti (art. 17, comma 3).
In una prospettiva di equiparazione fra documento cartaceo e documento informatico, la firma digitale autenticata ai sensi dell'art. 16, si considera come riconosciuta ai sensi dell'art. 2703 c.c. e farà piena prova della provenienza delle dichiarazioni da parte di chi ha sottoscritto il documento informatico, anche se colui contro il quale è prodotto, non riconosce la sottoscrizione, salvo l'esperibilità della querela di falso (art. 2702 c.c.)[100].
Le conseguenze di questa simmetria fra i due tipi di documentazione sono "rivoluzionarie", in quanto potrebbero essere stipulati in originale ed in forma esclusivamente informatica tutti, o quasi, gli atti giuridici ammessi nel nostro ordinamento, con esclusione di quelli per i quali è richiesta la forma minima dell'atto pubblico.
Gli atti così stipulati potranno essere direttamente immessi nei pubblici registri immobiliari (art. 2657 c.c.)[101] e nel registro delle imprese (art. 2189, comma 2, c.c.)[102], anche mediante trasmissione telematica in via definitiva, della richiesta (nota o domanda) e del titolo[103].
In perfetta applicazione del regolamento, si può affermare che costituisca forma scritta e soddisfi letteralmente i requisiti richiesti dall'art. 1350 c.c., un documento informatico, con autentica notarile, recante la registrazione audio e video della conclusione di un negozio (da trascrivere mediante indicizzazione non automatica del contenuto).

---

[99] Cfr. anche quanto commenta sul punto F. DE SANTIS, *La disciplina normativa del documento informatico*, in Corriere Giuridico, 1998, p. 390.
[100] Cfr. R. ZAGAMI, *La firma digitale, op. cit.,* p. 914.
[101] Attualmente "la formalità si intende richiesta quando viene presentato in conservatoria (…) il titolo relativo (su carta), anche se la produzione del supporto informatico o la trasmissione telematica sia avvenuta in precedenza". L'art. 10, comma 19, del d.l. 323/1996 inoltre, stabilisce che il richiedente la formalità, "fermo restando l'obbligo di presentare (…) il titolo nelle forme richieste dal codice civile, può altresì produrre il contenuto del titolo stesso su supporto informatico".
[102] Il regolamento di attuazione (d.p.r. 581/1995) all'art. 8 della Legge 580/1993, prevede il rilascio telematico dei certificati (art. 2 lett *d*) e la possibilità di presentare la domanda anche su supporto informatico (art. 11), ma non anche la trasmissione telematica della domanda, ritenendo la Commisione che ha redatto il regolamento, di escludere tale possibilità per la necessità di autenticazione posta dal codice civile.
[103] Vedi R. ZAGAMI, *Firme 'digitali', crittografia e validità del documento elettronico, op.cit*, p. 169.

Nuove prospettive si aprono anche per la forma del testamento, per cui, accanto a quello olografo, potrebbe così assumere valore anche quello nuncupativo[104].

Il compito di autenticare firme digitali è attribuito al "cybernotary"[105], una nuova figura di professionista nell'ordinamento statunitense, delineato nell'ambito dell'*American Bar Association* (ABA), e suggellato per la prima volta con legge nello stato della Florida[106], la cui istituzione deriva dalla diversità di tradizioni giuridiche tra i sistemi di *common law* e quelli di *civil law* e, quindi, dall'esigenza di rendere i documenti giuridici provenienti dai primi, accettabili nei secondi.[107]

Come è noto, l'ordinamento statunitense non conosce la figura del notaio quale è nei Paesi di *civil law*, come l'Italia.

Il *public notary* è un semplice certificatore e non ha alcun dovere di verificare la conformità alla legge del contenuto dell'atto che gli è sottoposto per l'autenticazione.

Il *cybernotary*, invece, avrà il compito di assicurare la legalità dei documenti destinati all'estero (*authentication*), affinchè essi non siano respinti dall'ordinamento destinatario, costituendo così un ponte di collegamento tra le due tradizioni giuridiche. I requisiti che dovrà possedere il *cybernotary* saranno l'abilitazione all'esercizio dell'avvocatura, la conoscenza di diritto straniero e nozioni non superficiali di informatica e telematica, con particolare riguardo ai sistemi di firma digitale[108].

Il regolamento non prevede la redazione di un atto pubblico notarile originale in forma informatica. L'efficacia probatoria privilegiata e la complessità della Legge notarile (Legge. 89/1913) e della Legge. 15/1968, hanno evidentemente sconsigliato tale eventualità.

Si deve rilevare inoltre, la minore utilità della firma digitale per la conclusione degli atti notarili, dato che non potrebbero in ogni caso essere conclusi telematicamente.

---

104 Con le firme digitali, la funzione del notaio non è sminuita, ma piuttosto è richiesta nei suoi compiti di maggior valore professionale (funzione di adeguamento e controllo di legalità). Mentre l'intervento notarile diventerebbe invece eccessivo, per i compiti di mera certificazione, nei casi in cui l'autentica è richiesta esclusivamente ai fini di un controllo della provenienza soggettiva (autentica non negoziale), poiché sarebbe perfettamente funzionale una firma digitale anche non autenticata.

105 Vedi R. ZAGAMI, *La firma digitale, op. cit.,* p. 915; e P. TONALINI, *op.cit.,* p. 444; e inoltre M. MICCOLI, *Cybernotary,* in Notariato*,* 1996, p. 105.

106 *Electronic Commerce Act*; anche lo stato dello Utah ha redatto un progetto di *Act on Electronic Notarization*. Nella legge della Florida si è preferito usare la diversa locuzione di "international notary", in quanto l'uso delle firme digitali e degli strumenti informatici da parte di questi nuovi professionisti è opzionale. Vedi per la legislazione della Florida il sito http://www.leg.state.fl.us/session/1996 .

107 Vedi M. MICCOLI, *op. cit.*, p. 105 ss.; ABA*, Resolution concerning the cybernotary: an international computer-transation specialist,* 2 agosto 1994.

108 Il regolamento non istituisce evidentemente, una nuova figura di *cybernotary*, in quanto le sue funzioni di autenticazione sono già per tradizione secolare patrimonio del notariato italiano.

A differenza delle scritture private autenticate, infatti, è richiesta la contestuale presenza delle parti davanti al notaio per la lettura e la sottoscrizione[109].
L'utilità si rinviene invece, quando occorre duplicare o trasmettere telematicamente il documento pubblico già concluso.
Non potendo essere redatto un atto pubblico originale in forma informatica, si farà una copia informatica di un atto pubblico redatto su carta.
È stabilito, infatti, che i documenti informatici contenenti copia di un atto pubblico, se spediti o rilasciati dai depositari pubblici autorizzati e dai pubblici ufficiali, hanno piena efficacia probatoria ai sensi dell'art. 2714 c.c., ovvero "fanno fede come l'originale", se ad essi è apposta la firma digitale di colui che li spedisce o rilascia. La produzione o esibizione dell'originale cartaceo non è richiesta, essendo sufficiente ad ogni effetto di legge, la sua copia informatica[110].
Un'altra esigenza che potrebbe essere risolta dall'intervento del notaio sul documento elettronico, è l'attribuzione allo stesso della data certa.
La data, che è "la rappresentazione documentale delle condizioni di luogo e di tempo in cui un atto è avvenuto; oppure, tenendo conto dell'importanza prevalente del documento scritto, la indicazione scritta delle circostanze di tempo e di luogo che individuano un atto", è una dichiarazione aggiuntiva, non un elemento costitutivo necessario.
In alcuni casi la legge richiede, però, in considerazione di specifiche esigenze, la menzione della data come condizione di validità di una certa dichiarazione (si pensi all'esempio del testamento olografo), ma questo non vuol dire che la data allora assurga a elemento strutturale della dichiarazione resa in forma scritta[111].
In relazione ai rapporti fra le parti, essa è interamente assoggettata all'art. 2702 c.c., ovvero la sottoscrizione riconosciuta o considerata legalmente come tale (escluso il caso dell'autenticazione) costituisce prova legale della provenienza della data, ma non della sua veridicità. Il giudice quindi, può valutare, secondo il suo prudente apprezzamento, se la data è vera o falsa e le parti saranno ammesse a fornire la prova contraria.
La sicurezza della datazione del documento, e della sua veridicità, potrebbe essere assicurata dall'apposizione allo stesso di una dichiarazione, da parte del notaio, contenente la data, come avviene per l'attuale autentica di scrittura privata.
Successivamente il documento sarebbe di nuovo cifrato dal notaio, con l'utilizzo della propria chiave segreta, che svolgerebbe la funzione di una sorta di "sigillo elettronico"[112].

---

[109] Vedi in questo senso, G. CASU, *op. cit.,* p. 266 s.; DI FABIO, *Manuale di notariato*, Milano, 1981, p. 156.
[110] La sussistenza di un originale cartaceo dovrebbe essere anche funzionale alla risoluzione di eventuali controversie che potrebbero derivare dall'applicazione di una normativa ancora nuova e sperimentale. In mancanza di un originale cartaceo dell'atto pubblico, potrebbe riconoscersi piena efficacia probatoria alla sua copia digitale in base all'art. 2716 c.c..
[111] Sul punto vedi A. GRAZIOSI, *Premesse ad una teoria probatoria del documento informatico,* in Rivista trimestrale di diritto e procedura civile, 1998, p. 519.
[112] Vedi RAGOZZO e GIAQUINTO, *Il sigillo informatico*, in *Notariato*, 1997, p. 80. Vedi anche M.C. ANDREINI, *Forma contrattuale, formalismo negoziale e documentazione informatica,* in Contratto e

Nel rapporto tra le parti del negozio giuridico documentato e i terzi, la data interviene a risolvere ogni possibile conflitto circa l'anteriorità delle dichiarazioni documentate.
Chiunque entri in contatto con il documento, può agevolmente verificare che esso è stato "autenticato" dal notaio in una determinata data, che sarebbe la data certa del documento.
Ogni successiva falsificazione della data o alterazione del documento, risulterebbe in modo evidente, perché renderebbe impossibile la decifratura.
Il risultato di questa procedura informatica eseguita dalla cosiddetta terza parte fidata, è definito "validazione temporale": in questo modo si attribuiscono ad uno o più documenti informatici una data e un orario opponibili a terzi (art. 1, lett. 'b' del regolamento).
Il Regolamento non individua la terza parte fidata, rinviando alle regole tecniche, *ex* art. 3, comma 1, del Regolamento[113]; giuridicamente si realizza sostanzialmente l'effetto civilistico della registrazione degli atti già svolta dagli uffici del registro (art. 2704 c.c. e art. 18 d.p.r. 131/1986).
Orbene, ad una prima analisi del *corpus* normativo sulla firma digitale, si evince la "dissociazione fra l'evidenza fisica della persona e le sue manifestazioni (in primo luogo l'autografia), e la sua evidenza informatica"[114].
Fondamentale elemento rivelatore di questa "dissociazione" consiste nel fatto che il momento di apposizione della firma digitale e della data del documento stesso è diverso da quello in cui avviene il riconoscimento della validità della stessa: il procedimento di formazione della firma digitale infatti, necessita di una pluralità di fasi, a partire dalla cosiddetta. "apposizione dei sigilli informatici", cioè delle chiavi di cifratura, fino alla certificazione finale della validità del documento (perfezionato digitalmente nel suo contenuto estrinseco), da parte di un soggetto terzo ed imparziale, l'Autorità di certificazione, appunto.
L'ultimo passaggio che convalida la "sottoscrizione digitale" consiste, si è detto, nell'applicare al documento un sigillo temporale che possa certificare inequivocabilmente la data e l'ora di formazione del documento informatico.
La definizione di questa chiave di marcatura temporale è fornita dall'art. 1 del Regolamento del 1997 dove si stabilisce che "la validazione temporale è il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili a terzi".
Nell'autenticazione ex art. 16 è già ovviamente ricompresa una validazione temporale (art. 2704 c.c.), che rappresenta un minus rispetto alla prima, dato che non presuppone l'esistenza di una scrittura privata e non comporta alcuna indagine sulla volontà ed identità dei sottoscrittori e sul contenuto dell'atto.

Impresa*,* 2001, p.196-197; *Id.aut.,Dal tabellione al sigillo elettronico,* in Vita notarile*,* 1998, p.1777 ss..

113 Il servizio di validazione temporale (*time-stamping*) rientra nei cosiddetti "ancillary services" (*key repository*, *escrow service*, *confirmation service*, *key generation service*, ecc.), i quali possono essere svolti dagli stessi certificatori o da soggetti diversi.

114Osservazione di F. SARZANA DI SANT'IPPOLITO, Il Corriere Giuridico*,* n.7, 1999, p. 804, già rilevata da N. IRTI, *Idola libertatis,* Milano, 1985.

Anche per i documenti così certificati varrebbe l'osservazione circa la possibilità, da parte di chiunque, di creare un'infinita molteplicità di originali in luogo di copie.
Ferma restando l'impossibilità di modificarne il contenuto, il documento elettronico potrebbe essere facilmente riprodotto, conservando lo stesso valore.
In mancanza di un'autenticazione *ex* art. 16, e mancante anche una validazione temporale, la data di un documento informatico con firma digitale (in quanto scrittura privata *ex* art. 5, comma 1) potrà essere accertata ai sensi dell'art. 2704 c.c. (ma in certi casi solo fino a quando non è scaduta, revocata o sospesa la relativa chiave)[115].
L'elaborazione dei concetti giuridici di documentazione e di documento, si avvale, principalmente, dell'autorevole contributo di Francesco Carnelutti[116], al quale sono seguiti, nel tempo, una serie di interventi dottrinali e giurisprudenziali[117], che non hanno, peraltro, alterato l'impostazione fondamentale dallo stesso fornita.
Documento (da *docere*: insegnare, far conoscere) è stato quindi definito, volta per volta: "cosa che fa conoscere un fatto"[118]; "res signata (un oggetto percepibile, recante segni), onde è dato pronunciare il giudizio di esistenza di un fatto, che sia sussumibile sotto un tipo normativo"[119]; "cosa corporale, semplice o composta, idonea a ricevere, conservare, trasmettere, la rappresentazione descrittiva o emblematica o fonetica di un dato ente, giuridicamente rilevante"[120]; "cosa rappresentativa", i cui elementi essenziali sarebbero pertanto "la cosa cui si riconosce tale significato, la rappresentazione che essa fornisce ed il fatto rappresentato con quest'ultima"[121]; "qualsiasi supporto visivo, fonico, magnetico o cartaceo sul quale sono impressi segni comunicativi in grado di essere percepiti dall'uomo direttamente o attraverso l'impiego di particolari strumenti"[122].
Fondamentale, secondo quanto emerge dalle definizioni riportate, non è solo il supporto fisico, materiale, destinato ad incorporare la rappresentazione di un

---

115 La sospensione dovrebbe essere una misura cautelare e strumentale, da adottarsi con urgenza nei casi in cui non sia prontamente accertabile il fondamento dei presupposti per la revoca. In seguito, il certificatore farà le opportune indagini che potranno condurre alla revoca definitiva, oppure al ripristino di validità del certificato. Pertanto durante il periodo di sospensione, si deve mantenere la segretezza della chiave privata.
116 F. CARNELUTTI, *Documento, op. cit.,* p. 85 ss.(dove sono citati anche gli altri contributi dell'Autore in materia). Questo contributo era già apparso nel 1937 nel *Nuovo Digesto Italiano.*
117 Tra i principali interventi, vedi in particolare: N. IRTI, *Sul concetto giuridico di documento,* in *Studi sul formalismo negoziale,* Padova 1997, p. 159 ss.(e già in Rivista trimestrale di diritto e procedura civile*,* 1969); IRTI, *Il contratto tra faciendum e factum,* in *Studi sul formalismo negoziale,* cit., p. 95 ss. (e già in Rassegna di diritto civile*,* 1984, p. 938 ss.); DI SABATO, *Il documento contrattuale,* Milano, 1997; VERDE, *Prova documentale (Dir. Proc. Civ.),* in *Enc. Giur. Treccani*, XXV, Roma 1991; DENTI, *Prova documentale (Dir. Proc.Civ.),* in *Enc. Dir,* XXXVII, Milano 1989, p. 713 ss..
118 CARNELUTTI, *Documento (teoria moderna), op. cit.,* p. 86.
119 IRTI, *Sul concetto giuridico di documento,* op. cit., p. 196.
120 CANDIAN, *Documentazione e documento (teoria generale),*in Enc. Dir., XIII, Milano 1964, p. 579 ss.
121 ANGELICI, *Documentazione e documento (diritto civile),* in *Enc. Giur. Treccani,* Roma 1989.
122 DI SABATO, *Il documento contrattuale,* op. cit., p. 35.

fatto, ma soprattutto l'esistenza di segni che manifestano una data realtà esterna, giuridicamente rilevante (segni che assumono, nell'ipotesi di documento grafico, la veste di dichiarazione)[123].
Oltre al supporto documentale, altro elemento essenziale del documento è la rappresentazione, in esso contenuta ed incorporata tramite segni: rappresentazione che può essere di vario tipo (grafica, fotografica, fonetica, ecc.), tanto da rendere il documento grafico (in cui il segno è rappresentato dalla scrittura) solo una species del più ampio *genus* documentale. Documento e scrittura, generalmente identificati nel comune linguaggio, in realtà, quindi non coincidono[124].
Altra distinzione fondamentale è poi quella tra documento e documentazione: come è stato chiarito, mentre il documento è la cosa, la *res signata*, la documentazione è l'attività, il fare, a seguito del quale la cosa diviene signata.
Sotto questo profilo, è utile rilevare come la legge notarile (Legge 16 febbraio 1913, n. 89), agli artt. 51 e seguenti, regoli essenzialmente l'attività di documentazione, ossia l'attività notarile diretta a redigere la dichiarazione del notaio stesso, relativamente alle dichiarazioni delle parti e ai fatti avvenuti in sua presenza: solo di riflesso, viene disciplinato, in tali norme, il contenuto del documento notarile[125].
Chiarito, nei tratti fondamentali, il concetto di documento, si può evidenziare ora la differenza tra tale concetto e quello di forma del negozio giuridico: la dottrina ha chiarito che la forma coincide con la documentazione (come è stato incisivamente affermato, nell'ipotesi di forma scritta, "la forma sta nello

---

123 CARNELUTTI, *Documento (teoria moderna), op. cit.*, p. 86 ("Poiché il più antico e ancora il più diffuso tra i mezzi documentali è la scrittura e, oggi, la materia sulla quale si scrive è la carta, per lo più il documento è cartaceo…Ma il vero è che qualunque materia, atta a formare una copia rappresentativa, può entrare nel documento: tela, cera, metallo, pietra, e via dicendo"); CANDIAN, *Documentazione e documento (teoria generale), op.cit.*, p. 579 ("forma consta insolubilmente dell'elemento corporale o materiale mediante il quale l'evento diventerà percepibile -carta, pietra (ad esempio, lavagna); nastro magnetico; pellicola cinematografica; disco di grammofono; lastra radiografica; "negativa" fotografica (e cartoni che ne riprodurranno l'immagine); fonometro; ecc.") e p. 593 ("Si tratta di una cosa, normalmente, mobile. Non è escluso che un documento possa qualificarsi bene immobiliare, se si pensa, ad esempio, ad un documento lapideo, inserito in un muro, o comunque in un elemento strutturale di un edificio"). Significativo è quanto afferma la dottrina e riportato da G. PETRELLI (*op.cit.,* p. 568, nota n. 12), in tema di testamento olografo: "La scrittura…può esser fatta su qualunque materia idonea e con qualunque mezzo idoneo, quindi anche su pergamena, sulla tela, sulla seta, sul cuoio e non soltanto coll'inchiostro, ma anche col lapis o con un'altra materia colorante qualsiasi. La scrittura può anche eccezionalmente essere fatta su un muro o su una tavola di legno con un pezzo di carbone, o con una materia colorante, ovvero col gesso su dei mattoni o su una lavagna, ovvero mediante incisione, con una punta acuminata, sul legno, sul marmo o sul metallo" (GANGI, *La successione testamentaria* ,I, Milano 1964, p. 129-130).
124 L'erronea identificazione fra documento e scrittura viene rilevata da CARNELUTTI, *Documento (teoria moderna),* op. cit., p. 86: "come vi è nell'uso una sinonimia tra documento e scrittura, così vi è tra documento e carta, nel senso che scrittura e carta si adoperano per antonomasia, con significato di documento".
125 G. PETRELLI, *op. cit.,* p. 569.

scrivere"[126], cioè nell'attività dello scrivere, e non nello scritto inteso come risultato dell'attività)[127].
Nell'ambito della forma, una particolare importanza riveste notoriamente la forma scritta, nell'ambito della quale occorre ulteriormente distinguere (art. 1350 c.c.) tra atto pubblico e scrittura privata. Quest'ultima, disciplinata dal codice civile agli artt. 2702 e seguenti, non è tuttavia definita dallo stesso codice.
La dottrina, ricavando una definizione di scrittura privata come documento sottoscritto da un privato senza la partecipazione nell'esercizio delle sue funzioni di un pubblico ufficiale, individua concordemente alcuni elementi essenziali e caratterizzanti la scrittura privata[128].
Nessuna norma disciplina il tipo di linguaggio che occorre utilizzare per potersi avere scrittura privata: conseguentemente si è ritenuto, in dottrina e giurisprudenza, che anche il crittogramma, o messaggio segreto o in cifra, in quanto sottoscritto, sia scrittura privata, astrattamente idonea ad essere oggetto di perizia per scoprirne la "chiave".

7. Il documento informatico.

La materia della prova documentale ha conosciuto una rapida e profonda evoluzione. Soprattutto i progressi compiuti dall'informatica hanno posto dottrina e giurisprudenza di fronte all'esigenza di individuare la disciplina di nuove forme di documentazione, che si sono affermate nella pratica quotidiana e sembrano destinate ad acquistare un rilievo sempre maggiore.
La rapida diffusione dell'informatica, soprattutto fra gli operatori economici, attraverso lo scambio di informazioni o il perfezionamento di impegni contrattuali, ha indotto i Legislatori di tutti gli ordinamenti giuridici ad adottare progressivamente iniziative grazie alle quali la nozione di documento informatico è entrata nella considerazione del giurista.
L'impiego dell'informatica nel campo documentaristico comprende sia la predisposizione, con strumenti elettronici adeguati, di *microfilm*, sia il confezionamento, con procedura computerizzata, di appositi tabulati con contenuti e funzioni assai vari sia, infine, l'archiviazione su speciali supporti magnetici (*floppy disk*, *Cd-Rom*) di dati e notizie per diverse finalità.

---

126 Cfr. N. IRTI, *Il contratto tra* faciendum *e* factum*, op. cit.*, p. 113: "Forma scritta è lo scrivere, l'esprimersi scrivendo; scritto è il documento, la cosa, labile o duratura, su cui si fissano i segni grafici".
127 Vista la differenza da un altro punto di vista, si potrebbe dire che, mentre il documento ("factum") attiene al profilo della prova, la forma ("faciendum") attiene al momento dell'attività.
128 Il documento, cioè una cosa recante un insieme di segni grafici in forma di linguaggio; la dichiarazione, cioè il fatto rappresentato, documentato con espressioni linguistiche; la sottoscrizione, consistente nell'apposizione autografa del nome e del cognome dell'autore dello scritto in calce allo stesso; la provenienza, essendo la scrittura privata formata da un privato, e non da un pubblico ufficiale nell'esercizio delle proprie funzioni.

A tali ipotesi di utilizzazione nell'ambito del commercio giuridico devono essere aggiunte quelle in cui l'impiego del computer non è direttamente finalizzato ad ottenere un documento ma, semplicemente, a 'colloquiare' con altri elaboratori attraverso reti telematiche.
Il computer diventa così lo "strumento che incide direttamente nel processo di formazione della volontà negoziale, (…) il luogo d'incontro di volontà già perfezionate"[129].
In questo contesto è sorto il problema di stabilire quale valore probatorio debba riconoscersi ai tanti elaborati informatici che, a volte, si presentano come testi scritti incorporati su un supporto semplicemente magnetico, ma non sottoscritti. Il fatto che gli operatori economici e giuridici comunichino attraverso segnali trasmessi da apparati meccanici (telex, telefax e posta elettronica, ad esempio) ha ridotto il ricorso alla firma autografa quale criterio di assunzione della paternità del documento, tanto da far pensare ad una "crisi della sottoscrizione"[130].
L'assenza di firma autografa ha sostanzialmente impedito agli interpreti di ricondurre il documento informatico sotto la *species* di scrittura privata, e li ha spinti generalmente ad inquadrare il fenomeno nel contesto delle prove documentali di cui all'art. 2712 c.c.[131], che, riferendosi ad ogni riproduzione meccanica di fatti e di cose, consente di disciplinare l'efficacia probatoria dei documenti prodotti da qualsiasi strumento meccanico, al quale può equipararsi quello informatico[132], ma non consente di risalire ai termini di decadenza o alle

---

129 Così F. DE SANTIS, *La disciplina normativa del documento informatico,* in Corriere Giuridico*,* 1998, p. 384 ss., e, precedentemente, F. PARISI, *Il contratto concluso mediante computer* , Padova, 1987, p. 4 ss.. Sull'argomento cfr. anche R. CLARIZIA, *Informatica e conclusione del contratto*, Milano, 1985; F. BUFFA, *Il mercato telematico di borsa: la conclusione del contratto,* in Diritto della banca e del mercato finanziario, Padova, 1991, p. 548 ss.

130 Il fenomeno è già stato posto in luce da N. IRTI, *Il contratto tra* faciendum *e* factum, in *Idola libertatis*, Giuffrè, Milano 1985. Osserva incisivamente l'A.: "Questo processo, che chiamerei di crisi della sottoscrizione, è destinato ad accelerarsi ed intensificarsi. I soggetti dell'economia moderna non comunicano più con le lettere firmate dal mittente, ma attraverso segni trasmessi da apparati meccanici (telegramma su originale scritto, telegramma dettato per telefono, telex, telecopiert, etc.). Il risultato dell'attività espressiva è sempre in un testo scritto, ma sprovvisto di firma autografa. Il requisito della sottoscrizione, storicamente legato al contratto tra persone presenti e dall'uso sociale delle lettere missive, si scopre ormai incompatibile con le moderne tecniche di trasmissione e di fissazione della parola. I messaggi scritti vogliono liberarsi dal vincolo della firma, e perciò sollecitano nuovi metodi di imputazione, nuovi criteri di riferimento, alla persona del dichiarante. Metodi e criteri, non più legati alla firma autografa, ma all'uso esclusivo dell'apparato tecnico: codesta esclusività terrà il luogo della personalità della sottoscrizione. Una pronta ed accorta disciplina legislativa servirebbe a prevenire le tortuose strade dell'analogia e le arditezze della giurisprudenza". (*op. cit.*, p. 75).

131 Cass. Civ., sez. lavoro, 6 settembre 2001, n. 114455 : "Il documento informatico non munito di firma digitale ha l'efficacia probatoria prevista dall'art. 2712 c.c. nel senso che tale documento va ricondotto alla rappresentazione meccanica di fatti e cose, la quale forma piena prova dei fatti e delle cose rappresentate, se colui contro il quale è prodotta non ne disconosce la conformità ai fatti o alle cose medesime, con la conseguenza che il disconoscimento della loro conformità ai fatti rappresentati non impedisce che il giudice possa accertare la conformità all'originale anche attraverso altri mezzi di prova, comprese le presunzioni".

132 Sulla base della norma contenuta nell'art. 2712 c.c., infatti, le rappresentazioni meccaniche formano piena prova dei fatti e delle cose rappresentate, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti o alle cose medesime.

forme particolari per il disconoscimento dell'originale, quali quelli stabiliti a proposito della scrittura privata, stabilendo la sufficienza di una pura e semplice contestazione della conformità degli stessi agli atti o alle cose da documentare[133].
La necessità di una disciplina espressa del fenomeno è stata, dunque, pienamente avvertita[134], anche in considerazione della recente emanazione in diversi ordinamenti giuridici di norme specifiche, tendenti ad equiparare il documento elettronico alla scrittura privata, attraverso l'individuazione di uno strumento di imputazione del documento al suo autore equivalente alla sottoscrizione (sottoscrizione elettronica)[135].
Più volte, in dottrina, si è sottolineata l'incapacità del Legislatore di mantenersi al passo con i tempi e di adeguarsi alle novità che l'incessante evoluzione scientifica e tecnologica introduce nella realtà sociale, soprattutto alla luce delle innovazioni verificatesi in materia di strumenti di trasmissione a distanza della manifestazione della volontà.
In questo senso hanno indubbiamente costituito uno stimolo alla produzione legislativa, anche le novità introdotte negli ordinamenti giuridici di altri Paesi, appartenenti sia al sistema di *common law*,[136] sia a quello di *civil law*[137], che da tempo sono dotati di una disciplina giuridica dei cosiddetti "nuovi documenti".

---

133 Cass. 9 maggio 1977 n. 1772 in Foro Italiano, 1977, I, p. 1965; Cass. 17 luglio 1980 n. 4649, Cass. 22 maggio 1982 n. 3143 in Giurisprudenza Italiana, 1983, I, p. 968 con nota di TRIFONE; Cass. 17 giugno 1985 n. 3652 in Giustizia Civile 1986, p. 2535 con nota di RUSSO; Cass. 11 agosto 1987 n. 6881. Ciò comporta uno stato di incertezza sul valore probatorio del documento per tutta la durata del giudizio di merito. Una decisione della Cassazione, tuttavia, ha affermato, in difformità dalla giurisprudenza precedente, che il disconoscimento della conformità all'originale della copia fotostatica di un documento è soggetto alle modalità e ai termini fissati dagli artt. 214 e 215 cod. proc. civ. e, pertanto, non può essere effettuato per la prima volta in grado d'appello. (Cass. 3 maggio 1988 n. 3294; in dottrina nello stesso senso vedi VACCARELLA, *Sull'efficacia probatoria della prova fotografica di scrittura privata*, in Rivista di diritto processuale, 1969, p. 269).

134 Tra le iniziative, cfr. *lo Schema di legge sul documento informatico* e relativa *Relazione*, elaborato da un gruppo di lavoro su *Informatica ed ordinamento*, costituito presso il CED della Cassazione e coordinato da Fanelli (Cfr. Il Diritto dell'Informazione e dell'Informatica*,* 1994, p. 1057 ss.).

135 Vedi lo studio di AMORY e POULLET, *Le droit de la preuve face à l'informatique et à la telematique*, in Rev. int. dir. comp., 1985, p. 331 ss., trad. it. Il regime della prova nell'informatica e nella telematica, in Il Diritto dell'Informazione e dell'Informatica, 1986, p. 47 ss.; ed il recente studio di BRITZ, Urkundenbeweisrecht und Elektroniktechnologie, Munchen, 1996. La disciplina elettronica è stata di recente introdotta anche nella legislazione tedesca (Legge sulla regolamentazione dei servizi di informazione e comunicazione - *Gesetz zur Regelung der Rahmenbedingungen fur Informations und Kommunikationsdienste (IuKDG)*, del 22 luglio 1997, BGBI. I, S. 1870, del 28 luglio 1997), che all'art. 3 istituisce un'infrastruttura federale amministrativa, organizzata come un ente economico privato, che attribuisca chiavi d'accesso pubbliche grazie all'applicazione di congegni tecnici. Nel contesto di questa legilazione, la firma elettronica è configurata, tuttavia, non come una sottoscrizione in senso stretto, atta a chiudere un documento giuridicamente rilevante con assunzione di paternità o a concludere un accordo tra privati quanto, piuttosto, come un codice d'accesso digitale, posto a tutela dell'inviolabilità dei dati raccolti in forma elettronica, quasi una sorta di sigillo (*siegel*) a protezione dei dati informatici, senza nulla aggiungere sul concetto di forma elettronica.

136 In primo luogo rilevano, da un punto di vista comparativo, le innovazioni introdotte in materia nell'ambito degli ordinamenti di *common law*. Per quanto riguarda gli Stati Uniti d'America, una legge che stabilisce la piena equiparazione fra il documento cartaceo e il documento elettronico è entrata in vigore nel 1995 nello stato dello Utah. Si tratta del *Digital*

Peraltro, lo stesso Legislatore italiano ha dato chiara indicazione della volontà di apertura nei confronti di fenomeni di larga diffusione nella pratica giuridica, dettando, ad esempio, la Legge. 7 giugno 1993, n. 183, recante "Norme in materia di utilizzazione dei mezzi di telecomunicazione per la trasmissione degli atti relativi a procedimenti giurisdizionali", che, sia pure con riferimento

Signature Act. Analoghe iniziative sono state assunte in altri Stati e, stando agli ultimi dati, 39 Stati hanno già emanato, o stanno attualmente esaminando, in vista dell'emanazione, testi legislativi in materia di firma digitale e documento elettronico. Nel Regno Unito invece, in cui regole numerose e precise prevedono la possibilità e l'efficacia dei mezzi di prova, la possibilità di utilizzare i documenti elettronici come mezzi di prova era in contrasto con la regola del sentito dire (*Hearsay Rule*) e con la regola dell'originale (*Best Evidence Rule*). In base alla *Hearsay Rule* un documento non poteva essere fatto valere in Tribunale se il suo autore non fosse stato presente per testimoniare sul suo contenuto e per sottoporsi all'esame in contraddittorio (*cross examination*). In base alla *Best Evidence Rule* un documento poteva essere fatto valere in Tribunale soltanto quando è prodotto nella sua versione originale. Sia in base alla *Hearsay Rule* sia in base alla *Best Evidence Rule* un documento elettronico non avrebbe potuto valere di fronte all'Autorità Giudiziaria: l'elaboratore infatti non poteva essere sottoposto all'esame in contraddittorio e, pertanto, la dottrina e la giurisprudenza avevano sempre considerato i documenti dell'elaboratore come prove per sentito dire. Inoltre i documenti elettronici difficilmente costituiscono originale, ma, in genere, sono la trascrizione di una scrittura cartacea, spesso distrutta dopo la sua registrazione informatica. Per la producibilità del documento elettronico dinanzi alla Corte inglese è stata necessaria, quindi, l'emanazione di un'apposita legge, il *Civil Evidence Act* del 1968, in cui l'art. 5 prevede espressamente la possibilità di produrre in giudizio un documento elettronico se la sua conformità all'originale sia, ad avviso del tribunale, sufficientemente dimostrata. Nel diritto americano, invece, la producibilità in giudizio dei documenti elettronici è stata riconosciuta dalla giurisprudenza attraverso un'eccezione nota con il nome di *Business Records Exeption*; ed è stata quindi riconosciuta anche dalla legislazione federale con lo *Uniform Business Record as Evidence Act* e con le *Uniform Rules of Evidence*; una normativa innovativa è stata adottata senza sostanziali modificazioni dalla maggioranza degli Stati. La regola della "Best Evidence" è stata, invece, superata, sia in America sia in Inghilterra, da un indirizzo giurisprudenziale secondo il quale la produzione di una copia come prova del contenuto del suo originale è permessa se la parte che se ne avvale dimostra che non ha potuto procurarsi l'originale; in materia di documenti informatici è sufficiente dimostrare che gli originali di questi sono stati distrutti o non sono mai esistiti, come nel caso della registrazione diretta; inoltre, in base alla "Voluminous Writing Exeption", un riassunto in forma di documento informatico può essere esibito in giudizio al posto degli originali, qualora questi siano troppo complessi o voluminosi. Vedi E. GIANNANTONIO, *Il valore giuridico del documento elettronico*, in Rivista di diritto commerciale, 1986, p. 268-269; F. FERRARI, *La nuova disciplina del documento informatico*, in Rivista di diritto processuale, 1999, nota n. 7, p. 133.

[137] Per quanto concerne, invece, i Paesi di *civil law*, bisogna menzionare, *in primis*, la Legge del 22 dicembre 1986, mediante la quale in Lussemburgo è stato modificato l'art. 1348 del codice civile a proposito della presentazione in giudizio di "reproductions micrografiques et enregistrements informatiques effectuèe à partir de ces originaux": tali riproduzioni e registrazioni hanno lo stesso valore probatorio dell'originale fino a prova contraria. In Belgio e in Francia, invece, ci si è limitati ad ammettere le registrazioni informatiche in materia contabile ma, attualmente, si stanno elaborando disegni di legge finalizzati all'equiparazione del documento elettronico al documento tradizionale. In Francia è in vigore, poi, la Legge n. 90.1170 del 29 dicembre 1990 che contiene la disciplina dell'utilizzazione della crittografia e dei sistemi crittografici in generale e prevede, in alcune ipotesi specifiche, un'autorizzazione da rilasciarsi da parte del Primo Ministro. Rilevante è, poi, la già menzionata Legge tedesca, mediante la quale viene disciplinata la firma digitale senza, peraltro, stabilire una corrispondenza tra i due tipi di documento. Infine anche in altri Paesi sono state emanate leggi in materia o sono allo studio disegni di legge (a titolo puramente esemplificativo si possono citare la Corea del Sud e l'Argentina).

al limitato ambito dell'esercizio della professione forense, prevede la larga utilizzabilità dei mezzi di trasmissione elettronica a distanza degli atti del processo tra avvocati[138].

La volontà di adeguare il nostro ordinamento giuridico ad altri tecnologicamente più avanzati e la necessità di tutelare, in modo congruo, la fiducia che gli operatori economici sono portati ad attribuire ai documenti informatici, si è potuta concretizzare finalmente nell'ambito dell'iniziativa legislativa, collegata alla legge finanziaria del 1997, in materia di "Delega al Governo per il conferimento di funzioni e compiti alle regioni e agli enti locali, per la riforma della pubblica amministrazione e per la semplificazione amministrativa".

Infatti nell'ambito di tale Legge (la cosiddetta "prima legge Bassanini") è contenuta la norma che costituisce la fonte della disciplina del documento informatico[139].

Il primo pregio del Regolamento in questione si riscontra, indubbiamente, nella predisposizione di una serie di definizioni molto utili all'interprete, relative a strumenti ben noti in ambiente informatico, ma sicuramente non appartenenti di norma, al patrimonio culturale di un "non addetto ai lavori", quale può essere il giurista (si tratta dell'art. 1).

---

138 Sulla legge cfr. lo studio di COSTANTINO, *Sulla trasmissione degli atti processuali attraverso mezzi di telecomunicazione* (prime note sulla legge 7 giugno 1993, n. 183), in Foro italiano, 1993, I, p. 2500 ss.; i commenti di TRUNI e di DE SANTIS, in *Le nuove leggi civili commentate*, 1994, rispettivamente p. 164 ss. e p. 171 ss.; e le considerazioni di G. F. RICCI, *Aspetti processuali della documentazione informatica,* in Rivista trimestrale di diritto e procedura civile*,* 1994, p. 863 ss., 880 ss..

139 Il riferimento preciso è l'art. 15, comma 2, che recita: "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 trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge. I criteri e le modalità di applicazione del presente comma sono stabiliti, per la pubblica amministrazione e per i privati, con specifici regolamenti da emanare entro 180 giorni dalla data di entrata in vigore della presente legge, ai sensi dell'art. 17, comma 2, della legge 23 agosto 1988, n. 400. Gli schemi dei regolamenti sono trasmessi alla Camera dei Deputati ed al Senato della Repubblica per l'acquisizione del parere delle competenti Commissioni". Mediante tale disposizione non si può negare che il Legislatore abbia inteso integrare la disciplina del documento, così come delineata nel codice civile del 1942 che fa riferimento esclusivamente al documento cartaceo scritto, attribuendo rilevanza, nella stessa prospettiva della dottrina più recente, alla funzione, anziché alla struttura del documento e ponendo l'accento sulla nozione di "documento" anziché su quella di atto. Al di là di una mera enunciazione della validità del documento elettronico, tale disposizione rimanda necessariamente ad ulteriori regolamenti "da emanarsi entro 180 giorni dalla data di entrata in vigore della presente legge…". Con la pubblicazione sulla Gazzetta Ufficiale del 13 marzo 1998, n. 10, del d.p.r. n. 513 del 10 novembre 1997, è stato emanato il "Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione dei documenti con strumenti informatici e telematici, a norma dell'art. 15, comma 2, della legge 15 marzo 1997, n. 59". Il Regolamento, però, non esaurisce la materia. Il primo comma dell'art. 3 infatti, rinvia espressamente ad una serie di regole tecniche "per la formazione, la trasmissione, la conservazione, la duplicazione , la riproduzione e la validazione, anche temporale, dei documenti informatici" da emanare con decreto del Presidente del Consiglio dei Ministri "entro centottanta giorni dall'entrata in vigore del presente regolamento, sentita l'Autorità per l'Informatica nella Pubblica Amministrazione"*,* mentre l'art. 4 dello stesso, prevede che, con decreto del Ministero delle Finanze, vengano definiti gli oneri fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto.

In primo luogo viene definito il documento informatico come "la rappresentazione informatica di atti, fatti e dati giuridicamente rilevanti"; il Legislatore ha optato per una definizione molto lata che si distingue da quelle precedentemente date dall'interprete, consentendo di ricomprendere sia i cosiddetti documenti elettronici in senso stretto (documenti memorizzati in forma digitale e non percepibili se non tramite l'uso di elaboratori), sia i cosiddetti documenti elettronici in senso lato (prodotti normalmente cartacei formati mediante l'elaboratore).
In particolare, relativamente ai cosiddetti documenti elettronici in senso stretto, si pongono evidenti problemi, data la necessità di tutelare gli operatori economici in merito alla genuinità, autenticità e sicurezza delle informazioni in essi contenute: tali difficoltà derivano dalla lampante considerazione che i documenti elettronici in senso stretto non sono suscettibili di sottoscrizione tradizionale mediante apposizione autografa del nome e del cognome dell'autore.
La mancanza della sottoscrizione autografa viene, tuttavia, superata mediante le disposizioni del Regolamento che, proprio per colmare questa lacuna, prevedono l'impiego di tecniche come la crittografia, che consentono di impedire l'accesso indiscriminato alle informazioni contenute nel documento, di imputare il documento ad soggetto determinato e determinabile nonché di tutelare e verificare agevolmente l'integrità del documento stesso.
Affiora, quindi, l'importanza della nozione di firma digitale, che non è una firma nel senso tradizionale del termine[140], bensì il risultato della complessa procedura informatica di validazione già esaminata.
La firma digitale, dunque, apposta con il sistema delle doppie chiavi a crittografia asimmetrica, ha il vantaggio di assolvere a tutte le funzioni che,

---

[140] Non sono mancati, e non mancano tuttora, tentativi di surrogare la sottoscrizione con altri mezzi di imputazione del documento informatico al rispettivo autore. Alcuni particolari elaboratori possono leggere e memorizzare, quindi trasformare in forma digitale, le firme apposte personalmente dal sottoscrittore, ma non riescono ad eliminare il pericolo determinato dalla riproducibilità della sottoscrizione, cioè il rischio di eventuali, ma sempre possibili, contraffazioni; altri, invece, adottano tecniche studiate appositamente per garantire la sicurezza dei dati e si avvalgono delle tecniche della biometria, ossia di quella scienza che studia quantitativamente i fenomeni della vita: gli studi biometrici sono, effettivamente, alla base dei sistemi tecnici più precisi per l'identificazione di una persona. La prima caratteristica di un sistema biometrico-elettronico consiste nell'utilizzazione di mezzi che, da un lato, permettono l'identificazione di un individuo e, dall'altro, impediscono la copiatura o la rivelazione accidentale (come è possibile, invece, usando le *passwords* o i codici d'accesso) e assicurano l'impossibilità di perdita o duplicazione come accade con l'accesso mediante le chiavi o le tessere). La seconda caratteristica è che il controllo di un dato biometrico è effettuata dall'elaboratore elettronico, con una capacità di individuazione e di riconoscimento di gran lunga superiore a quella dell'uomo. I dati biometrici più comunemente usati sono le impronte digitali, la configurazione dei vasi sanguigni della retina, la geometria della mano, le impronte delle labbra, il riconoscimento della voce e, infine, il riconoscimento della grafia dell'individuo. La firma digitale si differenzia, inoltre, dalla firma cosiddetta grafica, prevista dall'art. 3, comma 2, del d.lgs. n. 13 del 1993 che, con formulazione analoga a quella di cui all'art.15-*quinquies* della Legge n. 38 del 1990 (in materia di certificazioni anagrafiche e di stato civile delle amministrazioni comunali) prevede per determinati atti della pubblica amministrazione, la sostituibilità della firma autografa con quella in formato grafico, sancendone la piena equiparabilità alla firma autografa

secondo la dottrina dominante[141], vengono attuate dalla firma autografa, precisamente la funzione dichiarativa, quella indicativa e quella probatoria.

8. Il valore giuridico del documento informatico.

Prima dell'emanazione della Legge 59/1997, la dottrina più attenta segnalava, in assenza di un apposito intervento normativo che prevedesse un equipollente della firma autografa, l'impossibilità di formare con lo strumento informatico una scrittura privata ai sensi degli artt. 2702 ss. c.c., non potendosi apporre alla fine del documento elettronico la sottoscrizione di pugno dell'autore (questa considerata come essenziale requisito della scrittura privata).
Ciò portava a ridurre di molto la rilevanza giuridica del documento elettronico (essenzialmente a quelle fattispecie, e per quegli effetti per i quali la legge non prevede la sottoscrizione).
Può tuttavia affermarsi che il documento elettronico avrebbe sempre potuto costituire principio di prova per iscritto ai sensi dell'art. 2724 c.c.[142], infatti, come ha più volte sottolineato la giurisprudenza, non è necessario che il principio di prova scritta sia sottoscritto da colui contro il quale viene richiesta la prova testimoniale, né che la sottoscrizione sia riconosciuta[143].
Un esempio è il caso in cui l'uso dei mezzi elettronici sia diventato una pratica comune e consuetudinaria, come nel caso dei trasferimenti elettronici di fondi, il giudice potrebbe, ai sensi del capoverso dell'art. 2721 c.c., ammettere la prova per testimoni dei contratti anche quando il valore dell'oggetto ecceda le lire cinquemila.
In questi casi, anzi, il giudice potrebbe forse giungere a considerare il documento elettronico come sottoscritto, qualora non ne sia contestata la provenienza.
Con riferimento alla forma ed efficacia del documento informatico nel sistema anteriore al d.lgs. 10/2002, l'art. 10 d.p.r. 445/2000, nel testo anteriore al recente intervento legislativo di attuazione della normativa europea, nel regolare la forma ed efficacia del documento informatico, stabiliva che il documento informatico sottoscritto con firma digitale, redatto in conformità alle regole tecniche, soddisfa il requisito legale della forma scritta e ha efficacia

---

141 A titolo esemplificativo vedi R. ZAGAMI, *Firme 'digitali', crittografia e validità del documento elettronico,* in Diritto dell'informazione e dell'informatica*,* 1996, p. 153 ss.; ID., *La firma digitale tra soggetti privati nel regolamento concernente 'atti, documenti e contratti in forma elettronica',* in Diritto dell'informazione e dell'informatica*,* 1997, p. 905 ss.; S. PATTI, *Informatica e nuovi documenti,* in Diritto bancario*,* 1997, p. 203-206; F. ORLANDI, *Il regolamento sul documento elettronico: profili ed effetti,* in Rivista di diritto commerciale*,* 1998, p. 748 - 750. F. FERRARI, *op.cit.,* p. 140-142. F. SQUILLARIO, *La firma digitale nell'attività notarile,* in Vita notarile, 1999, I, p. 432-433. F. RIZZO, *Valore giuridico ed efficacia probatoria del documento informatico,* in Diritto dell'informazione e dell'informatica*,* 2000, p. 222 e ss..

142 Articolo rubricato "Eccezioni al divieto della prova testimoniale".

143 Cass. 64/461; 75/1047. Occorre, naturalmente, che dal documento risulti la provenienza dalla persona contro la quale è diretta la domanda ovvero dal suo rappresentante.

probatoria ai sensi dell'art. 2712 cod. civ. e che il documento informatico, sottoscritto con firma digitale ai sensi dell'art. 23 del testo unico sulla documentazione amministrativa, ha efficacia di scrittura privata ai sensi dell'art. 2702 cod. civ.

9. La contestazione del documento informatico.

Il Regolamento, nello stabilire le conseguenze giuridiche che ricadono su colui che risulta autore di una firma digitale, dopo la verifica del relativo certificato, ha dovuto operare una scelta, in astratto, tra due opzioni di fondo: vincolatività, senza possibilità di eccepire l'incolpevole falsità della firma; vincolatività, con la possibilità di fornire, a certe condizioni, una prova contraria.
È stata adottata la prima soluzione, poiché l'effetto della revoca (o sospensione), cioè la "mancata sottoscrizione", si verifica solo dal momento della sua pubblicazione (art. 10, comma 5).
Prima di quel momento[144], salvo una limitata eccezione, il rischio dell'impiego abusivo della chiave privata[145] da parte di persona diversa dal titolare[146] è posto sempre a carico di quest'ultimo, sul quale grava, in sostanza, una forma di responsabilità oggettiva, per le conseguenze di tutti gli atti giuridici in forma informatica verificabili con la corrispondente firma digitale.
Orbene, si pone una presunzione assoluta, *iuris et de iure*, di riferibilità della firma digitale al soggetto titolare della chiave pubblica che risulta dal relativo certificato e non si ammette alcuna possibilità di fornire la prova contraria per sottrarsi alle conseguenze che derivano da un uso abusivo della chiave privata prima della richiesta di revoca (o sospensione).

---

144 Il certificatore è tenuto a procedere tempestivamente alla revoca o sospensione e a darne immediata pubblicazione (art. 9, lett. *h* e lett. *i*). Se la pubblicazione è stata omessa o ritardata dal certificatore, su quest'ultimo si sposta il relativo rischio per i danni che ne sono eventualmente derivati, a meno che non provi di aver adottato tutte le misure idonee ad evitare il danno (art. 9, comma 1) .

145 "L'apposizione di firme digitali sotto nome altrui può derivare, oltre che dalla sottrazione di una chiave privata, anche dalla creazione di una nuova coppia di chiavi e della loro falsa certificazione, derivante da dolo o negligenza di un certificatore, eventualmente risultante dall'esercizio abusivo della sua chiave privata. Il regolamento non fa distinzioni, quindi, anche in tale ipotesi, prima della pubblicazione della revoca, sembra che l'atto firmato abusivamente produca comunque i suoi effetti, non essendo ammessa prova contraria da parte del titolare, ferma restando l'eventuale responsabilità del certificatore (art. 9), e quella dell'usurpatore, se identificabile". Così R. ZAGAMI, *op. ult. cit.,* p. 920.

146 "L'uso abusivo di una chiave privata altrui, ripropone in parte gli stessi problemi derivanti da una sottoscrizione (su carta) apocrifa". Vedi M. ORLANDI, *La paternità delle scritture*, Milano, 1997, p. 107 ss..

Pur riconoscendo al documento informatico l'efficacia di scrittura privata *ex* art. 2702 c.c., non si ammette il principio del disconoscimento previsto dallo stesso articolo[147].
Si produrranno, infine, in capo al titolare della chiave tutti gli effetti che derivano dall'atto giuridico compiuto dall'usurpatore[148], privilegiando una scelta di massima tutela dell'affidamento negoziale.
Per fare da contrappeso a queste gravi conseguenze, è ammessa una limitata forma di pubblicità di fatto, grazie alla quale è consentito (con l'onere a carico del revocante o di chi ne richiede la sospensione) provare che la revoca o sospensione era già a conoscenza delle parti interessate, anche in mancanza (o prima) della necessaria pubblicazione (art. 10, comma 5)[149].
Tale prova, però, letteralmente sembra poter sostituire solo la mancanza o il ritardo della pubblicazione[150], ma non anche la mancata previa richiesta di revoca o sospensione al certificatore stesso; sembra che non sia consentito dimostrare la semplice conoscibilità della revoca o sospensione, cioè l'ignoranza dipendente da colpa.
Soluzione diversa sarebbe stata la previsione di una presunzione *iuris tantum* di provenienza e di integrità del documento, come stabilita in numerosi provvedimenti stranieri e sovranazionali sul tema[151].
Sembra ingiusto, infatti, che il titolare della chiave risponda oggettivamente anche quando per circostanze non attribuibili a sua colpa abbia perso la chiave e si sia trovato nell'impossibilità di effettuare una tempestiva denuncia.
Sarà a suo carico la difficile prova dell'impiego abusivo della chiave, ed il suo stato soggettivo di inconsapevolezza che ha determinato l'abuso, dimostrando la propria mancanza di colpa, dato l'impiego di tutte le misure di sicurezza idonee a salvaguardare la chiave stessa.

---

147 Se si considera la verifica positiva della firma digitale apposta, come equivalente al "riconoscimento" della sottoscrizione di cui all'art. 2702 c.c., potrebbe sostenersi, in base alla stessa norma (richiamata dall'art. 5, comma 1), l'ammissibilità della querela di falso.

148 "Per favorire la diffusione del sistema delle firme digitali, si potrebbero porre a carico dei certificatori i rischi economici derivanti dall'uso abusivo delle chiavi private (nei casi in cui l'usurpatore non sia identificabile e il certificatore stesso provi la sua mancanza di colpa), assegnando loro una sorta di funzione assicurativa, così come agiscono le società emittenti carte di credito, predeterminando un limite massimo di responsabilità per l'utente". Ancora R. ZAGAMI, *op. ult. cit.,* p. 921.

149 "La pubblicità della revoca della chiave privata ha efficacia dichiarativa, con il correttivo della pubblicità di fatto, in modo analogo a quanto è previsto per l'efficacia dell'iscrizione nel registro delle imprese" (art. 2193 c.c.). La revoca della chiave è opponibile dal momento della pubblicazione (efficacia positiva); l'omessa pubblicazione della revoca non può essere opposta (efficacia negativa), salvo la dimostrazione dell'effettiva conoscenza.

150 "La revoca o sospensione (…) hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate" (art. 5, comma 2).

151 ABA, *Guidelines*, *cit,* prevedono una presunzione di provenienza controvertibile, mediante inversione dell'onere della prova a carico di colui che appare sottoscrittore; Utah DSA, *cit.,* ammette che il titolare del certificato provi (inversione dell'onere della prova) che la firma è stata apposta da altri (o perché è stata sottratta la chiave privata, o perché il certificato è falso); nel contempo, però, il titolare deve provare, nel caso di sottrazione della chiave, che non ha violato i doveri di diligenza durante la sua custodia; inoltre, deve sempre provare che il destinatario era a conoscenza della falsità della firma e della violazione dell'obbligo di diligenza.

In adempimento del dovere di tutela dell'affidamento, la possibilità di fornire la prova contraria dovrebbe essere subordinata alla malafede dell'altro contraente, intesa come conoscenza o conoscibilità della falsità (invalidità) della firma (art. 1147, comma 3, c.c.), secondo un principio generale del nostro ordinamento (vedi artt. 428, 1431, 1439 comma 2, 1445 c.c.); malafede che andrebbe provata dalla persona che appare come sottoscrittore (art. 1147, comma 3, c.c.).
In caso di atti unilaterali si potrebbe richiedere la prova del grave pregiudizio all'autore (art. 428 c.c.).
Ulteriore ipotesi è quella dell'uso di una chiave associata ad un nome falso, inesistente (la cosiddetta "contraffazione per invenzione", contrapposta a quella per usurpazione), che può derivare dall'uso abusivo di una chiave privata di un certificatore, o dall'emissione (con dolo o con colpa) di falsi certificati da parte di quest'ultimo.
Il caso potrebbe inquadrarsi ed essere risolto nel tradizionale tema della conclusione del contratto sotto falso nome.
Infine, se la falsità riguarda una scrittura privata informatica autenticata *ex* art. 16, in applicazione degli artt. 2702 e 2703 c.c. (richiamati dagli artt. 5, comma 1, e 16, comma 1), dovrebbe essere proponibile il rimedio della querela di falso ai sensi degli artt. 221 e ss. c.p.c..
Si possono immaginare le seguenti ipotesi di infedele autentica notarile: effettuata utilizzando abusivamente la chiave privata di un notaio; relativa a firma applicata con una chiave scaduta, revocata o sospesa con regolare pubblicazione (è dovere del notaio controllare la validità attuale della chiave utilizzata, consultando gli appositi registri telematici, *ex* art. 16, comma 2); relativa a firma applicata con una chiave non revocata o sospesa, ma utilizzata da persona diversa dal legittimo titolare (il notaio dovrà accertare la corrispondenza tra identità del firmatario e generalità del titolare della chiave che risulta dal certificato, art. 16, comma 2).
Ammettendo la querela di falso, nell'ultima ipotesi, colui che appare falsamente come firmatario otterrebbe una certa tutela, anche in mancanza di revoca della chiave; a differenza di quanto avviene, invece, per la semplice scrittura privata informatica non autenticata, per la quale, come si è visto, la revoca non pubblicata non è opponibile.
Nelle ultime due ipotesi, la tutela della parte è ulteriormente rafforzata dalla responsabilità civile a carico del notaio (art. 76, Legge notarile).
Concludendo, l'efficacia di far "piena prova, fino a querela di falso, della provenienza delle dichiarazioni di chi l'ha sottoscritta" (art. 2702 c.c.) va attribuita al documento sottoscritto con firma digitale autenticata o certificata o, comunque, se non certificata, riconosciuta da colui contro il quale è prodotta.
Il disconoscimento, ad esempio, non si riconduce più alla non riconoscibilità della sottoscrizione, in quanto un'eccezione di tal genere sarebbe oggetto di verifica immediata e, quindi, prontamente respinta se infondata, una volta presentata la chiave pubblica (certificata) dell'autore.
Tutto ciò senza espletare alcuna analisi scientifica o grafologica imprescindibile, invece, per la verifica di una tradizionale sottoscrizione.

Un accettabile disconoscimento può solo consistere nell'eccezione che la firma digitale sia stata applicata impiegando una chiave privata da parte di chi non ne era legittimo titolare; ma, in questo caso, l'onere di provare l'invalidità della firma spetta alla persona che appare come sottoscrittore dal contenuto del certificato[152].
Riassumendo, mentre nella scrittura privata tradizionale disconosciuta l'onere di azionare il procedimento di verificazione spetta alla parte che ha prodotto il documento, in una scrittura privata con firma digitale l'onere di dimostrare la falsità della firma spetta a colui che risulta sottoscrittore: ciò che si disconosce è, sostanzialmente, l'esclusività dell'apparato tecnico, cioè della chiave privata, che viene presunta fino a prova contraria.

[152] Così anche F. ORLANDI, *Il regolamento sul documento elettronico: profili ed effetti,* in Rivista di diritto commerciale,1998, I, p. 750.

Capitolo Quarto

CRITTOGRAFIA E DIVIETI NELL'UTILIZZO DI PARTICOLARI TECNICHE DI SICUREZZA

SOMMARIO: 1. Un primo inquadramento delle problematiche nel panorama mondiale. – 2. Il Cocom, primi cenni. - 3. Il *Wassenaar Arrangement*, primi cenni. – 4. La situazione giuridica europea. – 5. La situazione giuridica italiana.

1. Un primo inquadramento delle problematiche nel panorama mondiale.

Nel momento in cui ci si accinge ad analizzare la liceità delle tecniche di sicurezza, ed in particolare i divieti nell'utilizzo delle stesse, con particolare riferimento alla tecnologia crittografica, è bene chiarire che cosa si intenda per 'divieto'.
Per 'divieto di utilizzo di alcune tecniche di sicurezza' si intende, in questa sede, il divieto normativamente espresso - quindi frutto dell'attività del Legislatore - che un sistema giuridico disponga in relazione ad una particolare tecnica di sicurezza.
Abbiamo già visto nel corso del Volume come la crittografia, più che il *watermarking* - il quale è ancora in uno stato embrionale come tecnica adottata di sicurezza - sia soggetta a diverse restrizioni in molti Paesi del mondo.
Abbiamo anche rilevato come la *ratio* di queste previsioni normative sia facilmente ravvisabile nello scarso controllo delle comunicazioni che la crittografia consente.
Sicuramente, infatti, la *privacy* di ogni singolo cittadino è un diritto fondamentale e decisamente meritevole di tutela, ma la quasi totale impossibilità di controllo delle comunicazioni crittografate - grazie, anche, al perfezionarsi degli algoritmi di cifratura - sia negli Stati caratterizzati da un regime totalitario, sia negli Stati in cui vi sia un particolare controllo della pericolosità sociale di determinati individui con tecniche sensibilmente invasive, ha prodotto una serie di norme che tendono a limitare l'applicazione, la vendita e l'esportazione dei prodotti e dei *software* crittografici, intendendo come 'prodotti' l'*hardware* espressamente disegnato per assolvere funzioni di crittografia (ad esempio: uno *scrambler* per le comunicazioni telefoniche).

Nel caso della crittografia, in particolare, abbiamo notato in più parti di questo Volume come non sia raro che la stessa venga considerata un'arma bellica vera e propria, com'è il caso della disciplina negli Stati Uniti d'America.
È proprio questa suscettibilità di qualifica delle tecniche crittografiche che le ha sempre rese difficilmente inquadrabili in un regime giuridico ben definito e, soprattutto, omogeneo a livello internazionale.
Senza scendere nel dettaglio di ogni singolo Stato, si possono fare due grandi suddivisioni prelimari, che si approfondiranno in seguito e nel Capitolo successivo, a seconda che si tratti di Paesi aderenti al COCOM prima, ed al *Wassenar Arrangement* poi, o meno.

2. Il Cocom, primi cenni.

Anteriormente all'accordo di Wassenar esisteva già un'organizzazione internazionale per il controllo dell'esportazione di prodotti definiti 'strategici' da parte degli Stati aderenti verso gli Stati non aderenti.
Questa organizzazione era il Cocom, acronimo di *Coordinating Committee for Multilateral Export Control.*
Per la precisione, nel 1991 il Cocom decise di occuparsi delle problematiche inerenti all'esportazione del materiale e delle tecniche crittografiche: le regole che furono dettate in quella sede vennero seguite praticamente da tutti gli Stati aderenti al Cocom, eccezion fatta per gli Stati Uniti d'America che optarono per una regolamentazione diversa e molto più restrittiva.
I Paesi aderenti al Cocom erano diciassette e, per l'esattezza, Australia, Belgio, Canada, Danimarca, Francia, Germania, Grecia, Italia, Giappone, Lussemburgo, Olanda, Norvegia, Portogallo, Spagna, Turchia, Regno Unito, Stati Uniti d'America.
Erano invece inclusi tra i membri cooperativi l'Austria, la Finlandia, l'Ungheria, l'Irlanda, la Nuova Zelanda, la Polonia, Singapore, la Slovacchia, la Corea del Sud, la Svezia, la Svizzera e Taiwan.
La finalità principale di un'organizzazione come il Cocom era quella di controllare e prevenire che strumenti crittografici abbastanza complessi e sofisticati venissero esportati verso quei Paesi che vengono classificati come 'pericolosi', come ad esempio la Libia e l'Iraq, e di consentire l'esportazione nei Paesi non pericolosi dietro lascito di una licenza, da parte del Paese importatore, che attesti le finalità di utilizzo non belliche del prodotto crittografico.
Il Cocom, tuttavia, venne sciolto nel 1994.

3. Il *Wassenaar Arrangement*, primi cenni.

Dietro impulso di ventotto Paesi, tutti *ex* membri del Cocom, si pensò di creare un organismo analogo che si occupasse sempre di definire le linee guida

dell'esportazione delle tecnologie che presentano la caratteristica di essere considerate sia semplici strumenti tecnologici sia strumenti bellici veri e propri.
Per rispondere a queste esigenze, fu creato, dietro impulso di ventotto Paesi, il *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*.
Nella sua stesura finale parteciparono trentuno Paesi e, per l'esattezza, Argentina, Australia, Austria, Belgio, Canada, Repubblica Ceca, Danimarca, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Italia, Giappone, Lussemburgo, Olanda, Nuova Zelanda, Norvegia, Polonia, Portogallo, Repubblica di Corea, Romania, C.S.I., Repubblica Slovacca, Spagna, Svezia, Svizzera, Turchia, Regno Unito e Stati Uniti d'America. In seguito ne entrarono a far parte anche Bulgaria ed Ucraina.
La crittografia è, in genere, classificata come *dual-use good*, si è visto, per via della sua ambiguità nell'utilizzo come mezzo di protezione della *privacy* e come mezzo bellico.
La previsione più interessante contenuta nel *Wassenaar Arrangement* è quella formulata in seguito ad una revisione generale dell'accordo nel 1998, e che è passata alla storia col nome di *General Software Note*.
In essa si liberalizza l'esportazione e la commercializzazione di qualunque *software* crittografico di massa o di dominio pubblico.
In particolare, si prevede la libera esportazione di tutti i prodotti crittografici a chiave simmetrica fino a 56 *bit*, e di quelli a chiave asimmetrica fino a 512 *bit*, e di tutti i prodotti basati su crittografia fino a 112 *bit*; la libera esportazione del *software* crittografico di massa e dell'*hardware* basati su chiave simmetrica; la libera esportazione di prodotti che utilizzano sistemi crittografici per la protezione della proprietà intellettuale; l'esportazione di tutto quanto non specificato nell'elenco è invece soggetta al rilascio di una licenza
Non tutti gli Stati membri del *Wassenaar Arrangement*, tuttavia, accettarono le disposizioni contenute nella *General Software Note*, ed in particolare Australia, Francia, Nuova Zelanda e Stati Uniti d'America continuano a controllare l'esportazione di *software* crittografico, anche se esso è di massa o di dominio pubblico.
Tuttavia, le previsioni del *Wassenaar Agreement* necessitano di essere recepite negli ordinamenti dei singoli Stati partecipanti mediante apposite disposizioni normative, che a volte integrano o a volte limitano i termini dell'accordo.

4. La situazione giuridica europea.

Il quadro della situazione europea, a dire il vero, non si presenta tanto armonizzato come lo si potrebbe credere: in effetti, i singoli Stati hanno fissato delle loro precise linee guida in materia di esportazione, utilizzo e controllo del *software* crittografico e sue implementazioni e derivazioni.
Il cammino per arrivare ad una disciplina omogenea per tutta l'Unione Europea non è stato affatto semplice, dal momento che vi è stata un'alternanza

tra tendenze permissiviste all'utilizzo ed esportazione di prodotti crittografici, seguite da tendenze restrittive, invece, in relazione allo stesso oggetto.
Nel 1994, con la *EU Council Regulation* n. 3381/94, successivamente emendata, si prevedeva la predisposizione di una licenza per l'esportazione di *software* o *hardware* crittografico verso Paesi non membri dell'Unione, eccezion fatta per quei prodotti che venivano classificati come prodotti crittografici di massa o di pubblico dominio.
Per un certo periodo, detta licenza era necessaria anche per lo scambio del *software* o *hardware* crittografico tra gli stessi Stati membri.
Solo successivamente vi fu un allargamento, per cui sia nei confronti degli Stati membri, sia nei confronti di Stati esteri con cui vi erano particolari accordi (Australia, Canada, Giappone, Nuova Zelanda, Svizzera e Stati Uniti d'America) l'esportazione era soggetta ad un numero di formalità estremamente ridotto.
Nel 1997 la Commissione Europea divulgò la comunicazione *Towards A European Framework for Digital Signatures And Encryption*, la quale per prima riconobbe il carattere primario della crittografia, ossia quello di garantire la *privacy* dei singoli cittadini, e che quindi adoperare criteri restrittivi per la libera circolazione della stessa (almeno all'interno degli Stati membri) non solo non teneva conto delle esigenze di riservatezza del singolo, per quanto creava problemi nella circolazione dei dati e, conseguentemente, nell'armonizzazione complessiva del mercato interno.
Gli scopi di questa comunicazione erano quella di abbattere progressivamente i controlli esistenti nell'*export* di prodotti crittografici tra i Paesi membri; chiarire bene gli ambiti che licenze del calibro della *General Software Note* andavano a disciplinare e regolamentare l'esportazione del *software* crittografico effettuata mediante mezzi di trasmissione non tangibili.
In effetti l'esportazione a mezzo Internet, ad esempio, non è mai stata regolamentata.
Basti pensare che gli Stati Uniti d'America, notoriamente molto restrittivi ed attenti nell'esportazione di *software* crittografico (anche se in questi giorni si assiste ad un'inversione di tendenza), disciplinano esclusivamente la trasmissione mediante strumenti materiali e tangibili (quali possono essere un supporto ottico, magnetico, ecc.).
Questo ha consentito di trovare l'*escamotage* per l'esportazione del Pgp (*software* crittografico studiato appositamente per la protezione delle *e-mail*), semplicemente postando su una pagina Internet l'intero listato del codice, in modo tale che chiunque fosse libero di copiarlo e compilarlo senza (apparentemente) violare alcuna legge.
Nel 1998, in Europa, si registrò una forte inversione di tendenza rispetto ai principi libertari espressi nella comunicazione della Commissione Europea, dovuta probabilmente al susseguirsi di attentati terroristici in alcuni stati dell'Unione, per cui i Ministri della Giustizia dei diversi Paesi membri, durante la conferenza di Birmingham, affermarono che l'autorità pubblica deve avere una forma di controllo sulle chiavi crittografiche, o mediante sistemi cosiddetti di *key escrow* (ovvero il deposito della chiave di decrittazione presso l'autorità pubblica, in modo tale che possa servirsene all'occorrenza), o mediante altri

mezzi tecnici, e si auspicò anche una forte attività di monitoraggio dell'utilizzo di tecniche crittografiche da parte di associazioni terroristiche.
Si arriva, quindi, ai nostri giorni, in cui la fonte normativa principale che regola l'esportazione in generale dei cosiddetti *dual-use goods*, e quindi anche della crittografia, la si rinviene nella *Council Regulation n. 1334/2000 setting up a Community regime for the control of exports of dual-use items and technology*.
Si tratta di una previsione normativa molto semplice, tendente, in linea di massima, a liberalizzare l'esportazione di *software* e materiale crittografico, anche se vi sono delle distinzioni da fare a seconda dei casi.
Come per lo più avviene quando si analizza un testo proveniente dall'Unione Europea, la grande linea di demarcazione è data dalla disciplina adottabile nei confronti degli altri Stati facenti parte dell'Unione Europea, e quella adottabile, invece, nei confronti degli Stati non membri.
Difatti si nota come l'esportazione di prodotti e *software* crittografico tra Paesi membri dell'Unione Europea sia perfettamente liberalizzata, ad meno che non si tratti di sofisticati strumenti di crittanalisi, per i quali è necessario sottoscrivere la *General Intra-Community Licenses*, la quale sostanzialmente vuole accertarsi dell'utilizzo che verrà fatto dello strumento crittanalitico nel Paese membro di destinazione.
L'esportazione, invece, verso l'Australia, il Canada, la Repubblica Ceca, l'Ungheria, il Giappone, la Nuova Zelanda, la Norvegia, la Polonia, la Svizzera e gli Stati Uniti d'America necessita di un'apposita *Community General Export Authorisation*, la quale autorizza lo Stato membro ad esportare il *software* crittografico.
Per tutti gli altri Paesi del mondo si utilizzerà, sempre ai fini dell'esportazione del *software* crittografico, la *General Nation License*, che autorizzerà lo Stato membro ad esportare quel determinato *software* o prodotto crittografico verso un determinato Paese.
Sono totalmente escluse le esportazioni di *software* specialistico di crittoanalisi.
Nel panorama generale europeo, la Francia si è sempre contraddistinta per la particolare restrittività delle norme in tema di crittografia.
Solo recentemente si è assistito ad una maggiore liberalizzazione per quanto riguarda l'esportazione di prodotti crittografici, mentre restano sempre soggetti a particolari restrizioni i prodotti crittoanalitici.
La *ratio* di ciò è da ravvisare nel timore, particolarmente sentito dal Governo francese, dei sofisticati sistemi di spionaggio elettronico, Echelon in testa.
Tutto ciò, unito ovviamente all'esigenza di tutelare i diritti individuali dei cittadini, ha avuto come effetto l'emanazione di norme connotate da una restrittività non comune rispetto agli altri Stati dell'Unione.
Anche la Francia è tra i firmatari dell'accordo di Wassenaar per i controlli sull'esportazione del materiale crittografico, del quale però non ha recepito fino al mese di Dicembre del 1998 la *General Software Note*.
In Francia la situazione giuridica è differente. Lo spartiacque in materia di crittografia nel diritto francese è rappresentato da una Legge del 26 Giugno 1996.
Prima della suddetta Legge la vendita, l'importazione, l'esportazione e l'utilizzo di tecniche o prodotti crittografici erano soggette, innanzitutto, ad una

dichiarazione, nella quale si affermava che l'unico scopo per cui veniva impiegata quella particolare tecnica crittografica era di garantire l'autenticità della comunicazione e la integrità del messaggio trasmesso, altrimenti era soggetto ad un'autorizzazione da parte del Primo Ministro per altri casi.
Questa autorizzazione era soggetta alla trasmissione di un *dossier* contenente le specifiche relative all'algoritmo di crittazione che si sarebbe utilizzato.
Queste disposizioni trovavano la loro motivazione nel fatto che il Governo voleva procedere ad una classificazione e, conseguentemente, autorizzare l'uso della crittografia sulla base di scriminanti quali il tipo di utente che se ne sarebbe avvalso ed il valore del dato da proteggere.
Nel 1995 vi è il primo segnale di apertura, laddove si riconosce la sufficienza di una dichiarazione nel caso la crittografia venisse utilizzata per proteggere *password*, o codici d'accesso, o numeri collegati a servizi bancari, siano essi numeri di conto corrente o di carta di credito.
Si arriva quindi alla Legge del 1996, che ha come precise finalità quelle di regolare l'*import* e l'*export* di prodotti crittografici.
In particolare, si prevede l'utilizzo di chiavi della lunghezza massima di 40 *bit*, l'abrogazione della dichiarazione nel caso la crittografia venga utilizzata per l'invio di informazioni non confidenziali, e, soprattutto, la creazione di un sistema di *Trusted Third Parties* (TTPs) e di Agenzie di *Key Escrow* (KEA).
La conseguenza di questo nuovo sistema è che, se la KEA ed il suo sistema di *Key-escrow* vengono approvati dalle Autorità, l'ipotetico registrante di determinate chiavi sarà libero di utilizzare lo schema crittografico risultante dall'impiego delle chiavi registrate.
La prima KEA abilitata in Francia è stata la SCSSI, alla quale è stato demandato il compito di valutare le strutture e la conformità delle altre KEA.
Altra svolta significativa è il comunicato del Primo Ministro francese del 19 Gennaio 1999, con il quale si palesa la volontà, da parte delle Autorità, di liberalizzare realmente la circolazione dello strumento crittografico.
I principi cardine contenuti in questo comunicato, ed ai quali si dovranno rifare le successive normazioni in Francia, possono essere riassunti nei seguenti punti:
1) liberalizzazione completa nell'uso della crittografia;
2) impiego consentito di chiavi a 128 *bit*, rimuovendo quindi il precedente limite delle chiavi a 40 *bit*;
3) eliminazione del ricorso obbligatorio alla SCSSI per il deposito delle chiavi;
4) emanazione di norme sull'obbligo di decifrazione dei documenti su richiesta dell'autorità giudiziaria.
Tutti questi principi sono stati in seguito ribaditi nella loro sostanza nel *Policy Paper on the adaptation of the legal framework to the information society* dell'Ottobre del 1999, ma al momento non trovano applicazione concreta in alcun testo normativo francese.
Sicuramente, comunque, dalla enunciazione di questi principi si può ravvisare anche un avvicinamento alle posizioni dell'Unione Europea, che magari potrebbero agevolare quell'omogeneità di disposizioni in materia di crittografia tanto agognata.

5. La situazione giuridica italiana.

Scendendo nello specifico dell'ordinamento italiano, si ravvisa subito l'assenza di norme specifiche tese a regolamentare l'*import*, *export* ed utilizzazione dei prodotti e *software* crittografici, eccezion fatta per le norme regolatrici della tutela del Segreto di Stato sia in campo civile sia in campo militare.
L'uso relativo ad altri scopi che non siano la tutela del Segreto di Stato, quindi senza voler procedere a distinzioni in merito all'uso domestico della crittografia o all'utilizzo, invece, da parte di enti o istituti governativi o aziende, non è assolutamente regolamentato.
Le uniche norme analogicamente applicabili possono essere quella contenuta nell'art. 130 del codice postale, che vieta la crittazione, da parte dei radioamatori, delle trasmissioni radio, e l'art. 9 della Convenzione per la concessione di ponti radio, il quale prescrive un preciso obbligo nel caso in cui le trasmissioni transitanti sul ponte radio in oggetto siano crittate, ovvero il deposito dei codici di cifratura presso l'Amministrazione postale.
Anche il regolamento interno della Telecom, principale azienda di telefonia presente in Italia, non prescrive alcunché in materia di comunicazioni crittografate, e le vieta solo nel caso in cui il loro utilizzo possa compromettere o influire in qualche modo sulla funzionalità della rete di trasmissione telefonica.
Ritornando, quindi, alla disciplina propria della tutela del Segreto di Stato, si ravvisa innanzitutto la presenza di un'apposita Autorità incaricata di controllare e verificare l'impiego di metodologie di cifratura dei dati.
Tale ente è l'ANS (Autorità Nazionale per la Sicurezza), identificato col Presidente del Consiglio dei Ministri, cui per l'appunto è affidata la tutela del Segreto di Stato.
Il Presidente del Consiglio ha la facoltà di delegare ad un alto funzionario dello Stato la responsabilità in materia di tutela amministrativa del Segreto.
Detto ente si avvale, per il concreto esercizio delle sue funzioni, del III Reparto dell'UCSi (Ufficio Centrale per la Sicurezza) che fa capo alla Segreteria Generale del CENSIS.
Tale Ufficio svolge funzioni di direzione, coordinamento, consultive, di studio e di controllo in ordine all'applicazione della normativa concernente la tutela amministrativa del Segreto di Stato e delle altre notizie di carattere riservato, nei riguardi dei soggetti e degli enti civili e militari che, nello svolgimento delle loro funzioni, trattano notizie, documenti o materiali ai quali è stata attribuita una classifica di segretezza.
In tale contesto provvede agli atti relativi all'omologazione di sistemi di telecomunicazione che contemplino l'utilizzo di tecniche atte a garantire la sicurezza dei dati, nonché allo studio delle disposizioni nazionali in materia di sicurezza tecnica.
Tentare di ricostruire, poi, la situazione della crittografia in generale, e del divieto dell'utilizzo di mezzi crittografici in particolare, all'interno dell'ordinamento italiano non è un'impresa semplice.

Non esiste, infatti, un *corpus* normativo omogeneo che consenta di tracciare una linea seguita dal Legislatore nel corso degli anni, ma ci si trova dinanzi a testi di legge che trattano, il più delle volte in via meramente incidentale, della crittografia e della sicurezza delle comunicazioni.
La base di partenza è sicuramente costituita dalla Legge 185/90, recante norme sul controllo dell'esportazione, importazione e transito dei materiali di armamento.
Come si ricorderà la crittografia, rientrando nella categoria dei cosiddetti beni a duplice uso, ossia suscettibili di essere visti come uno strumento perfettamente legittimo e liberamente diffondibile o come strumento bellico, ben potrebbe essere ricompresa nell'ambito di applicazione della suddetta Legge.
In particolare, all'art. 2, lett. O, si legge che rientrano nei materiali di armamento gli equipaggiamenti speciali appositamente costruiti per uso militare, la cui specificazione è possibile reperire negli elenchi approvati periodicamente con decreto ministeriale.
L'ultimo di questi è il d.m. 1 settembre 1995 il quale, nella categoria 11, fa rientrare alla lettera 'e' le "apparecchiature di sicurezza per il trattamento di dati, apparecchiature di sicurezza per dati ed apparecchiature di sicurezza per linee di trasmissione e di segnalazione, utilizzanti procedimenti di cifratura", e, nella lettera 'f', le "apparecchiature per l'identificazione, l'autenticazione ed il caricamento di chiavi crittografiche ed apparecchiature per la gestione, produzione e distribuzione di chiavi crittografiche".
La disciplina prevista per questa categoria di beni comprende la richiesta di autorizzazione a norma della Legge. 185/90, ma solo se tali beni sono stati "appositamente progettati per impiego militare" o se sono stati realizzati mediante "loro componenti appositamente progettati".
Segue la Legge 222/92, la quale però si rivelò essere una norma eccessivamente statica e, soprattutto, assolutamente non in linea con il Legislatore comunitario alla luce del Regolamento europeo sui beni a duplice uso n. 3381/94.
Per questo motivo detta Legge è stata più volte emendata, e molti suoi articoli sono stati abrogati con successivi interventi legislativi.
Più specificamente, vi è stata una Legge di riforma della 222/92, ovvero la Legge 6 febbraio 1996 n. 52, la quale aveva come scopo quello di omogeneizzare la situazione normativa italiana con quella comunitaria in materia di beni a duplice uso, dietro l'emanazione di un decreto legge che contenesse i seguenti elementi fondamentali: 1) semplificazione del procedimento autorizzativo; 2) definizione delle procedure di diniego, revoca, annullamento, sospensione e modifica delle autorizzazioni; 3) riorganizzazione delle competenze in materia di coordinamento, istruttoria e controllo; 4) revisione delle competenze del comitato consultivo e del comitato tecnico; 5) individuazione delle misure di controllo; 6) ridefinizione delle sanzioni.
Questi criteri sono stati poi formalizzati nel d.l. 24 febbraio 1997 n. 89, il quale appunto, oltre ad aver emendato in maniera particolarmente incisiva la Legge 222/92, vuole essere il decreto di attuazione del Regolamento UE 3381/94 poco sopra menzionato.
Allo stato attuale, quindi, della Legge 222/92 sono rimasti in vigore solo i seguenti articoli: art. 4, in tema di autorizzazioni specifiche per l'utilizzo di

prodotti ad alta tecnologia; art. 5, concernente il comitato consultivo per l'esportazione ed il transito dei prodotti e delle tecnologie; art. 6, in materia di presentazione delle domande di autorizzazione di esportazione ed importazione dei beni a duplice uso; art. 7, disciplinante l'attività istruttoria demandata al Ministero per il Commercio con l'Estero; art. 8, sul rilascio delle autorizzazioni specifiche per l'esportazione ed il transito dei beni a duplice uso.
Al momento è in discussione un Regolamento attuativo del d.l. 89/97, che dovrebbe fornire disposizioni più dettagliate in materia di presentazione delle istanze, del loro esame e dei controlli.
Altri testi normativi rilevanti in materia di beni a duplice uso sono il d.m. 18 novembre 1993, il quale disciplina l'attività di "verifica dell'arrivo a destino" per i beni considerati particolarmente pericolosi.
Al momento tali beni sono i prodotti nucleari, i prodotti chimico-biologici, i prodotti missilistici ed alcuni prodotti strategici.
Segue il d.m. 11 aprile 1994, il quale istituisce presso il Ministero per il Commercio con l'Estero l'Ufficio competente per il rilascio dei provvedimenti.
Mediante due Comunicati il Legislatore nazionale, all'indomani dell'entrata in vigore del Regolamento 3381/94, si è preoccupato di fornire delle indicazioni precise per la compilazione dei moduli e per il procedimento istruttorio, e più precisamente con il Comunicato del 14 giugno 1995 e successivamente con il Comunicato del 3 aprile 1996.
Restano da esaminare, per dare completezza al quadro normativo, il d.m. 18 giugno 1997, che disciplina il rilascio delle autorizzazioni globali, mediante il quale gli esportatori, dietro prova di una certa stabilità nei rapporti commerciali, possono chiedere il rilascio di un'autorizzazione cumulativa valida al massimo per tre anni e che comprenderà molteplici beni e molteplici destinazioni, ed il d.m. 12 giugno 1998 che disciplina le esportazioni effettuabili con l'autorizzazione generale.
In particolare, gli esportatori inseriti nell'apposito registro tenuto presso il Ministero per il Commercio con l'Estero potranno liberamente esportare i prodotti non considerati particolarmente sensibili verso quei Paesi non classificati come 'a rischio'.

Capitolo Quinto

CRITTOGRAFIA E QUADRO NORMATIVO

SOMMARIO: 1. Le fonti sovranazionali: un'introduzione. - 2. Aspetti giuridici del Cocom. - 3. Aspetti giuridici del *Wassenar Arrangement*. - 4. I principi fondamentali della Convenzione di Wassenaar. - 5. Lo scambio delle informazioni. - 6. I requisiti di ammissione. - 7. L'Assemblea Plenaria del Dicembre 2001 e gli orientamenti attuali. - 8. La *UN Security Council Resolution* n. 1373 del 2001. - 9. La politica dell'Oecd. - 10. L'inventario dei controlli sulla crittografia messo a punto dall'Oecd.

1. Le fonti sovranazionali: un'introduzione.

Lo sviluppo delle tecnologie, la loro diffusione e la scoperta di nuovi campi cui destinarle, hanno portato i Governi a predisporre delle regole che possano prevenire un loro eventuale uso distorto. La crittografia, in particolare, intesa come l'insieme di macchinari e *software* idoneo a codificare un'informazione, è considerata uno strumento di elevato pericolo ed una potenziale minaccia per la sicurezza nazionale ed internazionale degli Stati ed il mantenimento dei fragili equilibri politici internazionali[153].
Fatta questa premessa, è facile comprendere il motivo che ha determinato un aumento esponenziale della soglia di attenzione degli ordinamenti, sia a livello internazionale che regionale, ed ha portato alla creazione di organismi di controllo sui trasferimenti di beni militari, prodotti e tecnologie che possono avere una duplice valenza, militare e civile, tra cui è inclusa la crittografia. In realtà, non è corretto impostare il discorso solo dal punto di vista della pericolosità in termini di sicurezza pubblica. È vero, infatti, che l'attenzione per questo tipo di materia trova oggi altro tipo di giustificazione nella grande diffusione del commercio elettronico nel *World Wide Web*, nel moltiplicarsi delle transazioni *on-line* e nell'esigenza di maggior sicurezza in Internet.
Le tecniche di crittografia non servono solo a codificare informazioni militari da *spy stories*[154] ma anche, e forse più banalmente, a permettere di sottoscrivere

---

153 Cfr. C. REED, *Computer law*, Balckstone Press Limited, 1996, London.

154 A questo riguardo alcuni casi celebri: Ramsey Yousef fece parte del gruppo terroristico internazionale responsabile delle esplosioni al World Trade Center di New York nel 1994 e all'aereo di linea della Manila Air nel 1995. Quando il suo laptop fu sequestrato a Manila, l'FBI trovò alcuni file crittografati. Questi file, poi decodificati con successo, contenevano informazioni relative a ulteriori progetti di far esplodere 11 aerei di linea commerciali in

documenti *on-line* soddisfando quattro esigenze fondamentali: la riservatezza delle informazioni contenute nel documento, l'integrità o immodificabilità del documento, l'autenticazione della provenienza, la non ripudiabilità da parte del soggetto autore[155].
La rete normativa, originata dalle politiche delle grandi organizzazioni internazionali facenti capo alle Nazioni Unite, compone un quadro che va dai principi sanciti dalle Convenzioni multilaterali internazionali, alla normativa d'impronta europea, alle singole legislazioni nazionali e regionali.

2. Aspetti giuridici del Cocom.

A livello internazionale, i principi base, che hanno tradotto in articoli le istanze provenienti da Governi sparsi in tutto il mondo, sono quelli sanciti dal trattato internazionale del Cocom, *Coordinating Committee for Multilateral Export Controls*[156].
Il Cocom nacque nel 1950 come l'organizzazione internazionale per il reciproco controllo delle esportazioni di prodotti strategici ed informazioni tecniche, dai Paesi Membri verso determinate aree geografiche proibite. Esso era preposto alla gestione ed aggiornamento, *inter alia*, della *International Industrial List* e della *International Munition List*, tra cui erano incluse tutte le tipologie di crittografia. Sotto il regime del Cocom la crittografia venne considerata un bene strategico con applicazioni militari soggetta a restrizioni commerciali, ed effettivamente i controlli sulla esportazione di crittografia furono disciplinati per oltre quattro decadi da questo organismo. Nel 1989 il

---

Estremo Oriente. Dei criptovirus, una nuova forma di terrorismo finanziario, sono stati introdotti in almeno nove sistemi finanziari a Londra. Questi frammenti di codice ostile sono come gli altri virus, eccetto che codificano i dati anziché danneggiarne il sistema: in questi casi i virus mettevano in cifra dati e file bancari. Le compagnie venivano in seguito contattate da hacker che richiedevano riscatti fino a 100.000 dollari. In diversi casi l'FBI ha reso noto il ritrovamento di messaggi di posta elettronica e file codificati nelle corso di indagini relative a pedofili e pornografia infantile. In molti casi i soggetti utilizzavano il noto programma PGP o mascheravano messaggi nelle immagini che venivano scambiate o rese disponibili sul loro sito Internet. (fonte: http://inews.tecnet.it/Articoli/1998/1998-03/tecnica9803.html, sito consultato il 15 luglio 2002)

155 Cfr. M. TERRANOVA, *Firma digitale: tecnologie e standard*: "I metodi crittografici a chiavi pubbliche possono essere utilizzati per costruire strumenti per la firma digitale, la differenza principale tra le due applicazioni risiede nel ruolo delle chiavi. Nella crittografia la chiave pubblica viene utilizzata per la cifratura mentre il destinatario usa quella privata per recuperare il messaggio. Nella firma il messaggio non è in genere cifrato ed è direttamente disponibile per il destinatario, viceversa l'autore utilizza la funzione di cifratura e la chiave privata per generare la firma che, aggiunta al documento, ne certifica la provenienza grazie alla segretezza della chiave privata. Chiunque può accertare la provenienza del messaggio utilizzando la chiave pubblica per verificare che il valore della firma corrisponda al messaggio"

156 I Paesi facenti parte del Cocom erano 17: Australia, Belgio, Canada, Danimarca, Francia, Giappone, Germania, Grecia, Italia, Lussemburgo, Norvegia, Olanda, Portogallo, Regno Unito, Spagna, Stati Uniti d'America, Turchia. Cui successivamente si unirono altri 12 Membri aderenti: Austria, Corea del Sud, Finlandia, Irlanda, Nuova Zelanda, Polonia, Singapore, Svezia, Svizzera, Taiwan, Ungheria.

Cocom liberalizzò le esportazioni di sistemi crittografici di *password* e codici di autenticazione. Nel 1991, decise invece di permettere le esportazioni di programmi di crittografia destinati ad un mercato di massa.
In concomitanza con la fine della guerra fredda e con l'emergere di nuovi rischi per la sicurezza internazionale, nel Marzo del 1994, il Cocom venne dissolto per dare vita a nuovi Accordi internazionali.

3. Aspetti giuridici del *Wassenaar Arrangement*.

Nasceva dunque la necessità di stabilire un nuovo accordo che si occupasse dei rischi relativi alla sicurezza internazionale e regionale e della stabilità connessa alla diffusione delle armi convenzionali e dei prodotti e delle tecnologie a duplice uso. In tal modo, concordemente, il 16 Novembre 1993, all'Aja, durante la riunione dell'HLM (*High Level Meeting*), i rappresentanti dei 17 Paesi Membri del Cocom deliberarono di sciogliere il Cocom, e stabilirono una nuova Convenzione multilaterale, avente il nome temporaneo di "*New Forum"*..
La decisione assunta in quella sede venne successivamente confermata ed il Cocom cessò definitivamente la sua attività. I Paesi partecipanti continuarono in ogni caso, ad utilizzare, a livello locale, i principi di controllo sulle esportazioni stabiliti in seno al Cocom ed inseriti nella *control list* fino all'entrata in vigore della nuova Convenzione. Vennero dunque immediatamente costituiti tre gruppi di lavoro, scelti tra sei dei Paesi facenti parte dell'*ex* Cocom, con il precipuo scopo di dare vita ad una nuova Convenzione nel minor tempo possibile. Il primo dei tre gruppi si sarebbe occupato della individuazione degli obiettivi che dovevano animare il nuovo organismo, nonché delle regole e delle procedure di funzionamento. Il secondo gruppo fu incaricato di occuparsi dello sviluppo della lista dei beni e delle tecnologie che sarebbero state sottoposte al controllo, mentre il terzo gruppo si sarebbe occupato delle incombenze amministrative e burocratiche.
Al gruppetto iniziale dei sei Paesi si unì ben presto un gruppo di altri cinque e, nel Dicembre del 1995, in seno all'HLM tenutosi a Wassenaar, venne raggiunto l'accordo denominato "*Wassenaar Arrangement"*.
Dall'accordo dei Paesi firmatari, cui presto si unirono tutti gli altri che hanno portato al raggiungimento dell'adesione di 33 Membri, nacque il documento fondamentale della Convenzione "*The Initial Elements"* che venne adottato nell'assemblea plenaria del 11-2 Luglio 1996 e successivamente modificato, nella versione attuale, dalla Plenaria del 6-7 Dicembre 2001.
Il *Wassenaar Arrangement*, la prima convenzione multilaterale globale sul controllo all'esportazione di armi convenzionali e prodotti a duplice uso e tecnologie, ricevette l'approvazione finale, da parte di trentatré Paesi firmatari, nel Luglio del 1996, e dette inizio alla sua attività nel Settembre dello stesso anno[157].

[157] I Paesi firmatari sono: Argentina, Australia, Austria, Belgio, Bulgaria, Canada, Corea, Danimarca, Federazione Russa, Finlandia, Francia, Germania, Giappone, Grecia, Irlanda, Italia, Lussemburgo, Olanda, Nuova Zelanda, Norvegia, Polonia, Portogallo, Regno Unito,

4. I principi fondamentali della Convenzione di Wassenaar.

Tale Convenzione fu pensata per promuovere la trasparenza, lo scambio di vedute e di informazioni, la responsabilizzazione nel trasferimento di armi convenzionali e prodotti a duplice uso e tecnologie, delle quali intende prevenire l'accumulo. Essa completa e rinforza, senza duplicarlo, l'attuale regime circa la non proliferazione delle armi di distruzione di massa e la loro circolazione, ponendo l'attenzione sui trattati di pace regionale ed internazionale e sulla sicurezza che può derivare dal trasferimento di armamenti e prodotti a duplice uso e tecnologie qualora esista un reale pericolo[158].
La Convenzione, inoltre, è tesa ad accrescere la cooperazione al fine di prevenire l'accaparramento di armamenti e prodotti a duplice uso per fini militari, se la situazione in una regione o il comportamento di uno Stato è, o diviene, considerata di un certo peso politico per i Paesi partecipanti.
I Paesi firmatari fanno in modo, attraverso l'adozione di loro politiche nazionali, di assicurare che il trasferimento di armi e prodotti a duplice uso e tecnologie non contribuiscano allo sviluppo, o all'aumento in genere, delle capacità militari al punto da poter minare la sicurezza e la stabilità internazionale e nazionale e che non ne venga fatto un uso distorto. La convenzione non ostacola i trasferimenti dei prodotti tecnologici svolti in buona fede e non è diretta contro alcuno Stato in particolare o gruppi di Stati. Tutte le misure, adottate nel rispetto della convenzione, sono rispettose delle legislazioni e dei regimi giuridici nazionali dei singoli Stati e sviluppate in modo da lasciare un certo grado di discrezionalità nazionale.
L'"*Initial Elements*" è il documento fondamentale del *Wassenaar Arrangement* che prevede due liste di articoli e tecnologie che i Paesi Membri hanno concordato di inserire: a) una Lista di Munizioni che comprende beni militari e tecnologici; b) una Lista di prodotti e tecnologie a duplice uso, cioè beni che possono essere utilizzati a fini militari o civili. Quest'ultima si compone di tre sezioni: una *Basic list*, una *Sensitive list*, ed una sottosezione della seconda la V*ery Sensitive list*.
I Paesi che aderiscono alla convenzione mantengono un controllo effettivo sull'esportazione dei prodotti inseriti nelle liste concordate e, al fine di tenere

---

Repubblica Ceca, Romania, Slovacchia, Spagna, Stati Uniti d'America, Svezia, Svizzera, Turchia, Ucraina, Ungheria.

158 Il primo articolo della Convenzione recita: "The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities".

testa agli sviluppi tecnologici ed alle esperienze acquisite, tali liste vengono periodicamente aggiornate.
La crittografia e le tecnologie che permettono la sua utilizzazione sono ricomprese nella Lista dei beni e delle tecnologie a duplice uso nella Categoria 5, parte 2, "Information security". È importante sottolineare che rientrano in questa categoria sia i prodotti *hardware* che quelli *software*.
Produce un certo effetto scorgere sistemi di crittografia ed armi inserite nella medesima lista e sottoposte alle medesime restrizioni. Eppure, per quanto possa apparire incredibile, la storia ci insegna che un uso distorto della crittografia si è spesso rivelata un'arma infallibile, così come il suo sapiente uso ha costituito un'insostituibile mezzo di difesa.
Si sottraggono, invece, al controllo sulle esportazioni, costituendo dunque delle eccezioni, i prodotti elencati nel punto 5.A.2.
Inoltre, la lista non comprende *software* che siano anche: 1) normalmente utilizzabile dal grande pubblico poiché: a) venduti da uno *stock* presso un punto di vendita al dettaglio senza restrizioni, attraverso: una transazione "*over the counter*"; una transazione tramite ordine postale; una transazione telefonica; b) destinati all'installazione senza supporto tecnico del fornitore; 2) di pubblico dominio.

5. Lo scambio delle informazioni.

Attraverso la trasparenza e lo scambio di vedute ed informazioni, i fornitori di armi ed articoli a duplice uso possono sviluppare comuni linee di interpretazioni circa i rischi associati al trasferimento e valutare l'ipotesi di coordinare una politica nazionale di controllo per combattere tali rischi. Allo scopo di creare una efficiente rete di informazioni, la Convenzione prevede l'invio di una sorta di relazione "*notification*"[159] con cadenza semestrale avente ad oggetto la consistenza del trasferimento di armi. Allo stato attuale, esistono sette categorie di prodotti che corrispondono a quelle previste dal registro delle armi convenzionali delle Nazioni Unite.

---

[159] "Appendix 2 **Specific Information Exchange on Dual-Use Goods and Technologies, Indicative Content of Notifications.** The content of denial notifications for tier 1 will be based on, but not be limited to, the following indicative or illustrative list: • From (country) • Country of destination • Item number on the Control List • Short description • Number of licences denied • Number of units (quantity) • Reason for denial. Denial notification for items in the second tier and its sub-set of very sensitive items will be on the basis of, but not be limited to, the following indicative or illustrative list: • From (country) • Item number on the Control List • Short description • Number of units (quantity) • Consignee(s) • Intermediate consignee(s) and/or agent(s): Name Address Country • Ultimate consignee(s) and/or end-user(s): Name Address Country • Stated end-use • Reason for the denial • Other relevant information. The content of notifications for licences/transfers in the second tier will be based on, but not be limited to, the following indicative or illustrative list • From (country) • Item number on the Control List • Short description • Number of units (quantity) • Destination (country)".

Inoltre, è richiesto ai Membri di dare notizia di tutti i permessi di trasferimento, o dei dinieghi, al trasferimento di determinati articoli a duplice uso sottoposti a controllo. L'importanza di riferire anche degli eventuali divieti all'esportazione risiede nella necessità di attirare l'attenzione dei Membri su trasferimenti che possono cadere sotto l'applicazione della Convenzione.
Lo scambio di informazioni ai sensi della Convezione può riguardare anche altre materie soggette all'applicazione della Convenzione sulle quali uno Stato membro desidera richiamare l'attenzione degli altri.
I Paesi Membri si incontrano periodicamente a Vienna, luogo dove la Convenzione ha stabilito essere il suo quartier generale e dove ha sede il segretariato. Tutte le decisioni sono raggiunte tramite il meccanismo della votazione.

6. I requisiti di ammissione.

La Convenzione conserva una politica di apertura globale e non discrimina l'ingresso di Paesi terzi che intendano aderire ai suoi principi.
Ai fini dell'ammissione, un Stato terzo deve possedere alcuni requisiti precipuamente elencati nell'Appendice quarta[160]: a) essere un produttore/esportatore di armamenti o di equipaggiamenti industriali a questi correlati; b) mantenere una politica di non "proliferazione" dei menzionati prodotti ed un adeguato regime nazionale, inclusa l'adesione a politiche internazionali e trattati tesi alla non proliferazione; c) conservare controlli effettivi ed operanti sulle esportazioni.
Sebbene la Convenzione non preveda un osservatorio che assuma il compito di esaminare costantemente il quadro internazionale, tuttavia, tale risultato è ugualmente raggiunto tramite il meccanismo di informazione, cui si è accennato nel precedente paragrafo. Tale meccanismo, oltre a permettere a tutti gli Stati aderenti, di essere tempestivamente informati dei nuovi obbiettivi e delle attività svolte della Convenzione, incoraggia gli Stati terzi ad adottare politiche di controllo in linea con i principi dell'organismo, dei trattati internazionali e delle singole politiche di controllo nazionali.

7. L'Assemblea Plenaria del Dicembre 2001 e gli orientamenti attuali.

---

[160] "Appendix 4 **Participation Criteria -** When deciding on the eligibility of a state for participation, the following factors, inter alia, will be taken into consideration, as an index of its ability to contribute to the purposes of the new arrangement: Whether it is a producer/exporter of arms or industrial equipment respectively; Its non-proliferation policies and its appropriate national policies, including: Adherence to non-proliferation policies, control lists and, where applicable, guidelines of the Nuclear Suppliers Group, the Missile Technology Control Regime and the Australia Group; and through adherence to the Nuclear Non-Proliferation Treaty, the Biological and Toxicological Weapons Convention, the Chemical Weapons Convention and (where applicable) START I, including the Lisbon Protocol; Its adherence to fully effective export controls.

Nei giorni tra il 6 ed il 7 Dicembre 2001 l'assemblea generale dei Paesi aderenti al *Wassenaar Arrangement*, sotto la presidenza dell'Ambasciatore turco Aydin Sahinbas, si è riunita, per la settima volta dalla sua costituzione, per considerare l'attuale livello dei controlli sulle esportazioni dei prodotti inseriti nelle Liste, aggiornare le liste stesse e per decidere i nuovi obbiettivi cui mirare.
Alla luce dei recenti sviluppi internazionali, i Paesi Membri hanno chiaramente sottolineato l'importanza di rafforzare i controlli sulle esportazioni e riaffermato il loro fermo intento di mantenere responsabili i singoli regimi nazionali. L'assemblea, richiamando esplicitamente una delle ultime Risoluzioni delle Nazioni Unite[161], ha concordato che i Paesi Membri continueranno a porre ostacoli all'acquisto di armi e prodotti e tecnologie a duplice uso da gruppi ed organizzazioni terroristiche, così come da singoli terroristi, e che tali sforzi fanno parte integrante della lotta globale contro il terrorismo.
Questo concetto è stato espresso attraverso l'introduzione di un nuovo paragrafo nell'*Initial Elements*, il n.5 della Parte I (*Purposes*) che recita:
"5. In line with the paragraphs above, Participating States will continue to prevent the acquisition of conventional arms and dual-use goods and technologies by terrorist groups and organisations, as well as by individual terrorists. Such efforts are an integral part of the global fight against terrorism".
La prossima assemblea Plenaria del *Wassenar Arrangement* si riunirà a Vienna nel Dicembre 2002 sotto la presidenza, assunta dal 1 gennaio 2002, dell'Ambasciatore Volodymyr Ohrysko (Ucraina).
Navigando nella Rete, è piuttosto facile imbattersi in siti fondati da movimenti di protesta internazionali che puntano il dito contro i principi stabiliti dall'Accordo di Wassenaar. Attualmente è in corso una campagna internazionale alla quale aderiscono ventiquattro associazioni per la tutela dei diritti civili riunite nel progetto *Global Internet Liberty Campaign* (GILC), le quali mettono in discussione il presupposto cardine che la crittografia debba essere considerata un'arma[162].

8. La UN Security Council Resolution 1373 (2001).

---

161 UNSC 1373/2001.

162Come si legge nella lettera inviata alla segreteria dell'Accordo di Wassenaar: "(…) I membri del *Global Internet Liberty Campaign* (GILC) credono fermamente che, essendo la crittografia una tecnica di difesa, l'introduzione dei controlli sulla sua esportazione da parte del Trattato di Wassenaar non è giustificata in quanto contraria a quegli stessi principi sui quali il Trattato si basa; ritengono necessario che sia rimosso ogni controllo sulla esportazione delle tecniche di crittografia; ritengono inoltre necessario che il Trattato di Wassenaar non sia interpretato nel senso di limitare in qualsiasi modo o proibire lo sviluppo globale e la distribuzione di software e hardware per la crittografia; si appellano a tutti gli Stati Membri affinché rispettino gli intenti del Trattato di Wassenaar (1996) che espressamente esclude controlli sul mercato di massa e sul software di pubblico dominio (*General Software Note*); esortano i delegati delle nazioni firmatarie del Trattato di Wassenaar a valutare l'impatto negativo dei controlli esistenti sui programmi di crittografia e a rimuoverle nelle future versioni del Trattato. (Testo estrapolato da C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *Segreti spie codici cifrati,* Apogeo, 1999).

La UN Security Council Resolution 1373 (2001) del 28 settembre 2001, riaffermando le risoluzioni 1269 (1999) del 19 October 1999 e 1368 (2001) del 12 September 2001, e condannando gli attentati terroristici a New York, Washington D.C. e Pennsylvania dell'11 settembre, al fine di prevenire simili atti ha disposto alcune regole interessanti, sulla premessa che ogni atto terroristicvo costituisce una minaccia alla pace e alla sicurezza intern azionale.
IN particolare "Recognizing the need for States to complement international cooperation by taking additional measures to prevent and suppress, in their territories through all lawful means, the financing and preparation of any acts of terrorism",
"3. Calls upon all States to: (a) Find ways of intensifying and accelerating the exchange of operational information, especially regarding actions or movements of terrorist persons or networks; forged or falsified travel documents; traffic in arms, explosives or sensitive materials; use of communications technologies by terrorist groups; and the threat posed by the possession of weapons of mass destruction by terrorist groups".

9. La politica dell'OECD.

Nell'ambito delle politiche di controllo della crittografia, l'OECD[163], a partire dal 1996, ha messo a punto delle linee guida. Le prime discussioni e le bozze dei principi guida cominciarono nel Dicembre del 1995 a seguito di una riunione di esperti in materia di crittografia. La bozza delle linee guida fu sottoposta a discussioni e revisioni durante numerosi incontri, finché, nel marzo del 1997, la raccomandazione, nella quale erano state inserite, ricevette la definitiva approvazione e venne adottata con il nome di *Recommendation of the Council concerning Guidelines for Cryptography Policy.*
Le linee guida, che si indicano di seguito, costituiscono dei principi, non vincolanti per i Paesi Membri, cui ispirarsi per l'adozione, da parte di ogni singolo Governo, di una politica nazionale in materia di crittografia[164]: a) fiducia nei metodi crittografici: nel senso che i singoli Governi dovrebbero incoraggiare all'uso della crittografia; b) scelta dei metodi crittografici: gli utenti dovrebbero avere il diritto di scelta, nel rispetto della legge, sulle tecniche di crittografia; c) sviluppo di un mercato portante per i sistemi di crittografia: il mercato dovrebbe poter determinare sviluppi e previsioni dei sistemi di crittografia e soprattutto mirare all'armonizzazione dei sistemi con gli *standard* internazionali; d) protezione della *privacy* e dei dati personali: le politiche nazionali in materia di crittografia e lo sviluppo e l'uso della stessa devono agire nel rispetto del fondamentale diritto degli individui alla *privacy* compresa la riservatezza delle comunicazioni e dei dati personali; e) accesso per motivi legali: i sistemi di regolamentazione della crittografia devono poter garantire il libero accesso per motivi di ordine legale a *plaintext* e chiavi crittografate; f) responsabilità: devono essere chiare le posizioni di responsabilità degli utilizzatori e dei fornitori di sistemi crittografici; g) cooperazione

---

163 *Organisation For Economic Co-operation and Development.*
164 Cfr. B.-J. KOOPS, *The Crypto Controversy, a Key Conflict in the Information Society,* Kluwer Law International, 1999, The Hague, The Netherlands, pagg. 97-100.

internazionale: alla luce delle politiche internazionali sostenute dall'OECD, i governi devono cooperare per creare politiche comuni di regolamentazione della crittografia.
I principi appena esposti conservano un loro significato solo ed esclusivamente se letti in un unico insieme in quanto costruiti e bilanciati in modo tale da creare un equilibrio tra le istanze di continua modernizzazione tecnologica e quelle di sicurezza pubblica nazionale ed internazionale.
Tali principi, tuttavia, come sostiene parte della dottrina[165], sono stati accolti in modi molto diversi gli uni dagli altri. Da una parte, infatti, hanno rappresentato la vittoria della politica della tutela della *privacy* e dei diritti sottesi sulla politica americana di scarsa sensibilità in questa materia. Dall'altra, sono sembrati troppo severi ed inflessibili o, all'opposto, troppo vaghi. In realtà, le linee guida tracciate dall'OECD, pur nella loro voluta vaghezza, costituiscono una base solida di regolamentazione della materia che orienta il Legislatore e, allo stesso tempo, lascia i Governi liberi di darsi una propria disciplina.

10. L'inventario dei controlli sulla crittografia messo a punto dall'OECD.

Il Comitato per la politica relativa a Informazioni, Computer e Comunicazioni (ICCP)[166] dell'OECD si occupa di tecnologie di crittografia, all'interno dei suoi studi in merito alla sicurezza e alla tutela della *privacy*, fin dal 1989. Attualmente il lavoro viene portato avanti da un Gruppo di Esperti sulla Sicurezza Informatica e sulla *Privacy* (GESP) che, sulla base delle ricerche effettuate dalla Segreteria dell'OECD e su impulso dei Paesi Membri, ha dato vita all'*Inventory of Controls on Use of Cryptography Technologies.*
Attraverso questa raccolta, l'Organizzazione persegue lo scopo di agevolare la cooperazione internazionale con un'indagine sugli strumenti nazionali ed internazionali relativi ai controlli sulle esportazioni, importazioni e l'uso a livello locale delle tecnologie di crittografia nei Paesi Membri.
In particolare, l'indagine riguarda il grado di sviluppo dei controlli nazionali sulla crittografia e sulle eventuali modifiche alle legislazioni in materia ed il livello di sviluppo della normativa sui controlli all'*import/export* di crittografia, e gli eventuali emendamenti.
L'Inventario predisposto dall'OECD rivela che uno dei modi su cui differiscono i vari controlli sulle esportazioni di prodotti di crittografia è rappresentato dal trattamento del *software* di crittografia come "genericamente disponibile al pubblico" o "di pubblico dominio".
Si deve inoltre rilevare che esistono differenti approcci, a livello nazionale, in relazione ai controlli sull'*export*, a seconda che i *software* vengano distribuiti su

---

165 Cfr. B.-J. KOOPS, *The Crypto Controversy, a Key Conflict in the Information Society,* Kluwer Law International, 1999, The Hague, The Netherlands, pagg.97-100.
166 ovvero *The Information, Computer and Communications Policy.*

supporto materiale ovvero su un supporto immateriale (ad esempio tramite Internet)[167].

[167] Un esempio di questo differente approccio ci viene fornito dall'ordinamento dei Paesi Bassi, orientato a disciplinare espressamente l'esportazione di crittografia effettuata attraverso il transito in formato elettronico di *software* in rete.

Capitolo Sesto

L'APPROCCIO NORMATIVO DEI SINGOLI ORDINAMENTI NAZIONALI

SOMMARIO: 1. Gli Stati Uniti d'America. – 2. Il caso 'Clipper'. – 3. La politica del *National Research Council*. – 4. I tentativi di liberalizzazione. – 5. L'*Electronic Data Security Act* del 1997. – 6. L'attuale orientamento del Governo americano. - 7. Il *Computer Security Enhancement Act H.R. 1259*. - 8. La politica dell'Unione Europea. - 9. Il Regolamento del 1994. - 10. La Decisione. - 11. La Comunicazione del 1997. - 12. L'attuale orientamento normativo comunitario. - 13. La procedura per il rilascio dell'autorizzazione. - 14. Altre iniziative d'origine europea. - 15. La Convenzione sui crimini informatici. – 16. I singoli ordinamenti. – 17. La Francia – 18. La Germania. - 19. L'Italia. – 20. I Paesi Bassi . – 21 La Svezia.

1. Gli Stati Uniti d'America.

Gli Stati Uniti d'America hanno ristretto le esportazioni di tecnologie di crittografia in modo più severo rispetto a quanto previsto dal Wassenaar Arrangement e, precedentemente, dal Cocom[168].
Fino al 1996, le esportazioni di crittografia rientravano nell'ambito del regolamento sul traffico internazionale di armi[169] (I.T.A.R.); alla fine di quell'anno, la competenza per il controllo venne trasferita, in base all'*Export Administration Regulation* (E.A.R.), dal Dipartimento di Stato al Dipartimento del Commercio statunitense presso il *Bureau of Export Administration.*[170]
L'I.T.A.R., attraverso l'inserimento della tecnologia crittografica nella lista delle munizioni militari sottoposte a controllo, aveva effettuato una forte restrizione delle esportazioni di crittografia a duplice uso.
Negli Stati Uniti, gli unici tipi di crittografia liberamente esportabili erano costituiti dai prodotti utilizzabili per decifrare informazioni, per i quali poteva essere emessa una licenza ad uso esclusivo delle sedi secondarie all'estero di imprese americane e degli enti creditizi. Oltre a ciò, gli unici altri strumenti di

168 V. Cap. precedente.
169 *The International Traffic in Arms Regulation.*
170 Per avere un idea delle attuali procedure previste dal *Bureau of Export Administration*, si segnala il sito:www.bxa.doc.gov

crittografia non soggetti a controllo erano quelli a 40 bit, che rappresentavano, e lo sono ancora, uno strumento di crittografia "debole".[171]

2. Il caso *Clipper*.

Nel 1993 l'Amministrazione Clinton annunciò gli *Escrowed Encryption Standards* (EES) denominati nella prassi *Clipper*. Con questo sistema, le agenzie di intercettazione delle comunicazioni potevano, attraverso l'EES, e grazie alla tecnica del c.d. *backdoor* ("passaggio segreto"), violare il sistema di cifratura[172] ed avere accesso alle informazioni decodificate ottenendo, per ordine del tribunale, le due parti della chiave di decodificazione, depositate presso due agenzie governative.[173]
Com'è ovvio pensare, ne scoppiò un caso ed il governo fu assalito da proteste.[174]
Il sistema fu, dunque, abolito ed il governo dichiarò che non avrebbe ulteriormente sviluppato il progetto.

3. La politica del *National Research Council*.

Nel giugno del 1996, si ebbe una prima svolta nella politica di controllo delle esportazioni. Il *National Research Council* (N.R.C.), infatti, pubblicò lo studio, da tempo auspicato, relativo alla politica di crittografia attraverso il quale suggeriva di alleggerire, senza eliminarlo, il sistema dei controlli sulla esportazione.
Un passo in più, rispetto all'iniziale severità, era stato compiuto: sarebbe stata liberalizzata l'esportazione di prodotti crittografici simmetrici a 56 bit, mentre, quelli superiori avrebbero potuto essere esportati solo a condizione che gli utenti accordassero al governo degli Stati Uniti il permesso di avere accesso alle informazioni decodificate.[175]
La politica di controllo sostenuta dal N.R.C. rimase immutata per lungo tempo, nonostante che il progresso tecnologico promosso dalle grandi *Software House*

---

171 *A contrariis*, ROGNETTA G., *Firma digitale e documento informatico*, nota n.34: "Per *crittografia forte* s'intende quella basata su algoritmi di una certa robustezza, variamente quantificata a seconda delle interpretazioni delle varie autorità. Ad es. L'*Office of Defence Trade Control* statunitense di norma colloca gli algoritmi superiori a 40 *bit* in questa categoria, con la conseguenza di far scattare il divieto di esportazione".
172 ROGNETTA G., *op.cit.*, nota 33.
173 Il *National Institute of Standard and Technologies* e la *Treasury Department's Automated System Division*.
174 ROGNETTA G., *op.cit*: "il problema fu talmente sentito dalla comunità telematica, da provocare l'immediata reazione di un apposito newsgroup, tuttora molto attivo: alt.privacy.clipper".
175 Gli Stati Uniti adottano da sempre una politica fortemente tesa alla protezione della sicurezza nazionale e poco sensibile alla riservatezza.

americane, in merito ai sistemi di sicurezza a base crittografica, continuasse a crescere ininterrottamente.
Il sistema di restrizioni predisposto andava ad ostacolare sia le imprese statunitensi produttrici di prodotti crittografici veri e propri, sia quelle che realizzavano prodotti aventi delle applicazioni crittografiche o compatibili con sistemi di crittografia.
Spesso, le aziende statunitensi, nell'impossibilità di produrre doppie versioni dello stesso prodotto, per il mercato interno e per quello estero, si sono adattate a produrre e commercializzare un unico prodotto che non fosse soggetto a restrizione.

4. I tentativi di liberalizzazione.

La disciplina dell'E.A.R. mostrava di essere assolutamente anacronistica cosicché si susseguirono varie iniziative, in Parlamento come nei tribunali, tese a modificare, alleggerendolo, il regime delle esportazioni, ma nessuna di queste ebbe il successo auspicato.[176]
Nell'ottobre del 1996, il Vice-Presidente Gore fece una dichiarazione pubblica sul regime di controllo alle esportazioni, nel quale face riferimento anche all'uso nazionale della crittografia. L'uso della crittografia e delle chiavi crittografate, sosteneva, avrebbe dovuto essere volontario, così come la scelta del sistema di crittografia da utilizzare avrebbe dovuto essere libero.
Il governo avrebbe, in ogni caso, promosso la vendita di prodotti e servizi a base crittografica, stimolato lo sviluppo di dibattiti a livello internazionale ed incentivato lo sviluppo di sistemi e prodotti con tecnologie crittografiche. Emergeva, inoltre, l'impegno del governo a predisporre un apparato legislativo che agevolasse l'uso dei sistemi cifrati e che prevedesse delle ipotesi di responsabilità per il rilascio delle chiavi.

5. L'*Electronic Data Security Act* del 1997.

Alla fine del Marzo del 1997 fu emanato un progetto di legge in tema di *key-recovery*[177]: l'*Electronic Data Security Act of 1997*. Tale progetto, pensato per promuovere un'infrastruttura a chiave pubblica, era basato sul sistema di *key-recovery*, tramite registrazione delle Autorità di certificazione (pubbliche e private) ed Agenzie di *key-recovery* (KRAs).

---

[176] Ad eccezione del caso *Bernstein v Department of State*, nel quale un matematico (Daniel Bernstein) nel 1996 aveva pubblicato su internet le sue formule per la realizzazione di un programma di crittografia e per questo era stato accusato, dal governo, di aver esportato armi da guerra. La Corte Distrettuale e quella Federale si pronunciarono affermando che le restrizioni imposte all'esportazione dell'algoritmo crittografato, ideato dal Sig. Bernstein, erano troppo severe.
[177] Attraverso il *key recovery*, pur non essendo previsto il deposito della chiave, è tuttavia, possibile per le Autorità statali decifrare ogni informazione precedentemente codificata.

Era previsto che le KRAs, registrate o non registrate che fossero, rilasciassero la chiave alle autorità pubbliche alle stesse determinate condizioni previste per le intercettazioni telefoniche. Inoltre, si prevedeva che l'uso della crittografia, quando tesa ad incoraggiare la commissione di atti criminali, sarebbe stato punito con una pena dai 6 mesi ai 5 anni di reclusione. Infine, il progetto di legge prevedeva che il Presidente degli Stati Uniti avrebbe condotto delle negoziazioni con le Autorità di altri paesi allo scopo di raggiungere il reciproco riconoscimento delle KRAs.
Tuttavia, i tentativi di promulgazione del progetto di legge si arenarono poiché il Congresso emanò, di lì a poco, una legge dai contenuti molto simili: il *Secure Public Network Act*. Questa legge fu oggetto di molte proposte di emendamento che risvegliarono un vivace dibattito politico in relazione ai controlli sulle esportazioni di tecnologie *key-recovery* e *key-escrow*.
Il primo marzo del 1997 fu promulgato il SAFE Bill (H.R. 695)[178] che sanciva, finalmente, l'alleggerimento delle restrizioni all'export di crittografia. Tuttavia, anche questo documento fu oggetto di un lungo dibattito e di profondi emendamenti che lo resero, alla fine, tutt'altro rispetto a quella che era la sua versione originale.
Il 12 maggio del 1998, vide la luce l'*E-Privacy Act*[179], una legge tesa a garantire libertà d'uso della crittografia quale metodo di protezione e salvaguardia della sicurezza e della riservatezza delle comunicazioni, considerate diritti costituzionalmente protetti. Tale legge, tuttavia, allo scopo di agevolare solo determinati settori economici, quali banche ed istituzioni finanziarie, oltre a prevedere pene detentive molto più severe delle precedenti per l'uso della crittografia a fini criminali, introduce, ancora una volta, metodi e procedure mediante i quali gli organi preposti possono ottenere la decrittazione di qualsiasi testo elettronico.
Nel 1999, venne presentata al Congresso n.106, la seconda versione del SAFE H.R. 850[180]. Questa versione sosteneva, in modo certamente più democratico

---

178 *Security and Freedom though Encryption Act* (SAFE): Introduced 2/12/97 by Rep. Bob Goodlatte (R-VA).
**Gives all Americans the freedom to use any type of encryption anywhere in the world, and allows the sale of any type of encryption domestically;*
**Prohibits the government from creating a back door into peoples' computer systems (mandatory key escrow);*
**Relaxes U.S. export controls to permit the export of generally available software, including mass market or public domain software such as PGP, and other types of software and hardware under a license if a product with comparable security is commercially available from foreign suppliers; and*
**Creates criminal penalties for the unlawful use of encryption in furtherance of a crime -- up to 5 years imprisonment for a first offense, and up to 10 years for each subsequent offense.*" THE CENTER FOR DEMOCRACY AND TECHNOLOGY

179 L'acronimo sta per: *Encryption Protect the Right of Individuals for Violation and Abuse in Cyberspace*.

180*The "Security and Freedom Through Encryption Act" (SAFE, HR 850)*
"*The Security and Freedom through Encryption Act (SAFE), championed by Representatives Bob Goodlatte (R-VA) and Zoe Lofgren (D-CA), and cosponsored by a solid, bi-partisan majority of the U.S. House of Representatives, is designed to promote privacy, security, and competitiveness in the Informaiton Age. HR 850, similar to the previous version of SAFE, and would:*

- *Affirm Americans' freedom to use the strongest possible encryption.*
- *Defeat attempts to force Americans to provide the government with some government-approved "third party" with "keys" to their encrypted information.*

- Allow the U.S. to compete in the rapidly growing market for strong encryption products.

della prima, il diritto dei cittadini statunitensi di usufruire delle migliori tecnologie di crittografia in modo da poter aumentare la soglia di sicurezza delle comunicazioni personali e, allo stesso tempo, in nome della difesa del paese dal terrorismo, riservava il diritto delle autorità statali di accedere alle comunicazioni.
Evidentemente le pressioni dei produttori e degli operatori dell'e-commerce hanno prevalso sulle esigenze di sicurezza perché nel settembre del 1999, sotto l'amministrazione Clinton, con un comunicato stampa, tre ministri USA[181] hanno dichiarato: «*Gli Stati Uniti allenteranno le restrizioni sull'esportazione dei software di crittografia. I programmi di "encryption" di massima sicurezza, cioè, non saranno più considerati, come è avvenuto finora "armi da guerra" e potranno anche varcare le frontiere nazionali*»[182].
Questo atteggiamento di apertura, tuttavia non deve illudere sulle intenzioni del governo americano in merito all'esportazione di crittografia, poiché, già all'epoca del comunicato, si precisava che la liberalizzazione riguardava solo alcuni settori industriali e che, in ogni caso era escluso qualsiasi tipo di esportazione verso quelli individuati come i sette paesi terroristi: Cuba, Lybia, Iran, Iraq, North Corea, Syria, Sudan.

6. L'attuale orientamento del governo americano.

Nel gennaio del 2000, il Governo degli Stati Uniti ha emanato un nuovo regolamento sull'esportazione di crittografia che ha rappresentato una svolta della politica americana in materia. Tale regolamento, nel corso dei mesi, di pari passo con il rafforzamento della politica di liberalizzazione dell'Unione europea, è stato soggetto a vari emendamenti, che hanno condotto all'emanazione dell'attuale versione, emanata il 19 ottobre 2000, che liberalizza l'esportazione di crittografia ai 15 paesi membri dell'UE ed alleggerisce il regime in favore di altri otto paesi per i quali prevede l'abolizione della licenza preventiva.
La nuova disciplina, inoltre, instaura un sistema che avvantaggia il consumatore liberalizzando molti prodotti d'uso comune ed i loro codici sorgente.
Dopo gli attentati terroristici dell'11 settembre 2001 a New York, l'attenzione degli Stati Uniti per la sicurezza delle comunicazioni e per la prevenzione di un uso distorto delle informazioni ha condotto all'emanazione, in tutta fretta, il 29 novembre 2001, di un testo di legge: il *Computer Security Enhancement Act H.R. 1259*.

Americans for Computer Privacy enthusiastically supports SAFE. The bill also enjoys support from the financial services industry, the health care industry, privacy organizations, both liberal and conservative think tanks and the high-tech community, among others". Il testo integrale, così come tutti gli emendamenti ed i dibattici politici sono visionabili sul sito di un'associazione che difende il diritto dei cittadini americani alla riservatezza, all'indirizzo: www.computerprivacy.org

[181] Janet Reno (Ministro di Giustizia), William Cohen (Ministro della Difesa) e William Daley (Ministro del Commercio).

[182] 19 Settembre 1999, www.repubblica.it/online/tecnologie/encryption/encryption/encryption/html.

7. Il *Computer Security Enhancement Act H.R. 1259.*

Gli scopi perseguiti dal Governo statunitense con l'adozione di questo nuovo testo legislativo sono due:
1) rinforzare il ruolo del *National Institute of Standards and Technology* al fine di garantire la sicurezza delle informazioni non-classificate nel Sistema Informatico federale;
2) promuovere soluzioni tecnologiche, originate in ambito privato, tese a proteggere la sicurezza del Sistema Informatico Federale.
Per raggiungere questi obiettivi il Governo degli Stati Uniti si impegna a promuovere lo sviluppo della sicurezza informatica di per sé, e attraverso il finanziamento della ricerca tecnologica, in ambito pubblico[183] come in ambito privato, anche attraverso l'organizzazione di studi, convegni e pubblicazioni.
Come risulta evidente, il Governo degli Stati Uniti non cambia indirizzo: l'attenzione del legislatore è tutta incentrata sulla la promozione e lo sviluppo delle tecnologie utili a garantire un alto livello di sicurezza nazionale interna; solo un piccolo cenno è concesso al progresso tecnologico a livello internazionale ove si dichiara che il *Secretary of Commerce for Technologies* promuoverà ed incoraggerà l'uso di tecniche di sicurezza, come la crittografia, per favorire la protezione del sistema di informazioni esistente tra gli Stati.
L'intento è sempre quello di consentire alla giustizia di poter decifrare informazioni di matrice criminosa, con la creazione di un organismo tecnico presso il FBI.
E' evidente che l'amministrazione USA, resasi conto che una politica fortemente restrittiva disincentiva gli investimenti industriali, tenta di costruire un sistema liberale, senza peraltro riuscirci. La tendenza, infatti, rimane sempre quella di favorire i prodotti basati sul *key recovery*, sia pure con una semplificazione dei controlli: ciò al fine di svolgere improbabili indagini giudiziarie, ma sempre a danno della *privacy* dei cittadini. [184]

8. La politica dell'Unione Europea.

---

[183] La sez.10 lett.a) del *Computer Security Enhancement Act H.R. 1259*, recita nel modo seguente:
"*Not later than 90 days after the date of the enactment of this Act, the Secretary of Commerce shall enter into a contract with the National Research Council of the National Academy of Sciences to conduct a study of electronic authentication technologies for use by individuals, businesses, and government*".

[184] Così ROGNETTA G., *Firma digitale e documento informatico*, Edizioni Simone; il quale aggiunge anche: Tutto sommato, si può tranquillamente affermare che la politica seguita negli Stati Uniti mira ad una tendenziale compressione del diritto di crittografia dei cittadini. Sino a quando del resto, gli Stati Uniti manterranno in vita singolari iniziative, come la *Denied Persons List*, una vera e propria lista nera in cui vengono inserite le persone (indicate con nome, cognome e indirizzo) che si sono macchiate della grave colpa di aver violato l'EAR (*Export Administration Regulation*), non sembrano molto vicine delle soluzioni accettabili.

Il Regolamento e la Decisione del Consiglio dell'Unione Europea n.3381 del 19 dicembre 1994, relativo al controllo sulle esportazioni di beni a duplice uso, costituiscono la base della politica comunitaria in materia di esportazione di tecnologie crittografiche. La lista dei prodotti sottoposti a controllo è fondata su quanto previsto dal Wassenaar Arrangement e su altre politiche di restrizione di respiro internazionale.

9. Il Regolamento del 1994.

Il regolamento stabilisce, quale condizione necessaria per l'esportazione di un certo tipo di crittografia in un paese extra UE, il previo ottenimento di una licenza all'export. In un periodo di transizione verso l'attuale regime, tale licenza era considerata necessaria anche per l'esportazione in un paese comunitario o per prodotti di crittografia particolarmente sensibili.
Il regolamento, tuttavia, non coincide pienamente con i singoli regimi nazionali, non collimando con le politiche, gli obiettivi e la prassi individuali degli Stati membri.
Quale conseguenza di ciò, ogni paese ha sviluppato indipendentemente una propria politica di controllo, più o meno restrittiva, sulle esportazioni di crittografia.

10. La Decisione.

La Decisione, che modifica il Regolamento, prevede specifiche esenzioni in merito ai controlli sull'esportazione che producono taluni effetti anche nei riguardi dell'esportazione di crittografia. Inoltre, qualcuno ha inteso interpretare la Decisione in modo che l'esportazione di crittografia attraverso internet non ricadrebbe nell'ambito del Regolamento. In particolare, si sostiene da più parti, che ai sensi della Decisione, il controllo sulla tecnologia sarebbe limitato alle forme materiali, "*tangible form*". Inoltre, il "*General Technology Note*" della Decisione, statuisce che i controlli sulla tecnologia non trovano applicazione alle informazioni di pubblico dominio, così come il "*General Software Note*" (redatto sulle orme del *General Software Note* del Wassenaar Arrangement) statuisce che la lista delle esportazioni controllate non comprende i software "*in the public domain*" o "*generally available*" al pubblico. Tale esclusione è dettata dal fatto che tale tipologia di beni è venduta al dettaglio, senza restrizioni poiché costituisce una transazione *informale* a mezzo di ordini effettuati per posta, o per telefono, ovvero progettati per una facile installazione da parte dell'utente senza il supporto tecnico del fornitore.
Non esistono altre forme di controllo sulle esportazioni di crittografia di derivazione comunitaria. Tuttavia, il principio di libera circolazione dei beni sancito dal Trattato di Roma produce delle implicazioni nelle legislazioni dei singoli ordinamenti nazionali degli Stati Membri. Inoltre, La Risoluzione del

Consiglio d'Europa del 17 settembre 1995 sulle intercettazioni legali delle comunicazioni elettroniche prevede, nell'ambito dell'utilizzo della crittografia, quale requisito indispensabile per operatori del settore e providers, di effettuare il trasferimento dei segnali ricevuti senza codificarli.

11. La Comunicazione del 1997.

Nell'Ottobre del 1997, la Commissione Europea ha pubblicato la Comunicazione "Garantire la sicurezza e la fiducia nelle comunicazioni elettroniche - attraverso un quadro europeo per la Firma digitale e la Crittografia". Tale Comunicazione, nel trattare di chiavi crittografiche e di accesso alle stesse, descrive, con minuzia di dettagli, le tecniche di codificazione delle comunicazioni e sottolinea l'importanza che assume per privati cittadini, così come per le imprese, la sicurezza delle comunicazioni. In particolare, si legge che costituisce un preciso compito degli Stati Membri regolare i controlli sulle esportazioni di crittografia in modo conforme a quanto previsto dalla normativa europea, in relazione alla libera circolazione dei beni, ed alla Direttiva sulla protezione dei dati.
Sempre nell'ottica del divieto di ostacolare la libera circolazione dei beni e la sana concorrenza del mercato, la Comunicazione prosegue con un monito verso gli Stati Membri a puntare verso l'armonizzazione delle singole legislazioni nazionali in materia.
La Comunicazione, suggerisce l'emendamento del Regolamento sui beni a duplice uso al precipuo scopo di smantellare gradualmente il sistema dei controlli sull'esportazione di crittografia effettuati dai singoli ordinamenti, a meno che questi non siano da ritenersi davvero indispensabili per determinate tipologie di crittografia forte. Infine, la Comunicazione esorta tutti gli Stati Membri ad adoperarsi per sostenere la cooperazione al fine di creare un quadro unitario in materia di commercio elettronico nel quale standardizzare certificazioni e specifiche tecniche.
Nel Maggio del 1998, la Commissione ha adottato una Proposta di Regolamento per l'instaurazione di un regime comunitario sui controlli delle esportazioni di prodotti e tecnologie a duplice uso, che introduce piuttosto che un sistema di autorizzazioni, per il trasferimento all'interno dell'Unione europea dei prodotti di crittografia, una procedura di notificazioni.

12. L'attuale orientamento normativo comunitario.

Nel giugno del 2000 il Consiglio delle Comunità europee ha emanato un Regolamento[185] che istituisce un regime comunitario di controllo delle esportazioni di prodotti e tecnologie a duplice uso.

[185] Regolamento (CE) n.1334/2000 del Consiglio del 22 giugno 2000, in G.U. L.159, 30.06.2000. [Modificato dalle seguenti misure: Regolamento 2889/2000/CE del Consiglio del

In linea con quanto previsto dalle convenzioni internazionali, vengono considerati, dal Regolamento, beni a duplice uso tutti i prodotti, i software, le tecnologie (compresi i prodotti crittografici) che possono avere un'utilizzazione sia civile sia militare.[186] Tuttavia, rispetto al regolamento del 1994, il concetto esportazione viene allargato fino a ricomprendere le trasmissioni di software e tecnologie effettuate fuori dei paesi dll'UE mediante mezzi elettronici, fax e telefono.

13. La procedura per il rilascio dell'autorizzazione.

Ai sensi di questo regolamento l'esportazione di determinati prodotti elencati nell'allegato I è soggetta al rilascio di un'autorizzazione, da parte delle Autorità dello Stato Membro nel quale risiede l'esportatore è valida per tutto il territorio dell'Unione europea.[187] Il Regolamento prevede che, nel caso in cui si ritenga che un'esportazione possa nuocere agli interessi essenziali di sicurezza di uno Stato Membro, questo ha diritto di appellarsi all'altro Stato e chiedergli di non concedere l'autorizzazione all'esportazione o l'annullamento, la sospensione, la modifica o la revoca della stessa, dando così avvio ad una "consultazione" tra i due Stati.[188]

E' stato introdotto un altro tipo di autorizzazione, la "autorizzazione generale di esportazione della Comunità" per i prodotti compresi nell'All. I del regolamento 1334/2000, tranne quelli compresi nell'All.IV (controllo intracomunitario) ed altri 4 prodotti indicati nell'All. II. Tale autorizzazione è valida solo per le esportazioni verso 10 paesi (Australia, Canada, Repubblica Ceca, Ungheria Giappone, Nuova Zelanda, Norvegia, Polonia, Svizzera e USA).
Inoltre, è stato inserito, nel par. 2, il nuovo principio del "*catch more*" ai sensi del quale l'esportazione di beni duali non compresi nelle liste deve essere preventivamente autorizzata quando il Paese destinatario dei beni sia soggetto ad un embargo sugli armamenti dichiarato in sede internazionale congiuntamente al fatto che l'esportatore sia stato informato dalle competenti autorità che sono o possono essere destinati a scopi militari.
Per decidere il rilascio di un'autorizzazione, gli Stati Membri devono tener conto dei loro obblighi internazionali di non proliferazione, dalle posizioni

22 dicembre 2000 (G.U. L336, 30.12.2000); Regolamento 458/2001/CE del Consiglio del 6 marzo 2001 (G.U. L65, 07.03.2001); Regolamento 2432/2001/CE del Consiglio del 20 novembre 2001 (G.U. L338, 20/12/2001)].

186 Il Regolamento non si applica alla fornitura di servizi o alla trasmissione di tecnologie se ciò implica uno spostamento transfrontaliero di una persona fisica.

187 Per quanto riguarda, invece, i beni non compresi nell'elenco, anche la loro esportazione è subordinata all'ottenimento di un'autorizzazione d'esportazione nel caso in cui tali beni siano anche solo potenzialmente destinati allo sviluppo, produzione, utilizzo o disseminazione di armi chimiche biologiche o nucleari o di missili che fungano da vettori per tale tipo di armi.

188 Tutti i testi di legge di fonte comunitaria sono consultabili on-line nel sito dell'Unione Europea all'indirizzo: www.europa.eu.int

dell'Unione Europea, dell'OCSE o dell'ONU nonché dal codice di condotta dell'Unione europea in materia di esportazione di armamenti e dalle considerazioni relative alla finalità e al rischio di sviamenti di destinazioni.
Nel paragrafo 3 è stata inserita la clausola "*no-undercut*" per la quale, prima che uno Stato Membro rilasci un'autorizzazione, che sia stata precedentemente negata da un altro stato per una transazione sostanzialmente identica nei tre anni precedenti, deve consultare il paese che aveva negato l'autorizzazione. Se infine decide di rilasciare l'autorizzazione deve informarne tutti i partner e motivare la sua decisione alla Commissione.[189]

14. Altre iniziative d'origine europea.

Oltre a quanto previsto in seno all'Unione europea, altre iniziative, sebbene non dello stesso calibro, si sono succedute. Questa circostanza merita un breve cenno poiché dimostra come l'attenzione per questa delicata materia non sia limitata all'attività di quegli organismi prettamente preposti alla sua gestione bensì coinvolga altri soggetti in altri settori.
Nel 1995 il Consiglio d'Europa emanò un Regolamento che disciplinava questioni inerenti alla procedura penale e all'*information technology* e nel quale si legge: «le misure assunte debbono essere interpretate nel senso di minimizzare gli effetti negativi dell'uso della crittografia nelle investigazioni di stampo penale, senza tuttavia intaccare il suo legittimo uso più di quanto non sia strettamente necessario».
Un'altra iniziativa a livello europeo è rappresentata dalla conferenza "*Global Information Network*", tenuta a Bonn nel Luglio del 1997, e che radunava le rappresentanze ministeriali degli Stati Membri dell'Unione europea. I ministri congiuntamente riconobbero l'importanza della crittografia di tipo forte e la necessità della disponibilità al pubblico, a livello internazionale, dei prodotti crittografici. Tale tipo di dichiarazione, da una parte promuoveva e sollecitava il mercato di produzione dei prodotti e delle tecnologie di crittografia e, dall'altra, dava atto della necessità di predisporre una disciplina chiara coerente alle convenzioni internazionali ed ai principi sanciti a livello comunitario in riferimento alla libera circolazione dei beni.

15. La Convenzione sui crimini informatici.

Il 23 Novembre 2001, il Consiglio d'Europa ha adottato la *Convention on Cybercrime* in materia di crimini informatici.
La convenzione, finalizzata al controllo ed alla repressione dei crimini informatici disciplina ovviamente anche la crittografia e del suo possibile uso distorto ove sancisce che le Parti aderenti alla stessa, si obbligano a predisporre

[189] Si veda il commento al Regolamento pubblicato sul sito del Ministero del Commercio con l'Estero alla pagina www.mincomes.it/dualuse/reg1334_2000/comment.htm

e disciplinare una Autorità competente al controllo dei dati conservati in sistemi informatici e banche dati presenti sul proprio territorio, attraverso la quale gli altri stati firmatari, tramite una procedura particolare, possano acquisire le informazioni, i documenti ed in generale i dati che riterranno necessari per la repressione della criminalità informatica.
La finalità, peraltro apprezzabilissima di questo accordo, potrebbe, a mio avviso rivelarsi piuttosto pericolosa per la riservatezza delle comunicazioni che viaggiano in rete ed ancora di più per le comunicazioni ed i documenti legittimamente protetti da crittografia.
Questo scrupolo è stato evidentemente avvertito dal legislatore che, volendo tranquillizzare gli animi di utenti e *software house*, ha inserito nella Relazione Esplicativa alla Convenzione la seguente precisazione: "*(…) the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered as legitimate protection of privacy and, therefore, be considered as being undertaken with right.*".
La convenzione, firmata a Budapest, non è di applicazione automatica, è stata firmata da 33 paesi e ratificata solo dall'Albania. Entrerà in vigore solo con la ratifica di 5 paesi di cui almeno 3 membri del Consiglio d'Europa.[190]

16. I singoli ordinamenti.

Come abbiamo avuto modo di indicare in precedenza, la politica perseguita dall'Unione europea è improntata alla creazione di linee guida che lascino i singoli ordinamenti liberi di disciplinare in modo autonomo le questioni inerenti alla crittografia. I singoli ordinamenti, tuttavia, hanno reagito in modo assolutamente condizionato dalle politiche di derivazione comunitaria ed internazionale, adeguandosi in modo più o meno pedissequo alle indicazioni dell'Unione Europea o delle Convenzioni internazionali.
Solo alcuni degli Stati Membri, parte dei quali si intende portare all'attenzione del lettore, insieme con alcuni Paesi extra-UE, hanno adottato proprie politiche di regolamentazione della produzione di crittografia, del suo utilizzo e della sua esportazione.

17. La politica della Francia.

Per lungo tempo la Francia ha adottato un atteggiamento di forte restrizione sulle importazioni, esportazioni, utilizzazione e commercializzazione dei prodotti crittografici. Il suo regime era basato su un regolamento che, distinguendo tra crittografia utilizzabile solo ai fini dell'autenticazione del messaggio e crittografia utilizzabile a fini di riservatezza del messaggio stesso,

---

[190] Il testo della convenzione e la sua relazione esplicativa sono consultabili sul sito www.conventions.coe.int, dati aggiornati al 18/08/02.

prevedeva che la distribuzione, l'esportazione e l'uso della crittografia fossero sottoposti a due requisiti:

- dichiarazione che la crittografia sarebbe stata utilizzata esclusivamente a scopo di autenticazione dei documenti e garanzia di integrità dei messaggi trasmessi;
- preventiva autorizzazione del Primo Ministro, negli altri casi.

Da questo sistema fortemente restrittivo, con una legge del 1996[191], si passò ad un regime leggermente più liberale, ma in ogni caso severo rispetto allo scenario legislativo comunitario.
Il testo di legge del '96 prevedeva che fossero soggette al requisito della preventiva dichiarazione solamente le esportazioni di tecnologie a base crittografica utilizzate a fini di autenticazione e forniva una lista di tecnologie soggette a tale preventiva dichiarazione d'uso e ad autorizzazione (ad esempio le chiavi crittografiche di lunghezza superiore a 40 bits) [192].
Le *software house* produttrici di tecnologie crittografiche, inoltre, per poter sviluppare, utilizzare e presentare i loro prodotti erano soggette al preventivo controllo del SCSSI[193], l'organismo governativo preposto alla sorveglianza in tema di crittografia. Era perfino proibito l'uso di qualunque tipo di crittografia da parte di radio amatori. [194]
L'inosservanza della legge era punita con una sanzione pecuniaria fino a 500.000 franchi e tre mesi di reclusione.
Nel 1998 venne pubblicato il piano d'azione sull'e-commerce e, in quella occasione il Governo francese, sulla spinta dell'entusiasmo per le nuove tecnologie da una parte, e sulla base delle emergenti esigenze di sicurezza della rete dall'altra, dichiarò che il nuovo orientamento del Governo era diretto ad un'interpretazione in senso più liberale della legge, ponendo i presupposti per un lento cambiamento che avrebbe condotto al clamoroso annuncio del Primo Ministro francese Lionel Jospin del 19 gennaio 1999 con il quale, in occasione della conferenza innanzi al comitato interministeriale per la società dell'informazione, pur senza fare alcun riferimento al tema della esportazione, affermava una netta inversione di tendenza della politica francese ed annunciava l'elevazione della soglia di crittografia libera a 128 bits.
Il Primo Ministro dichiarò che la liberalizzazione dell'uso di crittografia costituiva uno strumento di lotta contro la "guerra elettronica", i cui effetti sono giudicati, a livello internazionale, molto più preoccupanti per la sicurezza del Paese.[195]

---

191 La cosiddetta "legge del 26 Luglio" i cui decreti di attuazione si fecero attendere per ben due anni.
192 Il Governo francese vietava l'uso del PGP e proponeva un software alternativo che, tuttavia, ebbe pochissima fortuna a causa della scarsa fiducia degli utenti nelle garanzie di riservatezza in capo ad uno strumento pubblico.
193 Servizio Centrale per la Sicurezza dei Sistemi di Informazione.
194 B.-J. KOPPS, *The Crypto Controversy, a Key Conflict in the Information Society,* Kluwer Law International, 1999, The Hague, The Netherlands, pagg.104-105.
195 *Le Monde* del 21 Gennaio 1999.

Attualmente, il *Projet de Loi sur la société de l'information*[196], presentato da Jospin, non ha ancora ricevuto la definitiva approvazione. Tuttavia, come anticipato dal comunicato stampa del 1999, il testo presenta un regime piuttosto liberale rispetto al passato. Scorrendo gli articoli dal 36 al 47, dedicati alla disciplina della crittografia, balza all'occhio l'*incipit* dell'art.37 in cui si legge: "*L'utilisation des moyens de cryptologie est libre*".
La fornitura, il trasferimento da o verso uno degli Stati Membri dell'Unione europea, l'importazione e l'esportazione dei sistemi di crittografia aventi la sola funzione di autenticazione o di controllo dell'integrità del documento, in particolare i fini della firma elettronica, sono interamente liberi. Tutti gli altri modelli di tecnologie a base crittografica, qualunque sia l'attività che se ne intenda fare, inclusa la fornitura di servizi di crittografia, sono sottoposti a preventiva autorizzazione del Primo Ministro.[197]
I criteri che regolano il rilascio della citata autorizzazione, e le eventuali esenzioni, saranno regolati con decreto. La mancata dichiarazione è sanzionata con la reclusione fino ad un anno.

18. La Germania.

L'esportazione di crittografia in Germania è regolata sulla base del regolamento comunitario e del Wassenaar Arrangement cui la Germania ha aderito.[198]
Nonostante l'adeguamento al regime generalmente adottato dagli altri Stati, Membri e non dell'Unione europea, il Governo, con un annuncio del 2 giugno 1999, ha dichiarato che la politica che intende perseguire in materia di crittografia può essere sommariamente riassunta in cinque principi.
- Il Governo tedesco non intende limitare la libera utilizzazione della crittografia e sosterrà lo sviluppo della sicurezza su base crittografica.
- Il Governo intende creare un'infrastruttura capace di rafforzare la fiducia degli utenti nella sicurezza delle tecnologie di crittografia.
- Il Governo ritiene indispensabile l'apporto delle *software house* nella produzione di tecnologie sicure ed efficaci.
- L'impulso dato alla materia non intaccherà il potere statale di intercettare le comunicazioni. Ogni sviluppo verrà attentamente monitorato.
- Viene riposta grande fiducia nella cooperazione internazionale.

Su queste basi, nell'agosto dello stesso anno, il Ministero degli Affari Economici rilasciò un comunicato stampa con il quale dichiarava che i controlli sulle esportazioni di crittografia a largo uso venivano ridotti al minimo necessario.
Le uniche eccezioni previste riguardano le esportazioni destinate a particolari aree geografiche o per particolari apparecchi militari, per i quali gli stessi produttori possono decidere se inserirli nella categoria dei prodotti a largo

---

196 Progetto n.3143, presentato alla Presidenza dell'Assemblea Nazionale il 14 giugno 2001, rinviato alla Commissione per gli affari culturali, familiari e sociali.
197 (*Tdr*)
198 Bundesanzeiger 31 Agosto 1999.

consumo o meno. L'organismo preposto al controllo della normativa è il BAFA (Bundesausfuhramt), l'agenzia federale per le esportazioni.

19. L'Italia.

Il quadro normativo italiano relativo ai modelli ed alle tecnologie a base crittografica si presenta disomogeneo e frazionato. I riferimenti normativi offerti dal nostro ordinamento sono costituiti, oltre alle leggi relative alla protezione del segreto di Stato e alla divulgazione di informazioni riservate (L. 24 ottobre 1977 n.801), le leggi n.185 del 1990 e n.222 del 1992, e relativi decreti di attuazione, sull'esportazione ed importazione dei beni a duplice uso e tecnologie di crittografia.
In ambito di e-Government e pubblica amministrazione, inoltre, rilevano alcune deliberazioni dell'AIPA[199], che trattano di sistemi di cifratura, e le leggi sulla semplificazione della Pubblica Amministrazione.[200]
Quale membro del Wassenaar Arrangement e dell'Unione Europea, l'Italia ha abbracciato la politica comunitaria di regolamentazione delle esportazioni[201] ed ha disciplinato la materia tramite l'emanazione della L. 185 del 1990 nella quale è confluito il precedente disegno di legge n.203 del 1987 ("Nuove norme sul controllo dell'esportazione, importazione e transito di materiali di particolare interesse strategico").
L'art.2 della legge in questione include tra i materiali di armamento i "sistemi o apparecchi elettronici (...) appositamente costruiti per uso militare" e, unitamente alla legge n.222 del 1992, prevede sanzioni penali per i reati di falsità nella documentazione, per l'esportazione, importazione e transito di materiali di armamento compiuti senza autorizzazione e per la violazione delle regole di consegna previste dalla normativa amministrativa.
L'autorità competente in materia è il Ministero del Commercio con l'Estero - Direzione Generale per la politica commerciale e per la gestione del regime degli scambi - Divisione IV, che provvede al rilascio delle autorizzazioni all'esportazione di prodotti e tecnologie a duplice uso nonché alle relative

---

[199] L'Autorità per l'Informatica nella Pubblica Amministrazione istituita con il decr. leg. n.39 del 1993.

[200] "In realtà un tentativo di regolamentare in generale l'uso dei 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, radiofiniche o di altre forme di telecomunicazioni." Tuttavia, il disegno di legge non trovò mai attuazione. CARLO SARZANA, di S. Ippolito - I riflessi normativi dei sistemi crittografici in Italia, n.4 gennaio -aprile 1996, Saggi e articoli, www.sisde.it

[201] L'adozione del nuovo Regolamento comunitario 1334/2000 è avvenuta con decreto del 13 novembre 2000 (G.U. n.278 del 28 novembre 2000). Il testo del decreto è visionabile sul sito del Ministero del Commercio con l'Estero (Ministero delle Attività produttive), alla pagina www.mincomes.it/dualuse/reg1334_2000/dm131100htm

misure di controllo e, ogni sei mesi, con decreto, aggiorna la lista dei beni sottoposti a controllo.
Passando ad indicare le fonti normative inerenti la pubblica amministrazione, le prime espressioni dell'esigenza di regolamentazione dell'uso della crittografia ci vengono fornite dall'AIPA, organo di controllo della sicurezza nelle comunicazioni, che possiede anche la facoltà di pronunciare deliberazioni.
Con deliberazione del 28 luglio 1994[202], tale autorità, sancendo l'equiparazione tra il documento elettronico ed il documento cartaceo, annunciava che l'uso della crittografia, la protezione e conservazione delle chiavi crittografiche e l'uso dei sistemi di firma elettronica sarebbero stati oggetto di successivi provvedimenti legislativi.
Inoltre, nella relazione esplicativa si legge 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 chiave individuali e le relative responsabilità".
E cenni relativi alla sicurezza delle comunicazioni e l'uso e la distribuzione di prodotti a base crittografica, nella fase di aggiornamento e ristrutturazione che sta attraversando la Pubblica Amministrazione, si rinvengono in ogni testo di legge.
L'impulso più forte, probabilmente, è arrivato con l'emanazione della Legge Bassanini n.59 del 1997 (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 amministrativa) che, perseguendo lo scopo di semplificare la lenta macchina burocratica del nostro Paese, ha prestato attenzione all'argomento delle comunicazioni elettroniche prevedendo che tutti gli atti, i dati ed i documenti trasmessi tanto da privati che da enti pubblici attraverso l'uso di computer, sistemi informatici e telecomunicazioni in genere devono considerarsi legalmente validi a tutti gli effetti di legge.
Il percorso legislativo del nostro ordinamento ha dunque predisposto un apparato normativo che, attraverso la legge sulla protezione dei dati personali (L.675/96 e successive modifiche), nella quale viene enfatizzata l'importanza dello strumento della cifratura per la riservatezza delle comunicazioni, passando per il D.P.R. 513 del 1997, che ha posto le fondamenta per la formulazione dei criteri e delle modalità di trasmissione dei documenti, è giunta alla formulazione della legge di recepimento della direttiva comunitaria n.93 del 1999 sulla firma elettronica.
Tale ultima legge, affiancata dal decreto legislativo n.10 del 2002 di recente emanazione, attraverso la distinzione tra firma elettronica "avanzata" e firma elettronica "leggera", l'identificazione e la regolamentazione degli enti di certificazione, è evidentemente incentrata quasi esclusivamente sulle tecnologie a base crittografica che permettono la codificazione dei documenti sottoscritti con firma digitale e che, come conseguenza di ciò dovrebbero portare alla crescita della sicurezza delle comunicazioni in rete della cui importanza abbiamo già avuto modo di parlare.

---

[202] G.U. n.216 del 15 settembre 1994.

20. I Paesi Bassi[203]

Anche i Paesi Bassi hanno aderito al Wassenaar Arrangement ed al sistema di controllo delle esportazioni di crittografia adottato dall'Unione Europea.
L'autorità competente al rilascio delle licenze di esportazione è L'*Afdeling Exportcontrole en Sanctiebeleid* del Ministero degli Affari Economici.[204]
Il legislatore olandese ha sempre riconosciuto e temuto la diffusione della crittografia forte, tanto che nel 1994 venne approvato un disegno di legge che vietava la detenzione, l'uso e la distribuzione di crittografia forte ed affidava alle autorità pubbliche il controllo delle chiavi.
Molte proteste si levarono a riguardo ed il progetto non trovò mai applicazione, tuttavia, pare che il progetto, emendato nei punti giusti, possa essere riproposto all'approvazione dell'assemblea.
La normativa esistente in Olanda prevede che, per motivi di pubblica sicurezza, se un agente durante una perquisizione rileva che un computer contiene documenti cifrati, può chiedere a chiunque si suppone possa conoscerne i codici, di decifrare i documenti, la collaborazione è obbligatoria, pena la reclusione fino a tre mesi.

21. La Svezia.

La Svezia è uno dei Paesi che hanno aderito al Wassenaar Arrangement e, come tale pratica una politica di restrizione sulle esportazioni di tecnologia di crittografia. L'autorità competente in materia è l'Ispettorato per i beni strategici (ISP).
Il Governo svedese, nonostante l'adesione al Wassennar Arrangement e l'adozione di un regime di controllo ha sempre professato l'esigenza di ridurre gradualmente i controlli sulle esportazioni fino al loro totale eliminazione.
Il suo ordinamento prevede che l'Autorità competente (ISP) possa emanare leggi atte a regolare le esportazioni di crittografia e nel 1999 l'ISP statuì la libera esportabilità di prodotti a base crittografica simmetrica a 128 bit, oltre che ai Paesi dell'Unione, verso i quali non si applica il concetto di esportazione, ad una rosa di 60 Paesi.[205]

---

[203] Il Prof. Bert-Jaap Koops ci riferisce che il Governo olandese intende emendare l'attuale apparato normativo per adeguarlo all'esigenza di regolare il fenomeno della ri-esportazione di beni a duplice uso che transitano nel territorio olandese e che possiedono una qualche rilevanza economica. www.rechten.kub.nl/koops/cryptolaw/index.htm
[204] http://ethesis.helsinki.fi/julkaisut/oik/julki/pg/parviainen/cryptogr/pdf
[205] La lista dei Paesi è visionabile sul sito www.id2tech.com/whitepapers/export.htm

Capitolo Settimo

Il Wassenaar Arrangement

Sommario: 1. Le finalità. – 2. La *control list*. – 3. Le procedure. – 4. Il coordinamento tra gli Stati.

1. Le finalità.

Il documento *The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*

Initial Elements
(See the new Appendix 3 that replaces the original Wassenar Arrangement Initial Elements adopted originally on 12 July 1996.)

I. Purposes
1. The Wassenaar Arrangement has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating states will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

2. It will complement and reinforce, without duplication, the existing control regimes for weapons of mass destruction and their delivery systems, as well as other internationally recognised measures designed to promote transparency and greater responsibility, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where the risks are judged greatest.

3. This arrangement is also intended to enhance cooperation to prevent the acquisition of armaments and sensitive dual-use items for military end-uses, if the situation in a region or the behaviour of a state is, or becomes, a cause for serious concern to the participating states.

4. This arrangement will not be directed against any state or group of states and will not impede bona fide civil transactions. Nor will it interfere with the rights of states to acquire legitimate means with which to defend themselves pursuant to Article 51 of the Charter of the United Nations.

II. Scope

1. Participating states will meet on a regular basis to ensure that transfers of conventional arms and transfers in dual-use goods and technologies are carried out responsibly and in furtherance of international and regional peace and security.

2. To this end, participating states will exchange, on a voluntary basis, information that will enhance transparency, will lead to discussions among all participating states on arms transfers, as well as on sensitive dual-use goods and technologies, and will assist in developing common understandings of the risks associated with the transfer of these items. On the basis of this information they will assess the scope for coordinating national control policies to combat these risks. The information to be exchanged will include any matters which individual participating states wish to bring to the attention of others, including, for those wishing to do so, notifications which go beyond those agreed upon.

3. The decision to transfer or deny transfer of any item will be the sole responsibility of each participating state. All measures undertaken with respect to the arrangement will be in accordance with national legislation and policies and will be implemented on the basis of national discretion.

4. In accordance with the provisions of this arrangement, participating states agree to notify transfers and denials. Initially, these notifications will apply to all non-participating states. In the light of the general and specific information exchange, the scope of these notifications, as well as their relevance for the purposes of the arrangement, will be reviewed. Notification of a denial will not impose an obligation on other participating states to deny similar transfers. However, a participating state will notify, preferably within 30 days, but no later than within 60 days, all other participating states of an approval of a licence which has been denied by another participating state for an essentially identical transaction during the last three years.

5. Upon the commencement of this arrangement, participating states agree that work on further guidelines and procedures will continue expeditiously and taking into account experience acquired. This will include, in particular, a review of the scope of conventional arms to be covered with a view to extending information and notifications beyond the categories described in Appendix 3. Participating states agree to discuss further how to deal with any areas of overlap between the various lists.

6. Participating states agree to assess the overall functioning of this arrangement regularly, for the first time in 1999.

2. La control list.

III. Control Lists
1. Participating states will control all items set forth in the List of Dual-Use Goods and Technologies and in the Munitions List (see Appendix 5)*, with the objective of preventing unauthorised transfers or retransfers of those items.

2. The List of Dual-Use Goods and Technologies (tier 1) has two annexes of sensitive (tier 2) and a limited number of very sensitive items (subset tier 2).

3. The lists will be reviewed regularly to reflect technological developments and experience gained by participating states, including in the field of dual-use goods and technologies which are critical for indigenous military capabilities. In this respect, studies shall be completed to coincide with the first revision to the lists to establish an appropriate level of transparency for pertinent items.

* (France and the Russian Federation view this list as reference list drawn up to help in the selection of dual-use goods which could contribute to the indigenous development, production or enhancement of conventional munitions capabilities.)

3. Le procedure.

IV. Procedures for the General Information Exchange
1. Participating states agree to exchange general information on risks associated with transfers of conventional arms and dual-use goods and technologies in order to consider, where necessary, the scope for coordinating national control policies to combat these risks.

2. A list of possible elements of the general information exchange on non-participating states is contained in Appendix 1.

V. Procedures for the Exchange of Information on Dual-Use Goods and Technology
1. Participating states will notify licences denied to non-participants with respect to items on the List of Dual-Use Goods and Technologies, where the reasons for denial are relevant to the purposes of the arrangement.

2. For tier 1, participating states will notify all licences denied relevant to the purposes of the arrangement to nonparticipating states, on an aggregate basis, twice per year. The indicative content of these denial notifications is described in Appendix 2.

3. For items in the second tier and its subset of very sensitive items, participating states will notify, on an individual basis, all licences denied pursuant to the purposes of the arrangement to non-participating states.

Participating states agree that notification shall be made on an early and timely basis, that is preferably within 30 days but no later than within 60 days, of the date of the denial. The indicative content of these denial notifications is described in Appendix 2.

4. For items in the second tier, participating states will notify licences issued or transfers made relevant to the purposes of the arrangement to non-participants, on an aggregate basis, twice per year. The indicative content of these license/transfer notifications is described in Appendix 2.

5. Participating states will exert extreme vigilance for items included in the sub-set of tier 2 by applying to those exports national conditions and criteria. They will discuss and compare national practices at a later stage.

6. Participating states agree that any information on specific transfers, in addition to that specified above, may be requested, inter alia through normal diplomatic channels

VI. Procedures for the Exchange of Information on Arms
1. Participating states agree that the information to be exchanged on arms will include any matters which individual participating states wish to bring to the attention of others, such as emerging trends in weapons programmes and the accumulation of particular weapons systems, where they are of concern, for achieving the objectives of the arrangement.

2. As an initial stage in the evolution of the new arrangement, participating states will exchange information every six months on deliveries to nonparticipating states of conventional arms set forth in Appendix 3, initially derived from the categories of the UN Register of Conventional Arms. The information should include the quantity and the name of the recipient state and, except in the category of missiles and missile launchers, details of model and type.

3. Participating states agree that any information on specific transfers, in addition to that specified above, may be requested, inter alia through normal diplomatic channels.

4. Il coordinamento tra gli Stati.

VII. Meetings and Administration
1. Participating states will meet periodically to take decisions regarding this arrangement, its purposes and its further elaboration, to review the lists of controlled items, to consider ways of coordinating efforts to promote the development of effective export control systems, and to discuss other relevant matters of mutual interest, including information to be made public.

2. Plenary meetings will be held at least once a year and chaired by a participating state on the basis of annual rotation. Financial needs of the arrangement will be covered under annual budgets, to be adopted by plenary meetings.

3. Working groups may be established, if the plenary meeting so decides.

4. There will be a secretariat with a staff necessary to undertake the tasks entrusted to it.

5. All decisions in the framework of this arrangement will be reached by consensus of the Participating States.

VIII. Participation

The new arrangement will be open, on a global and nondiscriminatory basis, to prospective adherents that comply with the agreed criteria in Appendix 4. Admission of new participants will be based on consensus.

IX. Confidentiality

Information exchanged will remain confidential and be treated as privileged diplomatic communications. This confidentiality will extend to any use made of the information and any discussion among participating states.

Capitolo Ottavo

Il Regolamento n. 3381/94

SOMMARIO: 1. Il Regolamento. - 2. Le disposizioni generali. - 3. L'ambito di applicazione. - 4. L'autorizzazione d'esportazione. - 5. Le procedure doganali. - 6. La cooperazione amministrativa.- 7. Le misure di controllo. - 8. Le disposizioni comuni e finali.

1. Il Regolamento.

Il Regolamento (CE) n. 3381/94 del Consiglio dell'Unione Europea, del 19 dicembre 1994
che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso (modificato dal Regolamento (UE) 837/95), è un documento particolarmente interessante. In esordio, nei vari considerando vengono espressi principi molto interessanti.
1) nella realizzazione del mercato interno, la libera circolazione delle merci, ivi compresa quella dei beni a duplice uso, dev'essere assicurata in conformità alle pertinenti disposizioni del trattato; che gli scambi intracomunitari di taluni beni a duplice uso sono attualmente assoggettati a controlli da parte degli Stati membri; che una condizione per l'abolizione di detti controlli è costituita dall'applicazione ad opera degli Stati membri di controlli il più efficaci possibile all'esportazione dei suddetti beni, sulla base di norme comuni, nel quadro di un regime comunitario; che l'abolizione di tali controlli migliorerà la competitività internazionale dell'industria europea;
2) che scopo del Regolamento è altresì quello di sottoporre a controlli efficaci i beni a duplice uso quando sono esportati dalla Comunità;
3) è necessario un efficace sistema di controllo all'esportazione dei beni a duplice uso su una base comune anche per rispettare gli impegni internazionali degli Stati membri e dell'Unione Europea, segnatamente in materia di non proliferazione;
4) gli elenchi comuni di beni a duplice uso, di destinazioni e di linee direttrici sono essenziali per un sistema di controllo efficace; che le decisioni riguardanti il contenuto di detti elenchi hanno natura strategica e sono quindi di competenza degli Stati membri; che tali decisioni sono oggetto di un'azione comune in base all'articolo J.3 del trattato sull'Unione europea;
5) i ministri degli Affari esteri della Comunità hanno adottato il 20 novembre 1984 la dichiarazione di politica comune, successivamente adottata dalla Spagna e dal Portogallo, riguardante in particolare le modalità relative ai trasferimenti intracomunitari di plutonio separato e di uranio arricchito al di là

del 20 %, nonché gli impianti, le componenti principali di fondamentale importanza e la tecnologia per il trattamento, l'arricchimento e la produzione di acqua pesante;
6) la suddetta azione comune e il presente regolamento costituiscono un sistema integrato;
7) tale sistema costituisce un primo passo verso la creazione di un sistema comune di controllo delle esportazioni dei beni a duplice uso, completo e coerente in tutti i suoi elementi; che è particolarmente auspicabile che le procedure di autorizzazione applicate dagli Stati membri siano armonizzate progressivamente e rapidamente;
8) la Comunità ha adottato un insieme di norme doganali che costituiscono il codice doganale comunitario (3) e le relative disposizioni di applicazione (4); i quali stabiliscono, tra l'altro, le disposizioni relative all'esportazione e alla riesportazione di beni; che il presente regolamento non pone alcuna restrizione ai poteri attribuiti dal codice e dalle relative disposizioni d'applicazione ovvero da questi ultimi derivanti;
9) è opportuno che, nell'esaminare le condizioni riguardanti la riesportazione o l'utilizzazione finale dei beni a duplice uso, gli Stai membri tengano conto dei pertinenti principi del diritto internazionale;
10) le disposizioni degli articoli 4 e 5 del presente regolamento hanno lo scopo di assicurare un controllo efficace delle esportazioni dei beni a duplice uso; che tali disposizioni non pregiudicano la possibilità degli Stati membri di adottare o di mantenere, allo stesso scopo e nel pieno rispetto del mercato interno, misure supplementari di controllo delle esportazioni che siano compatibili con gli obiettivi del presente regolamento;
11) per eliminare i rischi di deviazioni di traffico di beni a duplice uso dalla destinazione dichiarata in un altro Stato membro verso una destinazione fuori della Comunità, durante la fase iniziale di adeguamento degli Stati membri alle disposizioni del presente regolamento, è opportuno prevedere per detto periodo l'applicazione di controlli semplificati sugli scambi intracomunitari dei beni a duplice uso; che tale applicazione può comprendere un sistema di autorizzazioni generali; che il periodo di applicazione deve avere una durata limitata; che durante il periodo di applicazione gli scambi intracomunitari di beni a duplice uso non devono essere soggetti a controlli più rigorosi di quelli applicati alle esportazioni dalla Comunità;
12) in virtù ed entro i limiti dell'articolo 36 del trattato ed in attesa di una armonizzazione più approfondita, gli Stati membri conserveranno sia durante che dopo il periodo transitorio la possibilità di effettuare controlli su beni a duplice uso per garantire l'ordine pubblico o la pubblica sicurezza;
13) per garantire l'effettiva applicazione del presente regolamento, ciascuno Stato membro adotterà provvedimenti intesi a conferire adeguati poteri alle autorità competenti;
14) ciascuno Stato membro stabilisce le sanzioni da imporre in caso di violazione delle disposizioni del presente regolamento,

2. Le disposizioni generali.

Il Titolo I del Regolamento prevede le Disposizioni Generali.
Articolo 1: Il presente regolamento istituisce un regime comunitario di controllo delle esportazioni dei beni a duplice uso.
Articolo 2 : Ai fini del presente regolamento si intende per: a) "beni a duplice uso" i beni che possono avere un utilizzo sia civile che militare; b) "esportazione" il regime che permette l'uscita temporanea o definitiva di merci comunitarie dal territorio doganale della Comunità conformemente all'articolo 161 del codice doganale comunitario; tale regime comprende anche la riesportazione, ossia l'operazione che consiste nell'uscita di merci non comunitarie dal territorio doganale della Comunità, ai sensi dell'articolo 182 di detto codice; c)"esportatore" qualsiasi persona fisica o giuridica per conto della quale è resa la dichiarazione d'esportazione e che abbia la proprietà dei beni a duplice uso o un analogo diritto a disporre di essi al momento dell'accettazione della dichiarazione. Qualora titolare del diritto di proprietà o del diritto analogo sia una persona stabilita fuori della Comunità secondo il contratto in base al quale è effettuata l'esportazione, si considera esportatore la parte contraente stabilita nella Comunità; d)"autorità competenti" le autorità incaricate della applicazione del presente regolamento negli Stati membri; e)"dichiarazione d'esportazione" l'atto con il quale una persona manifesta, nelle forme e secondo le modalità prescritte, la volontà di sottoporre un bene a duplice uso al regime doganale di esportazione.

3. L'ambito di applicazione.

Il titolo II definisce l'ambito di applicazione.
L'articolo 3 dispone che 1. L'esportazione dei beni a duplice uso compresi nell'elenco di cui all'allegato I della decisione 94/942/PESC del Consiglio, del 19 dicembre 1994, relativa all'azione comune, adottata dal Consiglio in base all'articolo J.3 del trattato sull'Unione europea, riguardante il controllo delle esportazione dei beni a duplice uso (5), è subordinata ad autorizzazione; 2. Può essere subordinata ad autorizzazione conformemente agli articoli 4 e 5 anche l'esportazione verso tutte o talune destinazioni di determinati beni a duplice uso non compresi nell'elenco di cui all'allegato I della decisione 94/942/PESC. 3. I beni a duplice uso che attraversano semplicemente il territorio della Comunità, siano essi o meno sottoposti ad un regime di transito, non sono soggetti alle disposizioni del presente regolamento: uno Stato membro può adottare le misure appropriate per quanto riguarda tali beni.
L'articolo 4 dispone che 1. L'esportazione di beni a duplice uso non compresi nell'elenco di cui all'allegato I della decisione 94/942/PESC dev'essere subordinata alla presentazione di un'autorizzazione d'esportazione non appena l'esportatore è informato dalle sue autorità che detti beni sono o possono essere destinati, in tutto o in parte, a contribuire allo sviluppo, alla produzione, al maneggio, al funzionamento, alla manutenzione, alla conservazione, alla

individuazione, all'identificazione o alla disseminazione di armi chimiche, biologiche o nucleari o allo sviluppo, alla produzione, al mantenimento o alla conservazione di missili atti a portare tali armi, coperte dai corrispondenti regimi di non proliferazione; 2. L'esportatore, se ha conoscenza che i beni in questione sono destinati, in tutto o in parte, a una delle finalità di cui al paragrafo 1, deve informare le sue autorità, che decidono in merito all'opportunità di sottoporre la suddetta esportazione ad autorizzazione; 3. Gli Stati membri possono adottare o conservare le normative nazionali in cui sia previsto che l'esportatore sia tenuto ad informare le autorità del suo paese qualora abbia motivo di sospettare che i beni in questione siano destinati, in tutto o in parte, ad una delle finalità di cui al paragrafo 1 e che, in tal caso, l'esportazione possa essere soggetta ad autorizzazione.
L'articolo 5 indica che 1. Al fine di perseguire in modo efficace gli obiettivi del presente regolamento in materia di controllo delle esportazioni uno Stato membro può vietare o subordinare ad autorizzazione l'esportazione di beni a duplice uso non compresi nell'elenco dell'allegato I della decisione 94/942/PESC. 2. Il paragrafo 1 si applica alle misure: a) esistenti alla data di entrata in vigore del presente regolamento; b) adottate dopo la data di entrata in vigore del presente regolamento. 3. Gli Stati membri notificano agli altri Stati membri e alla Commissione le misure di cui al paragrafo 2, lettera a), entro un mese dalla data di entrata in vigore del presente regolamento. Gli Stati membri notificano agli altri Stati membri e alla Commissione le misure di cui al paragrafo 2, lettera b), immediatamente dopo la loro adozione. Gli Stati membri notificano inoltre agli altri Stati membri e alla Commissione ogni modifica riguardante le misure di cui al paragrafo 2, lettere a) e b). 4. La Commissione pubblica le misure notificate ai sensi del paragrafo 3 nella *Gazzetta ufficiale delle Comunità europee*, serie C.

4. L'autorizzazione di esportazione.

Il Titolo III si occupa della autorizzazione di esportazione.
L'articolo 6 dispone che 1. Per ogni operazione di esportazione soggetta al presente regolamento è richiesta un'autorizzazione specifica. Tuttavia gli Stati membri possono concedere le agevolazioni di formalità semplificate come previsto ai punti seguenti: a) un'autorizzazione generale per un bene o una categoria di beni a duplice uso, in conformità alle disposizioni di cui all'allegato II della decisione 94/942/PESC; b) un'autorizzazione globale ad un determinato esportatore per un tipo o una categoria di beni a duplice uso, valida per le esportazioni dirette ad una o più destinazioni specifiche; c) procedure semplificate nel caso in cui uno Stato membro richieda un'autorizzazione in forza dell'articolo 5. 2. Se del caso, un'autorizzazione d'esportazione può essere subordinata a determinati requisiti e condizioni. Le autorità competenti di uno Stato membro possono, in particolare, richiedere una dichiarazione sull'utilizzazione finale e imporre altre condizioni riguardanti

l'utilizzazione finale e/o la riesportazione dei beni. 3. L'autorizzazione d'esportazione è valida nell'insieme della Comunità.
L'articolo 7 indica che 1. L'autorizzazione di esportazione è rilasciata dalle autorità competenti dello Stato membro in cui risiede l'esportatore. 2. Se i beni a duplice uso per i quali è stata richiesta un'autorizzazione di esportazione individuale per una destinazione non specificamente menzionata nell'allegato II della decisione 94/942/PESC, o per tutte le destinazioni nel caso dei beni molto sensibili che figurano nell'allegato IV della stessa decisione si trovano o si troveranno in un altro Stato membro, ciò deve essere indicato nella richiesta. Le autorità competenti per il rilascio delle licenze dello Stato membro al quale viene chiesta l'autorizzazione consultano immediatamente le autorità competenti per il rilascio delle licenze dello Stato membro o degli Stati membri in questione e forniscono loro tutte le informazioni pertinenti. Lo Stato membro o gli Stati membri consultati comunicano, entro dieci giorni lavorativi dalla ricezione delle informazioni di cui all'articolo 14 o di qualsiasi altra informazione complementare richiesta, eventuali riserve nei confronti del rilascio dell'autorizzazione che vincolano lo Stato membro in cui è stata fatta la richiesta. In difetto di una risposta entro il termine suddetto, il parere dello Stato membro consultato sarà considerato positivo. 3. Qualora un'esportazione pregiudichi i suoi interessi vitali, uno Stato membro può chiedere ad un altro Stato membro di non concedere un'autorizzazione d'esportazione, oppure, qualora siffatta autorizzazione sia stata concessa, chiedere l'annullamento, la sospensione, la modifica o la revoca. Lo stato membro che ha ricevuto la richiesta avvia immediatamente consultazioni di natura non vincolante con lo Stato membro richiedente, che dovranno terminare entro dieci giorni lavorativi. 4. Gli Stati membri comunicano alla Commissione l'elenco delle autorità competenti per il rilascio delle autorizzazioni di esportazione dei beni a duplice uso. 5. La Commissione pubblica l'elenco delle autorità di cui al paragrafo 4 nella *Gazzetta ufficiale delle Comunità europee*, serie C.
L'articolo 8 nota come ai fini del rilascio di un'autorizzazione d'esportazione le autorità competenti tengono conto delle linee direttrici di cui all'allegato III della decisione 94/942/PESC.
L'articolo 9 indica che 1.Gli esportatori mettono a disposizione delle autorità competenti tutte le informazioni richieste relative alla loro domanda d'autorizzazione d'esportazione. 2. Le autorità competenti di cui all'articolo 7, paragrafo 1 possono, applicando il presente regolamento, negare l'autorizzazione d'esportazione e annullare, sospendere, modificare o revocare un'autorizzazione da esse già rilasciata. In caso di diniego, annullamento, sospensione, limitazione sostanziale o revoca dell'autorizzazione, esse informano le autorità competenti degli altri Stati membri e, ove opportuno, scambiano le informazioni pertinenti con gli altri Stati membri e con la Commissione nel rispetto della riservatezza di tali informazioni, in conformità alle disposizioni di cui all'articolo 13, paragrafo 2.

5. Le procedure doganali.

Il titolo IV si occupa delle procedure doganali.

L'articolo 10 indica che 1. In occasione dell'espletamento delle formalità d'esportazione presso l'ufficio competente per l'accettazione della dichiarazione d'esportazione, l'esportatore deve fornire la prova che l'esportazione è stata debitamente autorizzata. 2. All'esportatore può essere richiesta una traduzione dei documenti prodotti nella lingua ufficiale o in una delle lingue ufficiali dello Stato membro nel quale la dichiarazione è stata presentata. 3. Fatte salve le competenze attribuitegli ai sensi del codice doganale comunitario, uno Stato membro può, inoltre, per un periodo complessivo non superiore a 10 giorni lavorativi, sospendere la procedura di svincolo ai fini della esportazione a partire dal proprio territorio o, se necessario, impedire in altro modo che i beni a duplice uso, di cui all'allegato I della decisione 94/942/PESC, e coperti da autorizzazione rilasciata in buona e debita forma lascino la Comunità attraverso il proprio territorio qualora abbia ragioni di sospettare: - che al momento del rilascio dell'autorizzazione non siano state prese in considerazione informazioni pertinenti; - che le circostanze sono sostanzialmente cambiate rispetto al momento del rilascio dell'autorizzazione. In tali casi le autorità competenti dello Stato membro che ha rilasciato l'autorizzazione di esportazione sono consultate immediatamente affinché possano adottare provvedimenti ai sensi dell'articolo 9, paragrafo 2. Se dette autorità decidono di mantenere l'autorizzazione o se non è pervenuta alcuna risposta entro i 10 giorni lavorativi di cui al primo comma, i beni sono liberati automaticamente, a meno che lo Stato membro che ha richiesto la consultazione non faccia ricorso alle disposizioni di cui al paragrafo 4. 4. In circostanze eccezionali, uno Stato membro, allorché ritiene che l'esportazione sia in contrasto con i propri interessi essenziali di politica estera e di sicurezza, o con l'assolvimento dei propri obblighi o impegni internazionali, può impedire che i beni a duplice uso lascino la Comunità attraverso il suo territorio anche se l'esportazione è stata debitamente autorizzata. Se uno Stato membro agisce ai sensi del presente paragrafo, i beni in questione sono messi a disposizione dell'esportatore. Le autorità competenti dello Stato membro che ha rilasciato l'autorizzazione sono debitamente informate.

L'articolo 11 dispone come 1. Gli Stati membri possono disporre che le formalità doganali d'esportazione di beni a duplice uso possano essere espletate esclusivamente presso determinati uffici doganali all'uopo abilitati. 2. Qualora ricorrano alla facoltà di cui al paragrafo 1 gli Stati membri comunicano alla Commissione l'elenco degli uffici doganali abilitati a tal fine. La Commissione pubblica tali informazioni nella *Gazzetta ufficiale delle Comunità europee,* serie C.

L'articolo 12 nota che quando i beni a duplice uso circolano all'interno della Comunità passando attraverso il territorio di un paese AELS, si applicano le disposizioni della parte II, titolo II, capitolo 11 delle disposizioni di applicazione del codice doganale comunitario e dell'articolo 22 dell'appendice I della Convenzione relativa a un regime di transito comune (6) stipulata il 20 maggio 1987 tra la Comunità e i paesi AELS.

6. La cooperazione amministrativa.

Il Titolo V riguarda invece la cooperazione amministrativa.
L'articolo 13 indica che 1. Gli Stati membri, di concerto con la Commissione, adottano tutte le disposizioni utili per istituire una cooperazione diretta e uno scambio di informazioni tra le autorità competenti, in particolare per evitare il rischio che eventuali disparità di applicazione dei controlli all'esportazione provochino deviazioni di traffico che possono creare difficoltà a uno o più Stati membri. 2. Si applicano, mutatis mutandis e fatto salvo l'articolo 16 del presente regolamento, le disposizioni del regolamento (CEE) n. 1468/81 del Consiglio, del 19 maggio 1981, relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione della regolamentazione doganale o agricola (7), e segnatamente quelle relative alla riservatezza delle informazioni.

7. Le misure di controllo.

Il TITOLO VI si occupa delle **Misure di controllo.**
L'articolo 14 indica che 1. Gli esportatori devono tenere registri commerciali o estratti dettagliati delle loro attività, secondo la prassi in vigore nello Stato membro rispettivo. Tali registri o estratti devono contenere in particolare i documenti commerciali, quali fatture, manifesti, documenti di trasporto o altri documenti di spedizione che contengono gli elementi necessari per determinare: - la designazione dei beni a duplice uso; - la quantità dei beni a duplice uso; - il nominativo e l'indirizzo dell'esportatore e del destinatario; - qualora siano conosciuti, l'utilizzazione finale e l'utilizzatore finale dei beni a duplice uso. 2. I registri o gli estratti e i documenti di cui al paragrafo 1 devono essere conservati per una durata di almeno tre anni a decorrere dalla fine dell'anno civile nel corso del quale ha luogo l'operazione di cui al paragrafo 1. Essi devono essere presentati su richiesta delle autorità competenti.
L'articolo 15 dispone che Per assicurare la corretta applicazione del presente regolamento ogni Stato membro adotta le misure necessarie per consentire alle autorità competenti: a) di raccogliere informazioni su qualsiasi ordine o operazione riguardante beni a duplice uso; b) di verificare la corretta applicazione dei controlli, segnatamente accedendo ai locali nei quali ha luogo l'attività professionale delle persone che effettuano un'operazione di esportazione.

8. Le disposizioni comuni e finali.

L' articolo 16 dispone che 1. E' istituito un gruppo di coordinamento composto da un rappresentante per ogni Stato membro e presieduto da un rappresentante della Commissione. 2. Il gruppo di coordinamento di cui al

paragrafo 1 è incaricato di esaminare: a) qualsiasi questione riguardante l'applicazione del presente regolamento che può essere sollevata dal presidente o dal rappresentante di uno Stato membro, e b) i provvedimenti che dovrebbero essere presi dagli Stati membri per informare gli esportatori degli obblighi imposti loro dal presente regolamento. 3. Il gruppo di coordinamento, ogniqualvolta lo ritenga necessario, può consultare le organizzazioni che rappresentano gli esportatori interessati dal presente regolamento.
L'articolo 17 indica come Ogni Stato membro adotta le misure appropriate per assicurare la piena applicazione di tutte le disposizioni del presente regolamento e in particolare determina le sanzioni da irrogare in caso di violazione delle norme del presente regolamento e di quelle adottate in esecuzione di quest'ultimo; le sanzioni devono essere effettive, proporzionate e dissuasive. In particolare, ai fini dell'applicazione dell'articolo 4, paragrafo 2, ogni Stato membro definisce e qualifica la natura dell'infrazione nel diritto nazionale e determina il tipo di sanzione da irrogare.
L'articolo 18 nota come ogni Stato membro informa la Commissione delle disposizioni legislative, regolamentari e amministrative da esso adottate in applicazione del presente regolamento e della decisione 94/942/PESC. La Commissione comunica tali informazioni agli Stati membri. Essa trasmette ogni due anni al Parlamento europeo e al Consiglio una relazione sull'applicazione del presente regolamento.
L'articolo 19 dispone che 1. Per un periodo transitorio, si applicano le seguenti disposizioni alle spedizioni di beni a duplice uso da uno Stato membro all'altro: a) per i beni a duplice uso compresi nell'elenco di cui all'allegato I della decisione 94/942/PESC, i relativi documenti commerciali devono indicare chiaramente che essi sono soggetti a controllo in caso di esportazione dalla Comunità; b) per i beni a duplice uso compresi nell'elenco di cui all'allegato IV della decisione 94/942/PESC, tutti gli Stati membri esigono delle autorizzazioni che non potranno in nessun caso essere delle autorizzazioni generali. 2.I documenti e i registri relativi alle spedizioni di beni a duplice uso il cui elenco è pubblicato nell'allegato I della decisione 94/942/PESC, devono essere conservati per almeno tre anni a decorrere dalla fine dell'anno civile nel quale l'operazione ha avuto luogo e devono essere presentati alle autorità competenti su richiesta. La persona fisica o giuridica che intraprende degli scambi intracomunitari di beni a duplice uso compresi nell'elenco di cui all'allegato I della decisione 94/942/PESC è tenuta a dichiarare alle autorità competenti, anteriormente o nel termine di trenta giorni dalla prima operazione di questo tipo, il suo nome e l'indirizzo presso il quale i documenti e i registri di cui sopra possono essere ispezionati. 3.a) Uno Stato membro può imporre un'autorizzazione per il trasferimento di un bene a duplice uso dal suo territorio verso un altro Stato membro se, al momento del trasferimento: - all'operatore consta che la destinazione finale del bene in questione si trova al di fuori della Comunità, e - l'esportazione dei beni detta destinazione è soggetta ad autorizzazione in forza degli articoli 3, 4 o 5 e - i beni non devono essere sottoposti a trasformazione o a lavorazione ai sensi dell'articolo 24 del Codice doganale comunitario nello Stato membro verso il quale vengono trasferiti. b) L'autorizzazione di trasferimento dev'essere richiesta nello Stato membro dal

quale è stato trasferito il bene a duplice uso. c) Lo Stato membro che adotta una tale regolamentazione informa immediatamente gli altri Stati membri e la Commissione delle disposizioni che ha adottato in conformità all'articolo 13. 4. Le disposizioni del presente articolo non comportano l'effettuazione di controlli alle frontiere interne della Comunità, ma unicamente dei controlli effettuati nell'ambito delle normali procedure di controllo applicate in modo non discriminatorio in tutto il territorio delle Comunità. 5. La necessità delle disposizioni previste dal presente articolo è riesaminata entro tre anni dalla dsata di entrata in vigore del presente regolamento. 6. L'applicazione delle disposizioni del presente articolo non può in ogni caso avere come conseguenza che le spedizioni da uno Stato membro ad un altro di un determinato bene siano subordinate a condizioni più restrittive di quelle imposte per le esportazioni dello stesso bene verso paesi terzi.
L'articolo 20 nota come 1. Per le spedizioni da uno Stato membro all'altro di beni a duplice uso elencati nell'allegato V della decisione 94/942/PESC, gli Stati membri come indicato nel suddetto allegato possono richiedere delle autorizzazioni specifiche (ivi comprese, se del caso, le condizioni riguardanti l'utilizzazione finale e/o la successiva cessione). 2. Le disposizioni di cui al paragrafo 1 non implicano l'effettuazione di controlli alle frontiere interne della Comunità ma unicamente controlli effettuati nell'ambito delle normali procedure di controllo applicate in modo non discriminatorio in tutto il territorio della Comunità.
L'articolo 21 dispone che 1. E' richiesta un'autorizzazione per il trasferimento intracomunitario di plutonio separato e di uranio arricchito oltre il 20 %, come pure di impianti e di componenti principali di fondamentale importanza nonché di tecnologie per il ritrattamento, l'arricchimento e la produzione di acqua pesante, ai sensi della dichiarazione di politica comune del 20 novembre 1984. 2. Le disposizioni di cui al paragrafo 1 non implicano l'effettuazione di controlli alle frontiere interne della Comunità, ma unicamente controlli effettuati nell'ambito delle normali procedure di controllo applicate in modo non discriminatorio in tutto il territorio della Comunità.
L'articolo 22 nota come il presente regolamento non pregiudica: - l'applicazione dell'articolo 223 del trattato che istituisce la Comunità europea; - l'applicazione del trattato che istituisce la Comunità europea dell'energia atomica.
L'articolo 23 dice che Il regolamento (CEE) n. 428/89 del Consiglio, del 20 febbraio 1989, relativo all'esportazione di taluni prodotti chimici (8) è abrogato.
L'articolo 24 Il presente regolamento entra in vigore il giorno della sua pubblicazione. Esso si applica dal 1° luglio 1995 Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri: Fatto a Bruxelles, addì 19 dicembre 1994.

Capitolo Nono

Il Regolamento n. 1334 del 2000

Sommario: 1. Le premesse. – 2. L'oggetto e le definizioni. – 3. L'ambito di applicazione. - 4. L'autorizzazione d'esportazione. – 5. L'aggiornamento dell'elenco dei prodotti a duplice uso. – 6. La cooperazione amministrativa. – 7. Le misure di controllo. - 8. Le disposizioni generali e finali.

REGOLAMENTO (CE) N. 1334/2000 DEL CONSIGLIO
del 22 giugno 2000
REGOLAMENTO (CE) N. 1334/2000 DEL CONSIGLIO
del 22 giugno 2000

che istituisce un regime comunitario
di controllo delle esportazioni di prodotti e tecnologie a duplice uso

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 133,

vista la proposta della Commissione 1 ,

1. Le premesse.

considerando quanto segue:

(1) I prodotti a duplice uso (inclusi il software e la tecnologia) dovrebbero essere sottoposti a controlli efficaci quando sono esportati dalla Comunità.

(2) E' necessario un efficace sistema comune di controllo delle esportazioni dei prodotti a duplice uso per assicurare il rispetto degli impegni e delle responsabilità internazionali degli Stati membri, in particolare in materia di non proliferazione, e dell'Unione europea.

(3) L'esistenza di un sistema comune di controllo e di politiche armonizzate di applicazione e controllo in tutti gli Stati membri rappresenta un presupposto indispensabile per la libera circolazione dei prodotti a duplice uso all'interno della Comunità.

(4) L'attuale regime di controllo delle esportazioni di prodotti a duplice uso fissato dal regolamento (CE) n. 3381/94 2 e dalla decisione 94/942/PESC 3 deve essere ulteriormente armonizzato al fine di continuare a garantire controlli efficaci.

(5) Elenchi comuni di prodotti a duplice uso, di destinazioni e di linee direttrici sono elementi essenziali per un sistema di controllo efficace delle esportazioni. Tali elenchi sono stati stabiliti dalla decisione 94/942/PESC e dalle successive modifiche e dovrebbero essere incorporati nel presente regolamento.

(6) La responsabilità delle decisioni in merito alle richieste di autorizzazioni di esportazione spetta alle autorità nazionali. Le disposizioni e le decisioni nazionali relative alle esportazioni di prodotti a duplice uso devono essere adottate nell'ambito della politica commerciale comune e, in particolare, del regolamento (CEE) n. 2603/69 del Consiglio, del 20 dicembre 1969, relativo all'instaurazione di un regime comune applicabile alle esportazioni 4.

(7) Le decisioni relative all'aggiornamento degli elenchi comuni di beni a duplice uso devono essere pienamente conformi agli obblighi e agli impegni che ciascuno Stato membro ha assunto in quanto membro dei pertinenti regimi internazionali di non proliferazione e degli accordi in materia di controllo delle esportazioni, oppure a seguito della ratifica di pertinenti trattati internazionali.

(8) Anche la trasmissione di software e di tecnologie mediante mezzi elettronici, fax o telefono verso destinazioni al di fuori della Comunità dovrebbe essere sottoposta a controllo.

(9) Occorre prestare particolare attenzione alle questioni relative alla riesportazione e all'utilizzazione finale.

(10) Il 22 settembre 1998 i rappresentanti degli Stati membri e della Commissione europea hanno firmato protocolli aggiuntivi dei rispettivi accordi di salvaguardia conclusi tra gli Stati membri, la Comunità europea dell'energia atomica e l'Agenzia internazionale per l'energia atomica, che, tra altre misure, obbligano gli Stati membri a fornire informazioni sulle attrezzature e sulle materie non nucleari specificate.

(11) La Comunità ha istituito un complesso organico di norme doganali contenute nel regolamento (CEE) n. 2913/92 del Consiglio, del 12 ottobre 1992, che istituisce un codice doganale comunitario 5, e nel regolamento (CEE) n. 2454/93 6 della Commissione, che attua il regolamento (CEE) n. 2913/92, i quali stabiliscono, tra l'altro, le disposizioni relative all'esportazione e riesportazione di beni. Il presente regolamento non pone alcuna restrizione ai poteri attribuiti dal codice doganale comunitario e dalle relative disposizioni d'applicazione da questi ultimi derivanti.

(12) A norma ed entro i limiti dell'articolo 30 del trattato e in attesa di un maggiore grado di armonizzazione, gli Stati membri manterranno il diritto di effettuare controlli sui trasferimenti di determinati prodotti a duplice uso all'interno della Comunità europea al fine di salvaguardare l'ordine pubblico o la pubblica sicurezza. Tali controlli, essendo correlati all'efficacia dei controlli sulle esportazioni dalla Comunità, saranno periodicamente riesaminati dal Consiglio.

(13) Per garantire la corretta applicazione del presente regolamento, ciascuno Stato membro dovrebbe adottare provvedimenti intesi a conferire adeguati poteri alle autorità competenti.

(14) Ciascuno Stato membro dovrebbe stabilire le sanzioni da applicare in caso di violazione delle disposizioni del presente regolamento.

(15) Nella risoluzione del 13 aprile 1999 7 il Parlamento europeo ha espresso i suoi pareri.

(16) Il regolamento (CE) n. 3381/94 dovrebbe conseguentemente essere abrogato,

2. L'oggetto e le definizioni.

HA ADOTTATO IL PRESENTE REGOLAMENTO:

CAPO I

Oggetto e definizioni

Articolo 1

Il presente regolamento istituisce un regime comunitario di controllo delle esportazioni dei prodotti a duplice uso.

Articolo 2

Ai fini del presente regolamento:

a) "prodotti a duplice uso" sono i prodotti, inclusi il software e le tecnologie, che possono avere un utilizzo sia civile sia militare; essi comprendono tutti i beni che possono avere sia un utilizzo non esplosivo sia un qualche impiego nella fabbricazione di armi nucleari o di altri congegni esplosivi nucleari;

b) "esportazione" è:

un regime di esportazione ai sensi dell'articolo 161 del codice doganale comunitario;

una riesportazione, ai sensi dell'articolo 182 di detto codice, e

la trasmissione di software o di tecnologie mediante mezzi elettronici, fax o telefono verso una destinazione al di fuori della Comunità; ciò si applica alla trasmissione orale di tecnologia tramite telefono solo quando tale tecnologia è contenuta in un documento, di cui una parte pertinente è letta o è descritta al telefono in modo tale da conseguire un risultato sostanzialmente analogo;

c) "esportatore" è qualsiasi persona fisica o giuridica per conto della quale è resa una dichiarazione d'esportazione, vale a dire la persona che sia titolare del contratto concluso con il destinatario nel paese terzo e abbia la facoltà di decidere l'invio di prodotti al di fuori del territorio doganale della Comunità al momento dell'accettazione della dichiarazione. Qualora non sia stato concluso alcun contratto o il titolare del contratto non agisca per proprio conto è determinante la facoltà di decidere l'invio dei prodotti al di fuori del territorio doganale della Comunità.

Per "esportatore" si intende altresì qualsiasi persona fisica o giuridica che decida di trasmettere software o tecnologie mediante mezzi elettronici, fax o telefono verso una destinazione al di fuori della Comunità.

Qualora, ai sensi del contratto in base al quale è effettuata l'esportazione, titolare del diritto di disporre del prodotto a duplice uso risulti essere una persona non stabilita nella Comunità, la qualità di esportatore è assunta dal contraente stabilito nella Comunità;

d) "dichiarazione d'esportazione" è l'atto con il quale una persona manifesta, nelle forme e secondo le modalità prescritte, la volontà di sottoporre un prodotto a duplice uso al regime di esportazione.

3. L'ambito di applicazione.

CAPO II

Ambito di applicazione

Articolo 3

1. L'esportazione dei prodotti a duplice uso compresi nell'elenco di cui all'allegato I è subordinata ad autorizzazione.

2. Può essere subordinata ad autorizzazione, a norma degli articoli 4 o 5, anche l'esportazione verso tutte o talune destinazioni di determinati prodotti a duplice uso non compresi nell'elenco di cui all'allegato I.

3. Il presente regolamento non si applica alla fornitura di servizi o alla trasmissione di tecnologie qualora esse comportino un movimento transfrontaliero di persone fisiche.

4. Il presente regolamento non si applica ai prodotti a duplice uso che attraversano solamente il territorio della Comunità, vale a dire quelli che non sono sottoposti ad altro regime o controllo doganale oltre a quello del transito esterno, oppure che sono semplicemente introdotti in una zona franca o in un deposito franco e non devono essere iscritti in una contabilità di magazzino approvata.

Articolo 4

1. L'esportazione di prodotti a duplice uso non compresi nell'elenco di cui all'allegato I è subordinata alla presentazione di un'autorizzazione d'esportazione nel caso in cui l'esportatore sia stato informato dalle competenti autorità dello Stato membro in cui è stabilito che detti prodotti sono o possono essere destinati, in tutto o in parte, ad una utilizzazione collegata allo sviluppo, alla produzione, alla movimentazione, al funzionamento, alla manutenzione, alla conservazione, all'individuazione, all'identificazione o alla disseminazione di armi chimiche, biologiche o nucleari o di altri congegni esplosivi nucleari oppure allo sviluppo, alla produzione, alla manutenzione o alla conservazione di missili che possano essere utilizzati come vettori di tali armi.

2. L'esportazione di prodotti a duplice uso non compresi nell'elenco di cui all'allegato I è subordinata alla presentazione di un'autorizzazione d'esportazione anche nel caso in cui il paese acquirente o il paese di destinazione siano soggetti ad un embargo sugli armamenti deciso con una posizione comune o un'azione comune adottata dal Consiglio o con una decisione dell'OSCE o ad un embargo sugli armamenti imposto da una risoluzione vincolante del Consiglio di sicurezza delle Nazioni Unite, e qualora l'esportatore sia stato informato dalle autorità di cui al paragrafo 1 che detti prodotti sono o possono essere destinati, in tutto o in parte, a scopi militari. Ai fini del presente paragrafo per "scopi militari" si intende:

a) l'inserimento in prodotti militari figuranti nell'elenco dei materiali di armamento degli Stati membri;

b) l'utilizzazione di apparecchiature di produzione, controllo o analisi e loro componenti ai fini dello sviluppo, della produzione o della manutenzione dei prodotti militari figuranti nell'elenco summenzionato;

c) l'utilizzazione di eventuali prodotti non finiti in un impianto per la produzione di prodotti militari figuranti nell'elenco summenzionato.

3. L'esportazione di prodotti a duplice uso non compresi nell'elenco di cui all'allegato I è subordinata alla presentazione di un'autorizzazione d'esportazione anche nel caso in cui l'esportatore sia stato informato dalle competenti autorità di cui al paragrafo 1 che detti prodotti sono o possono essere destinati, in tutto o in parte, ad essere utilizzati come parti o componenti di prodotti militari figuranti nell'elenco dei materiali di armamento nazionale che sono stati esportati dal territorio dello Stato membro in questione senza autorizzazione o in violazione dell'autorizzazione prevista dalla legislazione nazionale dello stesso Stato membro.

4. Un esportatore, se ha conoscenza che i prodotti a duplice uso che intende esportare e che non sono compresi nell'elenco di cui all'allegato I sono destinati, in tutto o in parte, ad una qualsiasi delle utilizzazioni di cui ai paragrafi 1, 2 e 3, deve informarne le autorità di cui al paragrafo 1, che decideranno in merito all'opportunità di sottoporre la suddetta esportazione ad autorizzazione.

5. Uno Stato membro può adottare o mantenere le disposizioni nazionali che subordinano ad autorizzazione l'esportazione di prodotti a duplice uso non compresi nell'elenco di cui all'allegato I qualora l'esportatore abbia motivo di sospettare che i prodotti in questione siano o possano essere destinati, in tutto o in parte, ad uno degli usi di cui al paragrafo 1.

6. Uno Stato membro che, in applicazione delle disposizioni di cui ai paragrafi da 1 a 5, subordina ad autorizzazione l'esportazione di un prodotto a duplice uso non compreso nell'elenco di cui all'allegato I, ne informa, se del caso, gli altri Stati membri e la Commissione. Gli altri Stati membri tengono nella dovuta considerazione tali informazioni e le trasmettono, per quanto possibile, ai loro uffici doganali e alle altre autorità nazionali competenti.

7. Le disposizioni di cui all'articolo 9, paragrafi 2 e 3 si applicano ai casi relativi ai prodotti a duplice uso non compresi nell'elenco di cui all'allegato I.

8. Il presente regolamento lascia impregiudicato il diritto degli Stati membri di adottare misure nazionali ai sensi dell'articolo 11 del regolamento (CEE) n. 2603/69.

Articolo 5

1. Per motivi di sicurezza pubblica o di rispetto dei diritti dell'uomo, uno Stato membro può vietare l'esportazione di prodotti a duplice uso non

compresi nell'elenco di cui all'allegato I o imporre per gli stessi un requisito di autorizzazione.

2. Gli Stati membri notificano alla Commissione le misure adottate ai sensi del paragrafo 1, immediatamente dopo la loro adozione, indicandone con precisione i motivi.

3. Gli Stati membri notificano inoltre immediatamente alla Commissione ogni modifica riguardante le misure adottate ai sensi del paragrafo 1.

4. La Commissione pubblica nella Gazzetta ufficiale delle Comunità europee, serie C, le misure che le sono notificate ai sensi dei paragrafi 2 e 3.

4. L'autorizzazione d'esportazione.

CAPO III

Autorizzazione d'esportazione

Articolo 6

1. Il presente regolamento istituisce un'autorizzazione generale di esportazione della Comunità per talune esportazioni, come indicato nell'allegato II.

2. Per tutte le altre operazioni di esportazione per cui è richiesta un'autorizzazione ai sensi del presente regolamento, tale autorizzazione è concessa dalle autorità competenti dello Stato membro in cui è stabilito l'esportatore. Fatta salva la restrizione di cui al paragrafo 3, questa autorizzazione può essere specifica, globale o generale.

L'autorizzazione ha validità su tutto il territorio della Comunità.

Se del caso, l'autorizzazione può essere subordinata a determinati requisiti e condizioni quale ad esempio l'obbligo di fornire una dichiarazione relativa all'utilizzazione finale.

3. I prodotti di cui alla parte 2 dell'allegato II non sono inclusi in un'autorizzazione generale.

4. Gli Stati membri indicano nelle autorizzazioni generali che queste ultime non possono essere utilizzate qualora l'esportatore sia stato informato dalle sue autorità del fatto che detti prodotti sono o possono essere destinati, in tutto o in parte, ad una qualsiasi delle utilizzazioni di cui all'articolo 4, paragrafi 1, 2 e 3 o qualora l'esportatore sia a conoscenza del fatto che detti prodotti sono destinati alle utilizzazioni summenzionate.

5. Gli Stati membri mantengono o introducono nelle loro rispettive legislazioni nazionali la possibilità di concedere un'autorizzazione globale a un esportatore specifico per un tipo o una categoria di prodotti a duplice uso, che può essere valida per le esportazioni verso uno o più paesi specifici.

6. Gli Stati membri forniscono alla Commissione l'elenco delle autorità abilitate al rilascio delle autorizzazioni d'esportazione di prodotti a duplice uso.

Nella Gazzetta ufficiale delle Comunità europee, serie C, la Commissione pubblica l'elenco di tali autorità.

Articolo 7

1. Se i prodotti a duplice uso, per i quali è stata chiesta un'autorizzazione di esportazione specifica verso una destinazione che non figura nell'allegato II o verso tutte le destinazioni, nel caso dei prodotti a duplice uso che figurano nell'allegato IV, si trovano o si troveranno in uno o più Stati membri diversi da quello nel quale è stata presentata la richiesta, tale circostanza deve essere indicata nella richiesta. Le autorità competenti dello Stato membro al quale l'autorizzazione viene richiesta consultano immediatamente le corrispondenti autorità competenti dello Stato membro o degli Stati membri in questione e forniscono loro le informazioni pertinenti. Lo Stato membro o gli Stati membri consultati comunicano, entro dieci giorni lavorativi, le loro eventuali obiezioni nei confronti del rilascio dell'autorizzazione. La comunicazione di obiezioni vincola lo Stato membro cui è stata fatta la richiesta.

Se non pervengono obiezioni entro dieci giorni lavorativi, si considera che lo Stato membro consultato o gli Stati membri consultati non hanno obiezioni.
In casi eccezionali, qualsiasi Stato membro consultato può chiedere la proroga del termine di dieci giorni. Tuttavia questa proroga non può superare i trenta giorni lavorativi.

2. Qualora un'esportazione possa recare pregiudizio a interessi vitali in materia di sicurezza di uno Stato membro, questo può chiedere ad un altro Stato membro di non concedere l'autorizzazione di esportazione, oppure, qualora siffatta autorizzazione sia stata concessa, chiederne l'annullamento, la sospensione, la modifica o la revoca. Lo Stato membro che ha ricevuto la richiesta avvia immediatamente consultazioni di natura non vincolante con lo Stato membro richiedente, che dovranno terminare entro dieci giorni lavorativi.

Articolo 8

Ai fini del rilascio di un'autorizzazione d'esportazione ai sensi del presente regolamento gli Stati membri tengono conto di tutti i fattori pertinenti, tra cui:

a) gli obblighi e gli impegni che ciascuno di loro ha assunto in qualità di membro dei pertinenti regimi internazionali di non proliferazione e di accordi per il controllo delle esportazioni o con la ratifica dei pertinenti trattati internazionali;

b) gli obblighi derivanti dalle sanzioni imposte con una posizione comune o un'azione comune adottata dal Consiglio o con una decisione dell'OSCE o con una risoluzione vincolante del Consiglio di sicurezza delle Nazioni Unite;

c) considerazioni di politica estera e di sicurezza nazionale, comprese quelle cui si applica il codice di condotta dell'Unione europea per l'esportazione di armi;

d) considerazioni sulla prevista utilizzazione finale e sul rischio di sviamenti di destinazione.

Articolo 9

1. Gli esportatori mettono a disposizione delle autorità competenti tutte le informazioni pertinenti necessarie relativamente alla loro domanda d'autorizzazione di esportazione.

2. Le autorità competenti possono, ai sensi del presente regolamento, negare l'autorizzazione d'esportazione e annullare, sospendere, modificare o revocare un'autorizzazione da esse già rilasciata. In caso di rifiuto, annullamento, sospensione, limitazione sostanziale o revoca dell'autorizzazione, esse ne informano le autorità competenti degli altri Stati membri e la Commissione e comunicano le informazioni pertinenti agli altri Stati membri e alla Commissione, nel rispetto delle disposizioni di cui all'articolo 15, paragrafo 3, in materia di riservatezza delle informazioni.

3. Prima che qualsiasi Stato membro rilasci un'autorizzazione di esportazione che è stata negata da un altro Stato membro o da altri Stati membri per una transazione essenzialmente identica nei tre anni precedenti, esso deve prima consultare lo Stato membro o gli Stati membri che avevano rifiutato l'autorizzazione. Se a seguito delle consultazioni lo Stato membro decide di rilasciare comunque l'autorizzazione, esso ne informa gli altri Stati membri e la Commissione, fornendo tutte le informazioni pertinenti per giustificare la sua decisione.

Articolo 10

1. Tutte le autorizzazioni d'esportazione specifiche e globali sono rilasciate per mezzo di formulari conformi al modello di cui all'allegato III bis.

2. A richiesta degli esportatori, le autorizzazioni d'esportazione globali che contengono limitazioni quantitative possono essere suddivise.

3. Le autorizzazioni d'esportazione generali concesse ai sensi dell'articolo 6, paragrafo 2 sono pubblicate conformemente alle leggi e alle prassi nazionali. Esse vengono rilasciate agli esportatori conformemente alle indicazioni di cui all'allegato III ter.

5. L'aggiornamento dell'elenco dei prodotti a duplice uso.

CAPO IV

Aggiornamento dell'elenco dei prodotti a duplice uso

Articolo 11

Gli elenchi di prodotti a duplice uso di cui all'allegato I e all'allegato IV sono aggiornati conformemente ai pertinenti obblighi e impegni, e relative modifiche, accettati da ciascuno Stato membro in qualità di membro di regimi internazionali di non proliferazione e di accordi in materia di controllo delle esportazioni o a seguito della ratifica di pertinenti trattati internazionali.

CAPO V

Procedure doganali

Articolo 12

1. In occasione dell'espletamento delle formalità per l'esportazione di prodotti a duplice uso presso l'ufficio doganale competente per l'accettazione della dichiarazione d'esportazione, l'esportatore deve fornire la prova che tutte le autorizzazioni di esportazione necessarie sono state ottenute.

2. All'esportatore può essere richiesta una traduzione dei documenti prodotti in una lingua ufficiale dello Stato membro nel quale la dichiarazione di esportazione è presentata.

3. Fatte salve le competenze attribuitegli ai sensi del codice doganale comunitario, uno Stato membro può altresì, per un periodo non superiore ai periodi di cui al paragrafo 4, sospendere la procedura di esportazione dal proprio territorio o, se necessario, impedire in altro modo che i prodotti a

duplice uso di cui all'allegato I e coperti da valida autorizzazione d'esportazione lascino la Comunità attraverso il proprio territorio qualora abbia ragioni di sospettare:

a) che al momento del rilascio dell'autorizzazione non siano state prese in considerazione informazioni pertinenti;

b) che le circostanze siano sostanzialmente cambiate rispetto al momento del rilascio dell'autorizzazione.

4. Nel caso di cui al precedente paragrafo 3, le autorità competenti dello Stato membro che ha rilasciato l'autorizzazione d'esportazione sono consultate immediatamente affinché possano adottare provvedimenti ai sensi dell'articolo 9, paragrafo 2. Se dette autorità competenti decidono di mantenere l'autorizzazione, esse devono rispondere entro un termine di dieci giorni lavorativi che, su loro richiesta, può essere esteso a trenta giorni lavorativi in circostanze eccezionali. In tal caso, o se non è pervenuta alcuna risposta entro dieci o trenta giorni lavorativi a seconda delle circostanze, i prodotti a duplice uso sono liberati immediatamente. Lo Stato membro che ha rilasciato l'autorizzazione informa gli altri Stati membri e la Commissione.

Articolo 13

1. Gli Stati membri possono disporre che le formalità doganali d'esportazione dei prodotti a duplice uso possano essere espletate esclusivamente presso determinati uffici doganali all'uopo abilitati.

2. Qualora si avvalgano della facoltà di cui al paragrafo 1, gli Stati membri comunicano alla Commissione l'elenco degli uffici doganali debitamente abilitati. La Commissione pubblica tali informazioni nella Gazzetta ufficiale delle Comunità europee, serie C.

Articolo 14

Le disposizioni degli articoli da 463 a 470 e dell'articolo 843 del regolamento (CEE) n. 2454/93 si applicano anche alle restrizioni relative all'esportazione, alla riesportazione e all'uscita dal territorio doganale dei prodotti a duplice uso per la cui esportazione è necessaria un'autorizzazione ai sensi del presente regolamento.

6. La cooperazione amministrativa.

CAPO VI

Cooperazione amministrativa

Articolo 15

1. Gli Stati membri, di concerto con la Commissione, adottano tutte le disposizioni atte ad istituire una cooperazione diretta e lo scambio di informazioni tra le autorità competenti, in particolare per eliminare il rischio che eventuali difformità di applicazione dei controlli all'esportazione effettuati su prodotti a duplice uso inducano deviazioni di traffico che potrebbero creare difficoltà ad uno o più Stati membri.

2. Gli Stati membri adottano tutte le disposizioni necessarie per istituire una cooperazione diretta e lo scambio di informazioni tra le autorità competenti sugli utilizzatori finali sensibili, al fine di fornire agli esportatori interessati dal presente regolamento un livello di assistenza omogeneo.

3. Fatto salvo l'articolo 18 del presente regolamento, si applicano, con gli eventuali adattamenti, le disposizioni del regolamento (CE) n. 515/97 del Consiglio, del 13 marzo 1997, relativo alla mutua assistenza tra le autorità amministrative degli Stati membri e alla collaborazione tra queste e la Commissione per assicurare la corretta applicazione delle normative doganale e agricola 8 , in particolare quelle relative alla riservatezza delle informazioni.

7. Le misure di controllo.

CAPO VII

Misure di controllo

Articolo 16

1. Gli esportatori tengono dettagliati registri commerciali o documentazione dettagliata delle loro esportazioni secondo la prassi in vigore nel rispettivo Stato membro. Tali registri o documentazione comprendono in particolare i documenti commerciali, quali fatture, manifesti, documenti di trasporto o altri documenti di spedizione che contengono informazioni sufficienti per determinare:

a) la descrizione dei prodotti a duplice uso;

b) la quantità dei prodotti a duplice uso;

c) il nominativo e l'indirizzo dell'esportatore e del destinatario,

d) qualora siano conosciuti, l'utilizzazione finale e l'utilizzatore finale dei prodotti a duplice uso.

2. I registri o la documentazione di cui al paragrafo 1 sono conservati per una durata di almeno tre anni a decorrere dalla fine dell'anno civile nel corso del quale ha luogo l'esportazione. Essi sono presentati alle autorità competenti dello Stato in cui è stabilito l'esportatore quando ne facciano richiesta.

Articolo 17

Per assicurare la corretta applicazione del presente regolamento ciascuno Stato membro adotta tutte le misure necessarie per consentire alle proprie autorità competenti:

a) di raccogliere informazioni su qualsiasi commessa o operazione riguardante prodotti a duplice uso;

b) di verificare la corretta applicazione delle misure di controllo all'esportazione, che possono consistere in particolare nel potere di ispezionare i locali nei quali le persone interessate a un'operazione di esportazione svolgono la propria attività.

8. Le disposizioni generali e finali.

CAPO VIII

Disposizioni generali e finali

Articolo 18

1. È istituito un gruppo di coordinamento presieduto da un rappresentante della Commissione e composto di un rappresentante di ciascuno Stato membro.

Il gruppo di coordinamento esamina tutte le questioni riguardanti l'applicazione del presente regolamento, sollevate dal presidente o dal rappresentante di uno Stato membro e, tra l'altro:

a) i provvedimenti che dovrebbero essere adottati dagli Stati membri per informare gli esportatori degli obblighi loro imposti dal presente regolamento;

b) gli orientamenti in materia di formulari di autorizzazioni d'esportazione.

2. Il gruppo di coordinamento, ogniqualvolta lo ritenga necessario, può consultare le organizzazioni che rappresentano gli esportatori interessati dal presente regolamento.

Articolo 19

Gli Stati membri adottano i provvedimenti adeguati per assicurare la corretta applicazione di tutte le disposizioni del presente regolamento e, in particolare, determinano le sanzioni da irrogare in caso di violazione delle norme del presente regolamento e delle relative disposizioni di applicazione. Le sanzioni devono essere effettive, proporzionate e dissuasive.

Articolo 20

Gli Stati membri informano la Commissione delle disposizioni legislative, regolamentari e amministrative da essi adottate in applicazione del presente regolamento, comprese le misure di cui all'articolo 19. La Commissione comunica tali informazioni agli altri Stati membri. Essa trasmette ogni tre anni al Parlamento europeo e al Consiglio una relazione sull'applicazione del presente regolamento. Gli Stati membri forniscono alla Commissione tutte le informazioni necessarie per preparare tale relazione.

Articolo 21

1. Per il trasferimento all'interno della Comunità dei prodotti a duplice uso di cui all'allegato IV è richiesta un'autorizzazione. Per i prodotti di cui all'allegato IV, parte 2 l'autorizzazione non può essere un'autorizzazione generale.

2. a) Uno Stato membro può imporre un'autorizzazione per il trasferimento di altri prodotti a duplice uso dal suo territorio verso un altro Stato membro se, al momento del trasferimento:

- all'operatore consta che la destinazione finale dei prodotti in questione si trova al di fuori della Comunità;

- l'esportazione dei prodotti verso detta destinazione finale è soggetta ad autorizzazione nello Stato membro dal quale i beni devono essere trasferiti, a norma degli articoli 3, 4 o 5 e tale esportazione direttamente dal suo territorio non è consentita da un'autorizzazione generale o globale;

- i beni non devono essere sottoposti a processi o a lavorazioni di cui all'articolo 24 del codice doganale comunitario nello Stato membro verso il quale devono essere trasferiti.

b) L'autorizzazione di trasferimento deve essere richiesta nello Stato membro da cui devono essere trasferiti i prodotti a duplice uso.

c) Nei casi in cui la successiva esportazione dei prodotti a duplice uso sia già stata accettata dallo Stato membro dal quale i prodotti vengono trasferiti, nell'ambito delle procedure di consultazione di cui all'articolo 7, viene immediatamente rilasciata all'operatore l'autorizzazione di trasferimento, a meno che le circostanze non siano cambiate significativamente.

d) Gli Stati membri che impongono tale requisito informano la Commissione e gli altri Stati membri delle misure adottate. La Commissione pubblica tali informazioni nella Gazzetta ufficiale delle Comunità europee, serie C.

3. Le disposizioni adottate ai sensi dei paragrafi 1 e 2 non implicano alcun controllo alle frontiere interne della Comunità, ma unicamente controlli effettuati nell'ambito delle normali procedure di controllo applicate in modo non discriminatorio in tutto il territorio della Comunità.

4. L'applicazione delle misure adottate ai sensi dei paragrafi 1 e 2 non può in nessun caso avere come conseguenza che i trasferimenti da uno Stato membro ad un altro di un determinato prodotto siano subordinati a condizioni più restrittive di quelle imposte per le esportazioni dello stesso prodotto verso paesi terzi.

5. La documentazione e i registri relativi ai trasferimenti intracomunitari di prodotti a duplice uso elencati nell'allegato I sono conservati per almeno tre anni a decorrere dalla fine dell'anno civile nel quale il trasferimento ha avuto luogo e sono presentati alle autorità competenti dello Stato membro da cui i prodotti sono stati trasferiti su loro richiesta.

6. Uno Stato membro può prescrivere nella legislazione nazionale che per i trasferimenti intracomunitari da detto Stato membro di prodotti elencati nell'allegato I, categoria 5, parte 2 e che non sono elencati nell'allegato IV debbano essere fornite alle autorità competenti dello Stato stesso informazioni supplementari concernenti i prodotti in questione.

7. I documenti commerciali pertinenti relativi a trasferimenti all'interno della Comunità dei prodotti a duplice uso elencati nell'allegato I indicano chiaramente che i prodotti in questione sono soggetti a controllo se esportati dalla Comunità. Tra i documenti commerciali pertinenti figurano in particolare eventuali contratti di vendita, conferme dell'ordine, fatture ed avvisi di spedizione.

Articolo 22

Il presente regolamento non pregiudica:

l'applicazione dell'articolo 296 del trattato che istituisce la Comunità europea;

l'applicazione del trattato che istituisce la Comunità europea dell'energia atomica.

Articolo 23

Il regolamento (CE) n. 3381/94 è abrogato.

Tuttavia, per quanto riguarda le richieste di autorizzazione d'esportazione formulate prima dell'entrata in vigore del presente regolamento, si continuano ad applicare le disposizioni di cui al regolamento (CE) n. 3381/94.

Articolo 24

Il presente regolamento entra in vigore novanta giorni dopo la data di pubblicazione nella Gazzetta ufficiale delle Comunità europee.

Fatto a Lussemburgo, addì 22 giugno 2000

Per il Consiglio

Il Presidente

J Sòcrates

Capitolo Decimo

La legge 9 luglio 1990, n. 185

Sommario: 1. Le disposizioni generali. – 2. Gli organismi di coordinamento e di controllo. – 3. L'autorizzazione alle trattative. – 4. L'autorizzazione all'importazione, esportazione e transito. – 5. Gli obblighi delle imprese. – 6. Le sanzioni. – 7. Le disposizioni finali e transitorie.

LEGGE 185/'90 (Con modifiche approttate dal DDL 1927 approvato alla Camera)
Legge 9 luglio 1990, n. 185 (in Gazz. Uff., 14 luglio 1990, n. 163).
Nuove norme sul controllo dell'esportazione, importazione e
transito dei materiali di armamento (1) (2) (3).

In Rosso: le modifiche dal DDL 1927
In Verde: le modifiche da Emendamenti Governativi al DDL 1927
In Blu: le modifiche da Emendamenti proposti dall'Opposizione e accolti nel DDL 1927

(1) Vedi il d.p.c.m. 23 febbraio 1991, n. 94 di attuazione.
(2) Allo scopo di agevolarne la lettura, nel presente provvedimento la nomenclatura dei Ministri e dei Ministeri è stata aggiornata sulla base degli accorpamenti e delle soppressioni intervenute negli ultimi anni.
(3) A partire dal 1 gennaio 1999 ogni sanzione pecuniaria penale o amministrativa espressa in lire nel presente provvedimento si intende espressa anche in Euro secondo il tasso di conversione irrevocabilmente fissato ai sensi del Trattato CE. A decorrere dal 1 gennaio 2002 ogni sanzione penale o amministrativa espressa in lire nel presente provvedimento è tradotta in Euro secondo il tasso di conversione irrevocabilmente fissato ai sensi del Trattato CE. Se tale operazione di conversione produce un risultato espresso anche in decimali, la cifra è arrotondata eliminando i decimali (art. 51, d.lg. 24 giugno 1998, n. 213). Aggiornato alla G.U. del 14/06/1999, n. 137

1. Le disposizioni generali.

Capo I: DISPOSIZIONI GENERALI

Art. 1. Controllo dello Stato.

1. L'esportazione, l'importazione e il transito di materiale di armamento nonché la cessione delle relative licenze di produzione

devono essere conformi alla politica estera e di difesa dell'Italia. Tali operazioni vengono regolamentate dallo Stato secondo i princìpi
della Costituzione repubblicana che ripudia la guerra come mezzo di risoluzione delle controversie internazionali.

2. L'esportazione, l'importazione e il transito dei materiali di armamento, di cui all'articolo 2, nonché la cessione delle relative
licenze di produzione, sono soggetti ad autorizzazioni e controlli dello Stato.

3. Il Governo predispone misure idonee ad assecondare la graduale differenziazione produttiva e la conversione a fini civili delleindustrie nel settore della difesa.

4. Le operazioni di esportazione e transito sono consentite solo se effettuate con governi esteri o con imprese autorizzate dal governo del paese destinatario.

5. L'esportazione ed il transito di materiali di armamento, nonché la cessione delle relative licenze di produzione, sono vietati quando siano in contrasto con la Costituzione, con gli impegni internazionali dell'Italia e con i fondamentali interessi della sicurezza dello Stato, della lotta contro il terrorismo e del mantenimento di buone relazioni con altri Paesi, nonché quando manchino adeguate garanzie sulla definitiva destinazione dei materiali.

6. L'esportazione ed il transito di materiali di armamento sono altresì vietati:
a) verso i Paesi in stato di conflitto armato, in contrasto con i princìpi dell'articolo 51 della Carta delle Nazioni Unite, fatto salvo il rispetto degli obblighi internazionali dell'Italia o le diverse deliberazioni del Consiglio dei ministri, da adottare previo parere delle Camere;
b) verso Paesi la cui politica contrasti con i princìpi dell'articolo 11 della Costituzione;
c) verso i Paesi nei cui confronti sia stato dichiarato l'embargo totale o parziale delle forniture belliche da parte delle Nazioni Unite o dell'Unione europea (UE); (dal DDL art.3) d) verso i Paesi i cui governi sono responsabili di accertate violazioni delle convenzioni internazionali in materia di diritti dell'uomo; DIVENTA:
"d) verso i Paesi i cui governi sono responsabili di gravi violazioni delle convenzioni internazionali in materia di diritti umani, accertate dai competenti organi delle Nazioni Unite, dell'UE o del Consiglio d'Europa;" (dal DDL art.3)
e) verso i Paesi che, ricevendo dall'Italia aiuti ai sensi della legge 26 febbraio 1987, n. 49, destinino al proprio bilancio militare risorse eccedenti le esigenze di difesa del paese; verso tali Paesi è sospesa la erogazione di aiuti ai sensi della stessa legge, ad eccezione degli aiuti alle popolazioni nei casi di disastri e calamità naturali.

7. Sono vietate la fabbricazione, l'importazione, l'esportazione ed il transito di armi biologiche, chimiche e nucleari, nonché la ricerca preordinata alla loro produzione o la cessione della relativa tecnologia. Il divieto si applica anche agli

strumenti e alle tecnologie specificamente progettate per la costruzione delle suddette armi nonché a quelle idonee alla manipolazione dell'uomo e della biosfera a fini militari.

8. Le importazioni definitive o temporanee di materiale di armamento sono vietate, ad eccezione:
a) delle importazioni effettuate direttamente dall'Amministrazione dello Stato o per conto di questa per la realizzazione dei programmi di armamento ed equipaggiamento delle forze armate e di polizia, che possono essere consentite direttamente dalle dogane;
b) delle importazioni effettuate da soggetti iscritti al registro nazionale delle imprese di cui all'articolo 3, previa autorizzazione di cui all'articolo 13;
c) delle importazioni temporanee, effettuate da soggetti iscritti al registro nazionale delle imprese di cui all'articolo 3, per la revisione dei materiali d'armamento in precedenza esportati;
d) delle importazioni effettuate dagli enti pubblici, nell'ambito delle rispettive competenze, in relazione all'esercizio di attività di carattere storico o culturale, previe le autorizzazioni di polizia previste dall'articolo 8 della legge 18 aprile 1975, n. 110;
e) delle importazioni temporanee effettuate da imprese straniere per la partecipazione a fiere campionarie, mostre ed attività dimostrative, previa autorizzazione del Ministero dell'interno rilasciata a seguito di nulla osta del Ministero della difesa.

9. Sono escluse dalla disciplina della presente legge:
a) le esportazioni temporanee effettuate direttamente o per conto dell'Amministrazione dello Stato per la realizzazione di propri programmi di armamento ed equipaggiamento delle forze armate e di polizia;
b) le esportazioni o concessioni dirette da Stato a Stato,, a fini di assistenza militare, in base ad accordi internazionali;
c) il transito di materiali di armamento e di equipaggiamento per i bisogni di forze dei Paesi alleati, secondo la definizione della Convenzione sullo statuto delle Forze della NATO, purché non siano invocate a qualsiasi titolo deroghe agli articoli VI, XI, XII, XIII e XIV della Convenzione tra gli Stati partecipanti al Trattato Nord Atlantico, ratificata con legge 30 novembre 1955, n. 1335.

10. Le esportazioni temporanee di cui al comma 9, lettera a), sono comunque vietate verso i Paesi di cui al comma 6 del presente articolo.

11. Sono escluse altresì dalla disciplina della presente legge le armi sportive e da caccia e relative munizioni; le cartucce per uso industriale e gli artifizi luminosi e fumogeni; le armi e munizioni comuni da sparo di cui all'articolo 2 della legge 18 aprile 1975, n. 110, nonché le armi corte da sparo purché non automatiche; le riproduzioni di armi antiche e gli esplosivi diversi da quelli ad uso militare.

Art. 2. Materiali di armamento.

1. Ai fini della presente legge, sono materiali di armamento quei materiali che, per requisiti o caratteristiche, tecnico-costruttive e di progettazione, sono tali da considerarsi costruiti per un prevalente uso militare o di corpi armati o di polizia.

2. I materiali di armamento di cui al comma 1 sono classificati nelle seguenti categorie:
a) armi nucleari, biologiche e chimiche;
b) armi da fuoco automatiche e relativo munizionamento;
c) armi ed armamento di medio e grosso calibro e relativo munizionamento come specificato nell'elenco di cui al comma 3;
d) bombe, torpedini, mine, razzi, missili e siluri;
e) carri e veicoli appositamente costruiti per uso militare;
f) navi e relativi equipaggiamenti appositamente costruiti per uso militare;
g) aeromobili ed elicotteri e relativi equipaggiamenti appositamente costruiti per uso militare;
h) polveri, esplosivi, propellenti, ad eccezione di quelli destinati alle armi di cui al comma 11 dell'articolo 1;
i) sistemi o apparati elettronici, elettro-ottici e fotografici appositamente costruiti per uso militare;
l) materiali speciali blindati appositamente costruiti per uso militare;
m) materiali specifici per l'addestramento militare;
n) macchine, apparecchiature ed attrezzature costruite per la fabbricazione, il collaudo ed il controllo delle armi e delle munizioni;
o) equipaggiamenti speciali appositamente costruiti per uso militare (1).

3. L'elenco dei materiali di armamento, da comprendere nelle categorie di cui al comma 2 è approvato con decreto del Ministro della difesa di concerto con i Ministri degli affari esteri, dell'interno, delle finanze, dell'industria, del commercio e dell'artigianato, [delle partecipazioni statali] (2) e del commercio con l'estero, da emanarsi entro 180 giorni dalla data di entrata in vigore della presente legge. L'individuazione di nuove categorie e l'aggiornamento dell'elenco dei materiali di armamento sono disposti con decreto da adottarsi nelle forme suindicate, avuto riguardo alla evoluzione della produzione industriale, a quella tecnologica, nonché agli accordi internazionali cui l'Italia aderisce.

4. Ai fini della presente legge sono considerati materiali di armamento:
a) ai soli fini dell'esportazione, le parti di ricambio e quei componenti specifici dei materiali di cui al comma 2, identificati nell'elenco di cui al comma 3;
b) limitatamente alle operazioni di esportazione e transito, i disegni, gli schemi ed ogni tipo ulteriore di documentazione e d'informazione necessari alla fabbricazione, utilizzo e manutenzione dei materiali di cui al comma 2.

5. La presente legge si applica anche alla concessione di licenze per la fabbricazione fuori del territorio nazionale dei materiali di cui al comma 2 e alla lettera a) del comma 4.

6. La prestazione di servizi per l'addestramento e per la manutenzione, da effettuarsi in Italia o all'estero, quando non sia già stata autorizzata contestualmente al trasferimento di materiali di armamento, è soggetta esclusivamente al nulla osta del Ministro della difesa, sentiti i Ministri degli affari esteri e dell'interno, purché costituisca prosecuzione di un rapporto legittimamente autorizzato (3).

7. La trasformazione o l'adattamento di mezzi e materiali per uso civile forniti dal nostro Paese o di proprietà del committente, sia in Italia sia all'estero, che comportino, per l'intervento di imprese italiane, variazioni operative a fini bellici del mezzo o del materiale, sono autorizzati secondo le disposizioni della presente legge.

(1) Vedi anche, d.m. 1 settembre 1995.
(2) Soppresso, ora Ministero del tesoro, del bilancio e della programmazione economica.
(3) Vedi anche Dir. 11 maggio 1991.

Art. 3. Registro nazionale delle imprese.

1. Presso il Ministero della difesa, ufficio del Segretario generale - Direttore nazionale degli armamenti, è istituito il registro nazionale delle imprese e consorzi di imprese operanti nel, settore della progettazione, produzione, importazione, esportazione, manutenzione e lavorazioni comunque connesse di materiale di armamento, precisate e suddivise secondo le funzioni per le quali l'iscrizione può essere accettata. Copie di tale registro nazionale e dei suoi aggiornamenti sono trasmesse, per i fini della presente legge, ai Ministeri degli affari esteri, dell'interno, delle finanze, dell'industria, del commercio e dell'artigianato e del commercio con l'estero.

2. Solo agli iscritti al registro nazionale possono essere rilasciate le autorizzazioni ad iniziare trattative contrattuali e ad effettuare operazioni di esportazione, importazione, transito di materiale di armamento.

3. L'iscrizione al registro di cui al comma 1 tiene luogo dell'autorizzazione di cui all'articolo 28, comma secondo, del testo unico delle leggi di pubblica sicurezza, approvato con regio decreto 18 giugno 1931, n. 773, fermi restando i requisiti indicati all'articolo 9 della legge 18 aprile 1975, n. 110.

4. Le domande di iscrizione al registro nazionale, corredate della documentazione necessaria a comprovare l'esistenza dei requisiti richiesti, secondo le modalità che saranno prescritte con decreto del Ministro della difesa di concerto con i Ministri degli affari esteri e del commercio con l'estero, devono essere presentate dalle imprese che vi abbiano interesse purché in possesso dei seguenti requisiti soggettivi:

a) per le imprese individuali e per le società di persone, la cittadinanza italiana dell'imprenditore o del legale rappresentante, ovvero la residenza in Italia dei suddetti, purché cittadini di Paesi legati all'Italia da un trattato per la collaborazione giudiziaria;
b) per le società di capitali, purché legalmente costituite in Italia ed ivi esercitanti attività concernenti materiali soggetti al controllo della presente legge, la residenza in Italia dei soggetti titolari dei poteri di rappresentanza ai fini della presente legge, purché cittadini italiani o di Paesi legati all'Italia da un trattato per la collaborazione giudiziaria.

5. Possono essere altresì iscritti al registro nazionale i consorzi di imprese costituiti con la partecipazione di una o più imprese iscritte al registro nazionale purché nessuna delle imprese partecipanti versi nelle condizioni ostative di cui ai commi 8, 9, 10, 11 e 12, sempreché il legale rappresentante del consorzio abbia i requisiti soggettivi di cui al comma 4, lettera b).

6. Sono inoltre iscritti d'ufficio al registro nazionale i consorzi industriali promossi a seguito di specifiche intese intergovernative o comunque autorizzati dai competenti organi dello Stato italiano.

7. Gli iscritti al registro nazionale devono Comunicare al Ministero della difesa ogni variazione dei soggetti di cui al comma 4, lettere a) e b), e al comma 5, il trasferimento della sede, la istituzione di nuove sedi, la trasformazione o l'estinzione dell'impresa.

8. Non sono iscrivibili o, se iscritte, decadono dalla iscrizione le imprese dichiarate fallite.

9. Si applicano le norme di sospensione, decadenza e non iscrivibilità stabilite dalla legge 31 maggio 1965, n. 575, nonché dall'articolo 24 della legge 13 settembre 1982, n. 646.

10. Non sono iscrivibili o, se iscritte, decadono dalla iscrizione le imprese i cui rappresentanti indicati al comma 4, lettere a) e b), siano stati definitivamente riconosciuti come appartenuti o appartenenti ad associazioni segrete ai sensi dell'articolo 1 della legge 25 gennaio 1982, n. 17, o siano state condannate ai sensi della legge 20 giugno 1952, n. 645, del testo unico delle leggi di pubblica sicurezza approvato con regio decreto 18 giugno 1931, n. 773, e successive modificazioni, della legge 18 aprile 1975, n. 110, nonché della presente legge.

11. Non sono iscrivibili o, se iscritte, decadono dalla iscrizione le imprese i cui legali rappresentanti siano stati condannati, con sentenza passata in giudicato, per reati di commercio illegale di materiali di armamento.

12. Non sono iscrivibili o, se iscritte, sono sospese dalla iscrizione le imprese che, in violazione del divieto di cui all'articolo 22, assumano con le funzioni ivi

elencate, ex dipendenti delle amministrazioni dello Stato prima di tre anni dalla cessazione del loro servizio attivo.

13. Il verificarsi delle condizioni di cui ai precedenti commi 8, 9, 10 e 11 determina la sospensione o la cancellazione dal registro nazionale, disposta con decreto del Ministro della difesa, da comunicare al Ministeri di cui al comma 1.

14. Qualora venga rimosso l'impedimento alla iscrizione l'impresa potrà ottenere l'iscrizione stessa o, se cancellata, la reiscrizione nel registro nazionale.

15. In pendenza dell'accertamento definitivo degli impedimenti di cui ai commi 8, 9, 10, 11 e 12 l'impresa o il consorzio potranno esercitare le normali attività nei limiti delle autorizzazioni concesse e in corso di validità, ad eccezione di quelle oggetto di contestazione. Ad essi non potranno essere rilasciate nuove autorizzazioni.

Art. 4. Iscrizione al registro nazionale delle imprese.

1. Le modalità per l'iscrizione al registro sono definite con decreto del Ministro della difesa, emanato ai sensi dell'articolo 17 della legge 23 agosto 1988, n. 400.

2. Per la tenuta del registro nazionale di cui all'articolo 3 è costituita presso il Ministero della difesa una commissione presieduta da un magistrato del Consiglio di Stato, e composta da un rappresentante del Ministero degli affari esteri, del Ministero dell'interno, del Ministero delle finanze, del Ministero della difesa, del Ministero dell'industria, del commercio e dell'artigianato e del Ministero del commercio con l'estero.

3. Spetta alla commissione:
a) deliberare sulla base dei requisiti di cui al comma 4 dell'articolo 3 in merito alla iscrizione o reiscrizione al registro;
b) provvedere alla revisione triennale del registro;
c) fare rapporto all'autorità giudiziaria ai fini dell'applicazione delle sanzioni per illeciti relativi al registro;
d) formulare un parere al Ministro per la cancellazione e la sospensione dal registro.

4. Il funzionamento della commissione è disciplinato con decreto del Ministro della difesa, emanato ai sensi dell'articolo 17 della legge 23 agosto 1988, n. 400.

5. Agli oneri relativi al funzionamento della commissione si provvede a carico degli ordinari stanziamenti dello stato di previsione del Ministero della difesa (1).

(1) Vedi, anche, d.m. 19 febbraio 1991, n. 95, e d.m. 28 febbraio 1991, n. 96.

Art. 5. Relazione al Parlamento.

1. Il Presidente del Consiglio dei ministri riferisce al Parlamento con propria relazione entro il 31 marzo di ciascun anno in ordine alle operazioni autorizzate e svolte entro il 31 dicembre dell'anno precedente, anche con riguardo alle operazioni svolte nel quadro di programmi intergovernativi o a seguito di concessione di licenza globale di progetto o in relazione ad essi. (AGGIUNTO da EMENDAMENTO 3.03 al Ddl 1927)

2. I Ministri degli affari esteri, dell'interno della difesa, delle finanze, dell'industria, del commercio e dell'artigianato, delle partecipazioni statali e del commercio con l'estero, per quanto di rispettiva competenza, riferiscono annualmente sulle attività di cui alla presente legge al Presidente del Consiglio dei ministri il quale allega tali relazioni alla relazione al Parlamento di cui al comma 1.

3. La relazione di cui al comma 1 dovrà contenere indicazioni analitiche - per tipi, quantità e valori monetari - degli oggetti concernenti le operazioni contrattualmente definite indicandone gli stati di avanzamento annuali sulle esportazioni, importazioni e transiti di materiali di armamento e sulle esportazioni di servizi oggetto dei controlli e delle autorizzazioni previste dalla presente legge. La relazione dovrà contenere inoltre la lista dei Paesi indicati nelle autorizzazioni definitive, l'elenco delle revoche delle autorizzazioni stesse per violazione della clausola di destinazione finale e dei divieti di cui agli articoli 1 e 15 nonché l'elenco delle iscrizioni, sospensioni o cancellazioni nel registro nazionale di cui all'articolo 3.
"La relazione deve contenere infine l'elenco dei programmi sottoposti a licenza globale di progetto con l'indicazione dei paesi e delle imprese italiane partecipanti, nonché le autorizzazioni concesse dai paesi partners relative a programmi a partecipazione italiana e sottoposti al regime della licenza globale di progetto." (AGGIUNTO da EMENDAMENTO 3.05 del Governo al Ddl 1927)
"3-bis. I titolari di licenza globale di progetto forniscono annualmente al Ministero degli affari esteri una relazione analitica sulle attività espletate sulla base della licenza ottenuta, corredata dai dati su tutte le operazioni effettuate. Tale documentazione è parte integrante della relazione di cui al comma 1." (AGGIUNTO da EMENDAMENTO 3.02 al Ddl 1927)

2. Gli organismo di coordinamento e di controllo.

Capo II : ORGANISMI DI COORDINAMENTO E CONTROLLO

Art. 6. Comitato interministeriale per gli scambi di materiali di armamento per la difesa.

(1) Il CISD è stato soppresso dall'art. 1, l. 24 dicembre 1993, n.537.

Art. 7. Comitato consultivo.

1. E' istituito presso il Ministero degli affari esteri il Comitato consultivo per l'esportazione, l'importazione ed il transito di materiali di armamento. Detto Comitato esprime pareri al Ministro degli affari esteri ai fini del rilascio dell'autorizzazione di cui al successivo articolo 13.

2. Il Comitato è nominato con decreto del Ministro degli affari esteri ed è composto da un rappresentante del Ministero degli affari esteri, di grado non inferiore a ministro plenipotenziario, che lo presiede, da due rappresentanti dei Ministeri dell'interno, della difesa e del commercio con l'estero, e da un rappresentante dei Ministeri delle finanze, dell'industria, del commercio e dell'artigianato, delle partecipazioni statali e dell'ambiente. Nello stesso decreto vengono nominati i supplenti di tutti i componenti effettivi. Le funzioni di segretario sono assolte da un funzionario
del Ministero degli affari esteri.

3. Il Comitato si avvale della consulenza tecnica di due esperti nominati dal Ministro degli affari esteri, di concerto con il Ministro dell'industria, del commercio e dell'artigianato e delle partecipazioni statali e può avvalersi inoltre della consulenza tecnica di altri esperti designati di volta in volta dal presidente del Comitato stesso sentito il parere dei membri.

4. Il Comitato è validamente costituito con la presenza di due terzi dei suoi componenti.

5. Il Comitato è rinnovato ogni tre anni ed i componenti possono essere confermati per una volta sola.

Art. 8. Ufficio di coordinamento della produzione di materiali di armamento.

1. Entro 120 giorni dalla data di entrata in vigore della presente legge è costituito presso la Presidenza del Consiglio ufficio con il compito di fornire al CISD pareri, informazioni e proposte - nel quadro degli indirizzi generali delle politiche di scambio nel settore della difesa adottati dal Parlamento e dal Governo - relative alla produzione nazionale dei materiali di armamento, sui problemi e sulle prospettive di questo settore produttivo in relazione alla evoluzione degli accordi internazionali.

2. L'Ufficio contribuisce anche allo studio e alla individuazione di ipotesi di conversione delle imprese. In particolare identifica le possibilità di utilizzazione per usi non militari di materiali derivati da quelli di cui all'articolo 2, ai fini di tutela dell'ambiente, protezione civile, sanità, agricoltura, scientifici e di ricerca, energetici, nonché di altre applicazioni nel campo civile.

3. L'Ufficio è costituito con decreto del Presidente del Consiglio dei ministri, emanato ai sensi dell'articolo 17 della legge 23 agosto 1988, n. 400. Esso si avvale del contributo di esperti indicati dalle organizzazioni sindacali e dagli imprenditori (1).

(1) Il CISD è stato soppresso dall'art. 1, l. 24 dicembre 1993, n. 537.

3. L'autorizzazione alle trattative.

Capo III : AUTORIZZAZIONE ALLE TRATTATIVE

Art. 9. Disciplina delle trattative contrattuali.

1. I soggetti iscritti al registro di cui all'articolo 3 devono comunicare al Ministro degli affari esteri e al Ministro della difesa l'inizio di trattative contrattuali per l'esportazione, l'importazione e il transito di materiale d'armamento.

2. Entro 60 giorni il Ministro degli affari esteri, d'intesa con il Ministro della difesa, può vietare la prosecuzione della trattativa.

3. Il Ministro può disporre altresì condizioni o limitazioni alle attività medesime, tenuto conto dei princìpi della presente legge e degli indirizzi di cui all'articolo 1, nonché di motivi d'interesse nazionale.

4. L'inizio delle trattative contrattuali ai fini delle operazioni di esportazione, importazione e transito dei materiali di armamento da e verso Paesi NATO e UE (dal DDL art.4) ovvero delle operazioni contemplate da apposite intese intergovernative, deve essere comunicato al Ministero della difesa che, entro 30 giorni dalla ricezione della comunicazione, ha facoltà di disporre condizioni o limitazioni alla conclusione delle trattative stesse.

5. Sono soggette al solo nulla osta del Ministro della difesa importazioni ed esportazioni:
a) di ricambi, componenti e servizi per la manutenzione e riparazione di materiali già oggetto di contratti autorizzati, ma nei quali tali specifiche previsioni non erano contenute o siano scadute;
b) di materiali già regolarmente esportati e che debbano essere reimportati o riesportati temporaneamente, anche in altri Paesi, per riparazioni o manutenzione;
c) di materiali importati, ed eventualmente anche esportati, e che debbano essere restituiti ai costruttori per difetti, inidoneità e simili;
d) di attrezzature da inviare in temporanea esportazione o importazione per installazione, messa a punto, prove e collaudo di materiali già autorizzati alla importazione od esportazione, ma senza che gli atti relativi avessero contenuto

tali specifiche previsioni; e) di materiali di armamento a fini di esibizioni, mostre e dimostrazioni tecniche; dei relativi manuali e descrizioni tecniche e di ogni altro ausilio predisposto per la presentazione dei materiali stessi, nonché di campionature per la partecipazione a gare, appalti e prove di valutazione.

6. I Ministri degli affari esteri e della difesa per le attività di cui al presente articolo possono avvalersi del Comitato di cui all'articolo 7.

7. L'eventuale rifiuto di una autorizzazione, nonché eventuali condizioni e limitazioni, dovranno essere motivati e comunicati all'impresa interessata.

AGGIUNTO (aggiunto dal DDL 1927, art. 5):
"7-bis. Sono escluse dalla disciplina del presente articolo le operazioni svolte nel quadro di programmi congiunti intergovernativi di cui all'articolo 13, comma 1".

Art. 10. Effetti e durata dell'autorizzazione alle trattative.

1. L'autorizzazione ad iniziare le trattative contrattuali di cui all'articolo 9 non conferisce all'impresa il diritto di ottenere le successive autorizzazioni di cui all'articolo 13 e può essere soggetta a limitazioni o condizioni. Essa ha una durata di tre anni e può essere rinnovata in relazione all'andamento delle trattative.

2. L'autorizzazione è soggetta a sospensione o revoca ai sensi del successivo articolo 15.

4. L'autorizzazione all'importazione, esportazione e transito.

Capo IV : AUTORIZZAZIONE ALL'IMPORTAZIONE, ESPORTAZIONE E TRANSITO

Art. 11. Domanda di autorizzazione.

1. Per i materiali assoggettati alle disposizioni della presente legge la domanda di autorizzazione per l'esportazione, l'importazione, le cessioni di licenza e il transito, deve essere presentata al Ministero degli affari esteri che ne dà notizia al Ministero del commercio con l'estero. Tale domanda dovrà essere sottoscritta dal legale rappresentante o da suo delegato allo scopo designato.

2. Nella domanda devono essere indicati:
a) tipo e quantità del materiale di armamento, oggetto dell'operazione. Se trattasi di parti di ricambio dovranno essere indicati i tipi di materiali identificati ai quali esse appartengono;

b) l'ammontare del contratto e l'indicazione dei termini finali di consegna, anche frazionata, previsti dal contratto medesimo, nonché le condizioni per la disponibilità alla consegna di ricambi, per la prestazione di servizi di manutenzione o per la cessione di altri servizi di assistenza;
c) l'ammontare di eventuali compensi di intermediazione nonché la dichiarazione di cui agli articoli 12 e 20 del decreto del Presidente della Repubblica 29 settembre 1987, n. 454;
d) il Paese di destinazione finale del materiale ovvero eventuali Paesi, enti, imprese e soggetti di destinazione intermedia o finale ai sensi del comma 3, lettera c);
e) l'identificazione del destinatario (autorità governativa, ente pubblico o impresa autorizzata);
f) eventuali obblighi economici verso lo Stato per diritti di proprietà e di brevetto e simili;
g) eventuali impegni per compensazioni industriali;
h) eventuali affidamenti da parte di Amministrazioni dello Stato per la esecuzione della operazione pattuita.

3. Alla domanda di autorizzazione all'esportazione devono essere acclusi:
a) copia dell'autorizzazione a trattare o del nulla osta, ove previsti;
b) copia del contratto o del subcontratto di fornitura o acquisto o trasporto per la parte inerente alle condizioni commerciali e finanziarie dell'operazione; se il contratto è scritto in lingua straniera, la copia deve essere corredata dalla traduzione in lingua italiana;
c) 1) un certificato d'importazione rilasciato dalle autorità governative del Paese destinatario, per i Paesi che partecipano con l'Italia ad accordi di controllo reciproco sulle esportazioni di materiali di armamento; 2) per tutti gli altri Paesi, un <certificato di uso finale> rilasciato dalle autorità governative del Paese destinatario, attestante che il materiale viene importato per proprio uso e che non verrà riesportato senza la preventiva autorizzazione delle autorità italiane preposte a tale compito.

4. Il certificato di uso finale deve essere autenticato dalle autorità diplomatiche o consolari italiane accreditate presso il Paese che lo ha rilasciato.

5. La documentazione di cui al presente articolo non è richiesta per le operazioni previste all'articolo 9, commi 4 e 5.

AGGIUNTO (dal DDL 1927, art. 6):
"5-bis. Alla domanda di licenza globale di progetto di cui all'articolo 13, comma 1, deve essere acclusa copia dell'autorizzazione a trattare, fatta eccezione per i programmi di cui all'articolo 9, comma 7-bis, e devono essere indicati:

a) la descrizione del programma congiunto con indicazione del tipo di materiale di armamento che si prevede di produrre (EMENDAMENTO 6.4 al Ddl 1927)

b) le imprese dei Paesi di destinazione o di provenienza del materiale ove già individuate nell'ambito del programma congiunto. Laddove esse non siano ancora individuate, la loro identificazione successiva va comunicata al Ministero degli affari esteri entro novanta giorni dall'individuazione; (EMENDAMENTO 6.4 al Ddl 1927)

c) l'identificazione dei destinatari (autorità governative, enti pubblici o privati autorizzati) nell'ambito del programma congiunto. Tale identificazione non è richiesta per le operazioni previste dall'articolo 9 commi 4 e 5 della legge 9 luglio 1990, n. 185. (EMENDAMENTO 6.4 al Ddl 1927)

Art. 12. Attività istruttoria.

1. Il Ministero degli affari esteri effettua l'istruttoria per il rilascio dell'autorizzazione di cui all'articolo 13. A tal fine accertata la completezza della documentazione prodotta, la trasmette al Comitato di cui all'articolo 7, salvo i casi previsti all'articolo 9, commi 4 e 5.

2. Il Comitato, accertata la coerenza delle finalità dichiarate dell'operazione con le norme della presente legge nonché con le direttive formulate dal CISD ai sensi dell'articolo 6, esprime il proprio parere al Ministro degli affari esteri.
3. Il Ministro degli affari esteri, per operazioni che ritiene di particolare rilevanza politica può richiedere un ulteriore esame da parte del CISD (1). (1) Il CISD è stato soppresso dall'art. 1, l. 24 dicembre 1993, n. 537.

Art. 13. Autorizzazione.

1. Il Ministro degli affari esteri, sentito il Comitato di cui all'articolo 7, autorizza, di concerto con il Ministro delle finanze, l'esportazione e l'importazione, definitive o temporanee, ed il transito dei materiali di armamento, nonché la cessione all'estero delle licenze industriali di produzione dello stesso materiale e la riesportazione da parte dei Paesi importatori. L'eventuale rifiuto dell'autorizzazione dovrà essere motivato.
(AGGIUNTO dal DDL 1927, art. 7)
"L'autorizzazione può assumere anche la forma di licenza globale di progetto, rilasciata a singolo operatore, quando riguarda esportazioni, importazioni o transiti di materiali di armamento da effettuare nel quadro di programmi congiunti intergovernativi o industriali di ricerca, sviluppo, produzione di materiali di armamento svolti con imprese di Paesi membri dell'UE o della NATO con i quali l'Italia abbia sottoscritto specifici accordi che garantiscano, in materia di trasferimento e di esportazione di materiali di armamento, il controllo delle operazioni secondo i principi ispiratori della presente legge. Detti accordi devono inoltre prevedere disposizioni analoghe a quelle di cui all'articolo 13 dell'Accordo quadro tra la Repubblica francese, la Repubblica federale di Germania, la Repubblica italiana, il Regno di Spagna, il Regno di Svezia e il Regno Unito della Gran Bretagna e dell'Irlanda del Nord relativo alle

misure per facilitare la ristrutturazione e le attività dell'industria europea per la difesa, fatto a Farnborough il 27 luglio 2000. (EMENDAMENTO 7.3 e 7.40 del Governo al Ddl 1927)
Con la stessa licenza globale di progetto può, inoltre, essere autorizzata la fornitura di materiali di armamento, sviluppati o prodotti sulla base di programmi congiunti, ai suddetti Paesi per uso militare nazionale". (AGGIUNTO dal DDL 1927, art. 7)

2. L'autorizzazione di cui al comma 1 è rilasciata dal Ministro degli affari esteri senza il previo parere del Comitato di cui all'articolo 7 per le operazioni:
a) previste dall'articolo 9, comma 4;
b) che hanno avuto il nulla osta alle trattative contrattuali di cui all'articolo 9, comma 5.

3. Della autorizzazione va data notizia alle Amministrazioni interessate.

4. (Omissis) (1).

5. L'autorizzazione non può essere rilasciata in caso di domande incomplete ovvero mancanti della documentazione di cui all'articolo 11, comma 2 e comma 3. A tali fini il Ministero degli affari esteri richiede all'interessato gli elementi o la documentazione riscontrati carenti o incompleti rispetto a quanto previsto dalla presente legge.

6. Per l'ottenimento delle autorizzazioni per le operazioni di esportazione di componenti specifici e parti di ricambio di materiali di armamento, deve essere prodotto il certificato di importazione, rilasciato dalle autorità governative del Paese primo importatore ad una propria impresa, sempre che questa sia debitamente autorizzata dal proprio governo a produrre e commercializzare materiali di armamento, salva la facoltà di richiedere per quei Paesi che non rilasciano un certificato di importazione, il certificato di uso finale o documentazione equipollente.

(1) Comma abrogato dall'art. 13, d.p.r. 20 aprile 1994, n. 373.

Art. 14. Termine per le operazioni.

1. Le operazioni previste nella presente legge debbono essere effettuate entro i termini indicati nelle relative autorizzazioni. I termini possono essere prorogati per periodi non superiori a 24 mesi, su motivata domanda da presentare non oltre la scadenza, dal Ministro degli affari esteri sentito il comitato di cui all'articolo 7 "ad eccezione dei casi previsti dall'articolo 9, commi 4 e 5, ovvero in caso di licenza globale di progetto". (AGGIUNTO dalla Commissione al DDL 1927 A, art. 8)

2. Copia delle autorizzazioni e delle proroghe immediatamente inviata alle Amministrazioni rappresentate nel Comitato di cui all'articolo 7.

3. L'autorizzazione, fatta eccezione per la licenza globale di progetto che è rilasciata per un periodo massimo di tre anni ed è prorogabile, (AGGIUNTO dal DDL 1927, art. 8) non può essere rilasciata per un periodo di validità inferiore a quello previsto per l'esecuzione del contratto, eventualmente prorogabile in relazione all'effettivo andamento delle consegne e delle restanti operazioni contrattuali. Nel caso in cui non siano previsti termini di esecuzione del contratto, l'autorizzazione dovrà avere una validità di almeno 18 mesi eventualmente prorogabile.

Art. 15. Sospensione o revoca delle autorizzazioni.

1. Le autorizzazioni di cui all'articolo 9 e all'articolo 13 sono soggette a sospensione o revoca quando vengano a cessare le condizioni prescritte per il rilascio.

2. La sospensione o revoca delle autorizzazioni di cui all'articolo 9 sono disposte con decreto del Ministro della difesa d'intesa con il Ministro degli affari esteri.

3. La sospensione o revoca delle autorizzazioni di cui all'articolo 13 sono disposte con decreto del Ministro degli affari esteri sentito il CISD.

4. Le decisioni di cui ai commi 2 e 3 vengono comunicate al Comitato consultivo di cui all'articolo 7.

5. La copertura assicurativa prevista dalla legge 24 maggio 1977, n. 227, è estesa ai casi di revoca, sospensione o mancata proroga dell'autorizzazione di cui all'articolo 13 non imputabili alla volontà dell'operatore.

6. La revoca o la sospensione delle autorizzazioni di cui all'articolo 13, o il loro mancato rinnovo o proroga nel corso della esecuzione di un contratto, si devono intendere, ai sensi dell'articolo 14, numero 6, della legge 24 maggio 1977, n. 227, come cause non dipendenti da inadempienze contrattuali dell'operatore nazionale agli effetti dell'escussione di fidejussioni e della mancata o ritardata restituzione di cauzioni, depositi o anticipazioni prestati o costituiti per i motivi indicati alla lettera m) dell'articolo 15 della suddetta legge.

7. In casi eccezionali il CISD può temporaneamente vietare l'esportazione anche delle armi di cui all'articolo 1, comma 11, verso quei Paesi, di cui fornirà elenco al Ministero degli affari esteri, per i quali avrà ritenuto opportuno adottare misure cautelative.

8. Il divieto sarà rimosso dallo stesso CISD solo quando saranno cessate le cause che lo hanno determinato (1).
(1) Il CISD è stato soppresso dall'art. 1, l. 24 dicembre 1993, n. 537.

Art. 16. Transito e introduzione nel territorio dello Stato dei materiali di armamento soggetti alle disposizioni di pubblica sicurezza.

1. Le disposizioni della presente legge non si applicano ai casi di attraversamento nel territorio dello Stato dei materiali di armamento di cui all'articolo 2, oggetto di transazioni commerciali all'estero da parte di non residenti.

2. In tali casi, nonché in ogni altro caso di introduzione nel territorio dello Stato dei materiali di armamento di cui al comma 1 che non debbono varcare a qualsiasi titolo la linea doganale e che sono destinati ad altri paesi, si applicano, sempreché i materiali stessi siano iscritti a manifesto, esclusivamente le disposizioni dei commi terzo e quarto dell'articolo 28 del testo unico delle leggi di pubblica sicurezza approvato con R.D. 18 giugno 1931, n. 773, e dell'articolo 40 del relativo regolamento di esecuzione, approvato con R.D. 6 maggio 1940, n. 635.

3. Tali disposizioni, con esclusione dell'articolo 40 del regolamento succitato, si applicano altresì per le armi che facciano parte delle dotazioni di bordo risultanti dai documenti ufficiali.

4. Il prefetto può negare l'autorizzazione per l'introduzione nel territorio dello Stato dei materiali e delle armi suddetti per motivi di ordine pubblico o di pubblica sicurezza dandone tempestiva notizia ai Ministeri degli affari esteri e della difesa, ovvero, sentiti i Ministeri predetti, per ragioni inerenti alla sicurezza dello Stato.

5. Gli obblighi delle imprese.

Capo V : OBBLIGHI DELLE IMPRESE

Art. 17.Contributo per l'iscrizione nel registro nazionale.

1. Per l'iscrizione nel registro nazionale di cui all'articolo 3 gli interessati sono tenuti a versare un contributo annuo nella misura e secondo le modalità stabilite con. decreto del Ministro della difesa, di concerto con il Ministro del tesoro, del bilancio e della programmazione economica.

2. Il decreto è pubblicato nella Gazzetta Ufficiale entro il 31 ottobre dell'anno precedente a quello cui il contributo si riferisce (1).
(1) Vedi d.m. 19 settembre 1997.

Art. 18. Lista dei materiali.

1. Le imprese esportatrici dei materiali di armamento indicati nella presente legge, entro 120 giorni dalla data di entrata in vigore del decreto di cui all'articolo 2, comma 3, sono tenute a depositare presso la commissione di cui all'articolo 4 la lista dei materiali di armamento oggetto di esportazione con l'indicazione, per ognuno di essi, dell'eventuale classifica di segretezza precedentemente apposta dal Ministero della difesa. Allo stesso Ministero sono altresì comunicati, con gli stessi criteri, gli eventuali aggiornamenti della lista.

Art. 19. Comunicazioni relative a vettori e spedizionieri.

1. Per le operazioni che prevedono a carico dell'esportatore la spedizione e la consegna a destino del materiale di armamento è fatto obbligo agli esportatori di acquisire da vettori e spedizionieri ogni utile indicazione sulle modalità di trasporto e sull'itinerario relativo, nonché sulle eventuali variazioni che siano intervenute in corso di trasporto. I relativi documenti dovranno essere conservati agli atti dell'esportatore per il termine di dieci anni.

2. Per le operazioni che prevedono la consegna "franco fabbrica" o "franco punto di partenza", gli esportatori sono obbligati a comunicare contestualmente alle Amministrazioni (AGGIUNTO dal DDL 1927, art. 9) degli affari esteri, della difesa, dell'interno e delle finanze, la data e le modalità della consegna fornendo ogni utile indicazione sullo spedizioniere o vettore incaricato dell'operazione.

3. Tale comunicazione dovrà essere effettuata, da parte del legale rappresentante o da suo delegato, preventivamente e comunque non oltre il termine di tre giorni dalla data della ricezione del relativo avviso di ritiro da parte del destinatario o del vettore da questi incaricato.

4. Le disposizioni di cui al presente articolo non si applicano alle esportazioni effettuate per conto dell'Amministrazione dello Stato.

Art. 20. Utilizzo delle autorizzazioni.

1. L'impresa autorizzata all'esportazione o al transito di materiali di armamento è tenuta, ad eccezione delle operazioni effettuate per conto dello Stato ovvero in caso di licenza globale di progetto (AGGIUNTO dal DDL 1927, art. 10):
a) a comunicare tempestivamente al Ministero degli affari esteri la conclusione, anche se parziale, delle operazioni autorizzate;
b) ad inviare entro 180 giorni dalla conclusione delle operazioni di cui alla lettera a) al Ministero degli affari esteri: il formulario di verifica ovvero la bolletta doganale di entrata nel Paese di destinazione finale ovvero la documentazione di presa in consegna da parte dell'ente importatore, ovvero documentazione equipollente rilasciata dall'autorità governativa locale.

2. La proroga di ulteriori 90 giorni può essere concessa dal Ministro degli affari esteri, previo parere del Comitato consultivo di cui all'articolo 7, sulla base di

motivata e documentata richiesta dell'operatore, da presentarsi almeno 30 giorni prima della scadenza del termine originario.

3. Nel caso in cui l'esportatore italiano dichiari l'impossibilità per giustificati motivi di ottenere dalle autorità estere la documentazione di cui al comma 1, lettera b), il Comitato di cui all'articolo 7 esprime parere in ordine ai motivi di giustificazione addotti. Fino a che il Comitato di cui all'articolo 7 non esprimerà parere in merito ai motivi di giustificazione addotti, non potranno essere accordate proroghe all'autorizzazione.

4. In caso di ritardata presentazione della documentazione di cui al comma 1 e sinché il ritardo perduri, salvo il caso di giustificazione di cui al comma 3, non possono essere accordate proroghe alle autorizzazioni cui si riferisce la commissione.

4-bis. In caso di spedizione in utilizzo di licenza globale di progetto, l'impresa è tenuta a conservare per cinque anni la documentazione relativa ai materiali forniti, utile ad attestare l'arrivo a destinazione dei materiali stessi. Ai fini della presente legge tale documentazione dovrà essere esibita su richiesta del Ministero degli affari esteri. (AGGIUNTO dal DDL 1927, art. 10)

Art. 21. Seminari, soggiorni di studio e visite.

1. La Presidenza del Consiglio dei ministri, sentito il Ministro della difesa, su richiesta dell'impresa interessata, può autorizzare seminari, soggiorni di studio e visite di cittadini italiani e stranieri in Italia che abbiano ad oggetto materie attinenti a prodotti coperti da classifica di segretezza.

Art. 22. Divieti a conferire cariche.

1. I dipendenti pubblici civili e militari, preposti a qualsiasi titolo all'esercizio di funzioni amministrative connesse all'applicazione della presente legge nei due anni precedenti alla cessazione del rapporto di pubblico impiego non possono, per un periodo di tre anni successivo alla cessazione del rapporto stesso, a qualunque causa dovuta, far parte di consigli di amministrazione, assumere cariche di presidente, vice presidente, amministratore delegato, consigliere delegato, amministratore unico, e direttore generale nonché assumere incarichi di consulenza, fatti salvi quelli di carattere specificamente tecnico-operativo, relativi a progettazioni o collaudi, in imprese operanti nel settore degli armamenti.

2. Le imprese che violano la disposizione del comma 1 sono sospese per due anni dal registro nazionale di cui all'articolo 3.

6. Le sanzioni.

Capo VI : SANZIONI

Art. 23. Falsità nella documentazione.

1. Chiunque, in una documentazione prodotta ai sensi della presente legge, fornisce con dolo indicazioni non veritiere, inerenti al rilascio dell'autorizzazione prevista dall'articolo 13 o per il relativo rinnovo, è punito, nel caso abbia conseguito l'autorizzazione, con la reclusione da 2 a 6 anni ovvero con la multa da un decimo a tre decimi del valore del contratto (1).

2. Se le indicazioni non veritiere sono determinanti per l'ottenimento della iscrizione nel registro nazionale di cui all'articolo 3, ovvero del nulla osta previsto dall'articolo 9, comma 5, si applica, salvo che il caso non costituisca reato più grave, la pena della multa da 50 a 300 milioni di lire (2).

(1) La sanzione è esclusa dalla depenalizzazione in virtù del secondo comma dell'art. 32, l. 24 novembre 1981, n. 689.
(2) L'entità minima della multa è stata così elevata dall'art. 15, l. 27 febbraio 1992, n. 222. La sanzione è esclusa dalla depenalizzazione in virtù del secondo comma dell'art. 32, l. 24 novembre 1981, n. 689.

Art. 24.Inosservanza delle prescrizioni amministrative.

1. Chiunque effettui esportazioni o transito di materiali di armamento in violazione delle condizioni di consegna alla destinazione indicata nella richiesta di autorizzazione di cui all'articolo 13, salvo che il fatto costituisca più grave reato, è punito con la reclusione fino a cinque anni, ovvero con la multa da due a cinque decimi del valore dei contratti (1).

(1) L'art. 15, l. 27 febbraio 1992, n. 222, ha fissato in lire 50.000.000 l'entità minima della sanzione, che è esclusa dalla depenalizzazione in virtù del secondo comma dell'art. 32, l. 24 novembre 1981, n. 689.

Art. 25. Mancanza dell'autorizzazione.

1. Salvo che il fatto costituisca più grave reato, colui che senza l'autorizzazione di cui all'articolo 13 effettua esportazione, importazione o transito di materiali di armamento, contemplati nei decreti di cui all'articolo 2, comma 3, è punito con la reclusione da tre a dodici anni ovvero con la multa da 50 a 500 milioni (1).

2. Chiunque ponga in essere trattative in violazione di quanto disposto all'articolo 9, è punito con la reclusione fino a quattro anni ovvero con la multa da 50 a 500 milioni (1).

3. Sono confiscati quei materiali di armamento che, individuati dagli organi preposti come destinati all'esportazione, non risultino accompagnati dalle prescritte autorizzazioni.

(1) L'entità minima della multa è stata così elevata dall'art. 15, l. 27 febbraio 1992, n. 222. La sanzione è esclusa dalla depenalizzazione in virtù del secondo comma dell'art. 32, l. 24 novembre 1981, n. 689.

Art. 26.Obbligo di comunicazione da parte dell'autorità giudiziaria

1. L'autorità giudiziaria che procede per i reati previsti dagli articoli 23, 24 e 25 ne dà comunicazione immediata al Ministro degli affari esteri e al Ministro della difesa ai fini dell'adozione dei provvedimenti di rispettiva competenza.

Art. 27. Norme sull'attività bancaria.

1. Tutte le transazioni bancarie in materia di esportazione, importazione e transito di materiali di armamento, come definiti dall'articolo 2, fatta eccezione per le operazioni in utilizzo di licenza globale di progetto (AGGIUNTO dal DDL 1927, art. 11), vanno notificati al Ministero del tesoro, del bilancio e della programmazione economica.
2. Il Ministro del tesoro, entro 30 giorni dalla notifica, deve autorizzare, in base a quanto stabilito dalla presente legge, lo svolgimento delle operazioni bancarie.

3. La relazione al Parlamento, di cui all'articolo 5, deve contenere un capitolo sull'attività degli istituti di credito operanti nel territorio italiano nella materia indicata nel comma 1.

7. Le disposizioni finali e transitorie.

Capo VII : DISPOSIZIONI FINALI E TRANSITORIE

Art. 28. Disposizioni transitorie.

1. Fino all'emanazione del decreto di cui al comma 3 dell'articolo 2, resta in vigore l'attuale normativa per il materiale elencato nella <Tabella export> relativamente al materiale di armamento.

2. Fino alla istituzione del registro nazionale di cui all'articolo 3 nonché nel Comitato consultivo di cui all'articolo 7, non si applicano le disposizioni previste all'articolo 3, comma 2, e resta in vigore la normativa vigente.

3. Le autorizzazioni in corso all'entrata in vigore della presente legge continuano ad avere validità.

4. Per quanto riguarda le armi e i materiali menzionati nel comma 11 dell'articolo 1 la licenza del questore, prevista dall'articolo 31 del testo unico delle leggi di pubblica sicurezza, approvato con regio decreto 18 giugno 1931, n. 773, sostituisce la licenza del Ministro degli affari esteri di concerto con il

Ministro delle finanze. Il Ministro del commercio con l'estero emanerà le relative norme di attuazione.

Art. 29. Regolamento di esecuzione.

1. Entro 120 giorni dall'entrata in vigore della presente legge, con decreto del Presidente del Consiglio dei ministri, sarà emanato ai sensi dell'articolo 17 della legge 23 agosto 1988, n. 400, il regolamento contenente le norme di esecuzione.

Art. 30. Distacco di personale.

1. Per lo svolgimento delle attività connesse al rilascio delle autorizzazioni previste dalla presente legge, nel regolamento d'esecuzione di cui all'articolo 29 saranno emanate, ai sensi degli articoli 56 e seguenti del decreto del Presidente della Repubblica 10 gennaio 1957, n. 3, norme per il distacco al Ministero degli affari esteri di personale di altre amministrazioni.

Art. 31. Disposizioni vigenti e abrogate.

1. Restano in vigore, ove non incompatibili con la presente legge, le disposizioni del regolamento di esecuzione del testo unico delle leggi di pubblica sicurezza approvato con regio decreto 6 maggio 1940, n. 635, e successive modificazioni, della legge 2 ottobre 1967, n. 895, della legge 14 ottobre 1974, n. 497, della legge 18 aprile 1975, n. 110.
2. (Omissis) (1).
3. (Omissis) (2).
4. Tutte le disposizioni incompatibili con la presente legge sono abrogate.

(1) Modifica il paragrafo 6 dell'allegato al r.d. 11 luglio 1941, n. 1161.
(2) Modifica il paragrafo 8 dell'allegato al r.d. 11 luglio 1941, n. 1161.

Capitolo Undicesimo

CRITTOGRAFIA E FUNZIONI DELLA *NATIONAL SECURITY AGENCY*

SOMMARIO: 1. La *National Security Agency*. - 2. La struttura della *National Security Agency*. - 3. L'organizzazione e le funzioni della *National Security Agency*. - 4. L'avvento delle nuove tecnologie.

1. La *National Security Agency*.

Nel dicembre del 1951, il Direttore della CIA, Walter Bedell Smith, presentò un *memorandum* al *National Security Council* nel quale evidenziava il pessimo stato di sicurezza ed operatività nel quale si trovavano le attività di *intelligence* delle comunicazioni del Governo americano e del modo col quale queste operazioni venivano condotte.
Egli accusava che le attività SIGINT americane erano "diventate inefficaci a causa di un sistema di autorità divise e di responsabilità multiple"[206].
Smith, oltre alle sue accuse, propose al Presidente Truman di ordinare al Segretario di Stato Dean G. Acheson ed al Segretario alla Difesa Robert A. Lovett di effettuare un'indagine sull'AFSA – *Armed Force Security Agency* -, allo scopo di evitare che l'America perdesse quell'insostituibile fonte d'*intelligence*.
Neppure tre giorni dopo, esattamente il 13 dicembre 1951, Truman diede l'ordine di eseguire l'indagine.
Nel giro di sei mesi il *Brownell Committee*, l'organo che si occupò dell'indagine circa lo stato dell'*Armed Force Security Agency* consegnò il proprio rapporto contenente i risultati raggiunti nell'indagine: nelle 239 pagine del documento erano raccolti tutti i problemi e le carenze dell'agenzia e del settore COMINT.
In particolare, si evidenziava che "i membri dell'agenzia spendono la maggior parte del proprio tempo in frustranti dettagli per salvaguardare l'autonomia del proprio settore. Il direttore dell'AFSA è obbligato a sprecare energie in negoziazioni e compromessi in un'atmosfera di competizione settoriale. Egli non ha alcun grado di controllo [...] sulle tre unità COMINT. In effetti, egli è sotto il controllo delle unità dei tre settori"[207].
Quattro mesi più tardi, precisamente il 24 ottobre 1952 nell'Ufficio Ovale il Segretario alla Difesa Lovett, il Segretario di Stato Acheson ed Everett Gleason del *National Security Council* incontrarono il Presidente Truman.
L'esito di quell'incontro segnò per sempre il futuro, oltre che dei servizi

[206] Cfr. BAMFORD, *Body of Secrets*, op. cit., p. 30.
[207] Cfr. BAMFORD, *The Puzzle Palace*, op. cit., p. 77.

COMINT, anche di tutta l'*intelligence* americana: con un ordine altamente segreto, il Presidente Truman smantellò l'improduttiva *Armed Forces Security Agency* istituendo al suo posto una nuova agenzia segreta, da tenere nascosta al Congresso, ai cittadini ed al mondo intero.
La mattina del 4 novembre 1952 nacque, nel più assoluto riserbo, la *National Security Agency* (NSA): essa fu istituita nella più assoluta segretezza, non fu creata con un atto legislativo, come fu per la *Central Intelligence Agency*, ma con un ordine presidenziale di sette pagine firmato dal Presidente Truman.
Il livello di riservatezza era così alto che l'ordine di Truman non solo era classificato come *Top Secret*, ma era contrassegnato con un codice anch'esso segreto.
Quel giorno non ci fu nessun interessamento da parte degli organi di informazione, nessun dibattito fu discusso al Congresso, nessuna dichiarazione fu rilasciata alla stampa: persino la data di nascita dell'agenzia fu tenuta nascosta.
In ogni caso, se anche ci fosse stata una fuga di notizie, anche minima, l'attenzione della nazione era tutta concentrata sull'elezione del nuovo Presidente degli Stati Uniti d'America, Dwight Eisenhower.
La *National Security Agency* divenne così l'agenzia responsabile dell'*intelligence* delle comunicazioni degli Stati Uniti d'America, la quale avrebbe diretto, controllato e coordinato tutte le attività e le operazioni relative a questi settori.
Nel giro di pochi anni, sarebbe diventata la più segreta, potente e controversa agenzia americana non solo nel settore SIGINT, ma di tutto l'apparato dell'*intelligence* degli Stati Uniti.
Un problema che si voleva urgentemente affrontare e risolvere era la carenza di risorse e strutture adibite a questa attività, carenza che dava luogo a due problematiche: innanzitutto, era evidente, in quel periodo, il ritardo in ogni settore dell'*intelligence* delle comunicazioni, inferiore al livello che il Paese necessitava per la propria sicurezza nazionale, inferiorità che rendeva gli Stati Uniti d'America vulnerabili da questo punto di vista.
In secondo luogo, questo *deficit* impediva agli Stati Uniti di sfruttare al massimo il proprio potenziale d'*intelligence*: obiettivo dell'America era quello di elevare il proprio *status* a quello di superpotenza mondiale e di punto di riferimento del mondo occidentale capitalista, in contrapposizione a quello sovietico comunista, per frenare in questo modo l'espansionismo russo.
Ma questi obiettivi sarebbero rimaste mere utopie se l'America non avesse compiuto considerevoli progressi in questo campo e se non si fosse dotata rapidamente di una struttura COMINT, efficace ed avanzata, in grado di poter competere con quella utilizzata dall'Unione Sovietica[208].
Effettivamente, gli Stati Uniti da soli non avevano le capacità tecniche per riuscire a tenere sotto controllo l'Unione Sovietica, i suoi alleati ed ogni altro paese che si fosse rivelato ostile nei confronti dell'America.
Durante la guerra, gli Stati Uniti e la Gran Bretagna avevano ottenuto, grazie ai loro servizi COMINT, importanti successi militari nei confronti della Germania e del Giappone che capovolsero gli esiti del conflitto a loro favore: il

[208] Ibidem, *Body of Secrets*, op. cit., p.355.

programma Venona, ad esempio, permise agli americani di catturare spie sovietiche ed evitare che i segreti relativi alla bomba atomica cadessero nelle mani dei russi.
Durante i primi anni della guerra fredda, però, le cose stavano cambiando e non sarebbe stato semplice per gli Alleati ripetere i successi ottenuti in precedenza: i Sovietici stavano compiendo validi progressi nei vari settori dello spionaggio elettronico, i loro sistemi di crittografia erano stati cambiati e resi molto più sicuri.
Già dai primi anni '50, la maggior parte delle comunicazioni militari e diplomatiche sovietiche furono perfezionate, inviate utilizzando algoritmi di cifratura molto più complicati da decifrare.
I russi, inoltre, aumentarono lo scambio di messaggi via cavo, sotterranei e sottomarini, espediente che rendeva più complicato l'intercettamento.
Durante i primi anni della guerra fredda, i servizi COMINT americani stavano diventando incapaci di tenere il passo dei sovietici in questo settore, inabili di decifrare i nuovi codici crittografici: un ufficiale della CIA affermò che quel periodo era stato l'età nera dell'intelligence dei segnali e delle comunicazioni d'America[209].
Gli USA ritennero pertanto conveniente per la propria sicurezza proseguire l'Accordo UKUSA anche nel periodo post-bellico e sfruttare i territori, le risorse e le capacità degli alleati. Stati Uniti d'America, Gran Bretagna, Canada, Australia e Nuova Zelanda continuarono la loro collaborazione seguendo le tecniche operative utilizzate durante la guerra: essi avevano diviso il globo in differenti settori d'interesse a seconda della propria posizione geografica e ciascun Paese avrebbe avuto la responsabilità del traffico dei segnali elettronici e delle comunicazioni, in entrata ed in uscita nell'area assegnata, condividendo poi il materiale ottenuto con gli altri *partner*.
Le comunicazioni mondiali stavano per essere messe sotto controllo, allo scopo di creare un sistema di controllo globale delle comunicazioni: se si scopriva che una qualsiasi area era rimasta "scoperta", immediate misure venivano prese da uno dei cinque partner per colmare questo gap.
Ogni agenzia SIGINT dell'accordo avrebbe intercettato il materiale proveniente dall'area che doveva controllare e passato questo materiale "grezzo" ai servizi COMINT americani, i quali l'avrebbero decifrato, tradotto ed analizzato.
Questo sistema sarebbe pertanto stato gestito principalmente dagli Stati Uniti, i quali diventarono, in termini di risorse, i maggiori contribuenti al progetto ma anche i maggiori fruitori di esso.
L'America necessitava di una struttura in grado di affrontare con successo questo incarico, una struttura all'altezza di questa responsabilità, capace di gestire il proprio materiale e quello trasmesso dai suoi alleati.
Era necessario dotare l'America di una nuova struttura, più potente ed indipendente di qualsiasi altra, che raggruppasse le precedenti unità COMINT, divise e spesso in competizione tra loro, per creare la più efficiente e potente agenzia d'intelligence delle comunicazioni.

---

[209] Ibidem.

Inoltre, essa doveva essere in grado proteggere le comunicazioni del Governo degli Stati Uniti d'America, impedendo che venissero intercettati da altri Paesi. E il 4 novembre 1953, il Generale Maggiore Ralph J. Canine, nominato primo direttore della *National Security Agency*, cominciò questo compito.

2. La struttura della *National Security Agency*.

Il quartier generale della NSA si trova all'interno di una tenuta di 130 ettari a Fort "George G. Meade"[210], nel Maryland, a metà strada tra Baltimora e Washington: è l'agenzia d'*intelligence* più grande del mondo[211], formata da 50 edifici, collegati tra loro da oltre 50 km di strade e dal corridoio sotterraneo più lungo della nazione, 300 metri, situato sotto l'Operations Buildings[212].
Questo complesso, soprannominato "Crypto City", è una delle città con il più alto tasso d'incremento annuo in America.
Tra il 1982 e il 1996 il costo per la costruzione di nuovi edifici, strade e infrastrutture è costato circa mezzo miliardo di dollari, ed un altro mezzo miliardo il prezzo speso per l'acquisto di terreni circostanti.
Solo tra il 1996 e il 2000, si stima che circa 152,8 milioni di dollari siano stati spesi per ulteriori lavori all'interno di Fort Meade.
Al suo interno lavorano più di 38.000 persone, sia civili che militari, più del personale impiegato dalla CIA e dell'FBI congiuntamente, ai quali bisogna aggiungere 45.000 militari di ogni grado che operano nella stazioni d'intercettazione sparse in tutto il mondo[213].
Il *budget* dell'agenzia è sempre stato un oggetto di mistero per l'opinione pubblica: mentre i *budget* di altre agenzie d'*intelligence* statunitensi sono sempre stati dichiarati in rapporti pubblici, il budget della NSA è riservato e le stime sono spesso vaghe ed imprecise.
John Pike, un osservatore dell'intelligence americana e membro della Federazione degli Scienziati Americani (FAS, Federation of American Scientists) ha pubblicato un articolo sul quotidiano americano "The Baltimore Sun" nel quale stimava che il governo americano spende circa 8 miliardi di dollari l'anno per i servizi SIGINT, *budget* utilizzato per la maggior parte dal *National Security Agency* e dal *National Reconaissance Office* (NRO), agenzia di spionaggio che si occupa della costruzione e della gestione dei satelliti spia americani, la quale opera unitamente alla NSA.
James Bamford in *Body of Secrets* fornisce i dati più aggiornati e specifica che il budget complessivo per il periodo 1995-1999 è stato di 17.570.600.000 miliardi di dollari, e che solo per il biennio 2000-2001 ne sono stati preventivati

---

210 Dal nome del Generale George Gordon Meade (1815-1872), comandante delle "truppe nordiste" nella battaglia del Potomac durante la guerra civile.
211 Cfr. Parrish Thomas 1996, The Cold War Encyclopedia, Henry Holt Reference Book.
212 Cfr. Tully A. 1969, The Super Spies: more secret, more powerful than the CIA, William Morrow & Company, New York, p. 65.
213 Cfr. Bamford, Body of Secrets, op. cit., p. 481.

7.304.000.000[214].
Il consumo energetico è impressionante, 409.005.849 milioni di kilowatt all'ora, 54 milioni di watt al giorno, per un costo mensile di 2 milioni di dollari; la corrente elettrica è trasportata da più di mille kilometri di fili, l'equivalente di quelli di una città di medie dimensioni.
La superficie totale occupata dai computer e dagli elaboratori della NSA è di sei acri, più di 24.000 mq, raffreddati da una apposita torre che pompa ogni anno 170 milioni di metri cubici di aria condizionata e depurata[215].
Eccezionali misure di sicurezza la proteggono sia esternamente che internamente: alti recinti in muratura, ricoperti di filo spinato attraversato da corrente elettrica, 700 guardie armate armate di unità cinofile appositamente addestrate per ispezionare ogni persona ed ogni veicolo che varchi l'ingresso dell'Agenzia.
All'interno, esistono squadre specifiche per ogni evenienza, come le *Special Operations Units*, addestrate per fronteggiare attacchi alla sicurezza come un attacco terroristico, oppure come l'*Emergency Reaction Team*, pronte per emergenze come un incendio.
Tutto il personale, dal direttore fino all'ultimo addetto, è schedato dal punto di vista della segretezza fino ai parenti di terzo grado, ed è sempre obbligatorio esporre un cartellino, di colore differente, che indica i settori ed i livelli di segretezza a cui si può accedere.
I lavoratori all'interno dell'agenzia rappresentano una combinazione unica di specialità: analisti, ingegneri, fisici, matematici, informatici, ricercatori, managers, specialisti di sistemi, interpreti e traduttori (ogni giorno vengono analizzati documenti e messaggi in 95 lingue differenti) sono solo alcuni tra le varie attività che si svolgono al suo interno[216].
Il cuore della NSA è rappresentato dal palazzo centrale, l'Operations Building. La struttura dell'edificio è lo stato dell'arte dell'architettura moderna: esternamente, è ricoperto da uno strato di rame e da vetri neri, a prova di proiettile, composti da uno strato esterno oscurante, un'intercapedine di 12 centimetri per isolare acusticamente l'edificio, un ulteriore pannello di rame.
Questo insieme di materiali è stato progettato per impedire a qualsiasi suono o segnale, come le radiazioni elettromagnetiche emesse dai computer di fuoriuscire dall'edificio: conosciuto con il nome in codice di "Tempest", questa tecnica di rivestimento protettiva in rame e vetro è utilizzata nella maggior parte degli edifici allo scopo di impedire ad eventuali spie di intercettare qualunque tipo di emissione proveniente dall'interno delle strutture[217].
Tutte questi particolari precauzioni per garantire la massima sicurezza hanno valso all'agenzia il soprannome, parafrasando le iniziali, di "Not Such Agency", mentre il personale che lavora all'interno, il quale deve rispettare rigidissime procedure comportamentali per motivi di segretezza, si è guadagnato l'appellativo di "Never Say Anything", cioè "non dire mai nulla".

---

214 Ibidem.
215 Ibidem, p. 482
216 Ibidem, p. 488.
217 Ibidem.

3. L'organizzazione e le funzioni della National Security Agency.

Una delle novità principali di questa agenzia fu l'accresciuto potere e le maggiori responsabilità che le si attribuirono rispetto a quelle che in passato si erano concesse all'AFSA.
Un'altra significativa novità fu la sua minore dipendenza al Dipartimento della Difesa: la *National Security Agency* non sarebbe stata direttamente subordinata al Segretario della Difesa, ma quest'ultimo, al contrario, avrebbe delegato le sue responsabilità in materia COMINT al direttore dell'agenzia.
Egli sarebbe stato non solo indipendente da ogni forma di controllo e restrizione, ma avrebbe avuto la responsabilità dell'intero settore COMINT degli Stati Uniti a qualsiasi livello e settore.
Verso la metà degli anni '50 il Presidente Eisenhower e il suo staff cominciarono ad accorgersi delle potenzialità della NSA.
Una commissione della Casa Bianca fu incaricata di analizzare le attività del governo federale, compresa la comunità di intelligence, ed il responso a proposito fu proprio di aumentare le risorse destinate alla National Security Agency: "considerazioni sulla spesa dell'agenzia devono essere accantonate" raccomandò la Commissione ad Eisenhower, e "uno sforzo uguale almeno a quello del Manhattan Project[218] dovrebbe essere immediatamente attuato"[219] al fine di migliorare la produzione dell'intelligence dei segnali.
Il Presidente, il Pentagono, il Consiglio per la Sicurezza Nazionale si resero conto che la NSA era indispensabile *all'intelligence*, poteva diventare l'arma segreta per il futuro, l'occhio e l'orecchio dell'America sul mondo.
Tale risorsa non doveva essere assolutamente trascurata, era al contrario necessario farne la principale e più accurata agenzia di spionaggio del paese: il *budget* destinato alla *National Security Agency* crebbe fino ad oltrepassare i 500 milioni di dollari, più della metà del budget destinato all'intero apparato di *intelligence* degli Stati Uniti[220].
Il compito assegnato alla NSA consiste tuttora in due funzioni principali: intercettare le comunicazioni straniere e proteggere le comunicazioni del Governo americano.

---

[218] 13 Il Manhattan Project era il nome in codice per chiamare il progetto che, durante la seconda guerra mondiale, sviluppò e creò la prima bomba atomica. Il progetto cominciò nel più assoluto riserbo nel 1939 quando il fisico ebreo Albert Einstein, rifugiatosi negli Stati Uniti per fuggire dalla politica antisemita di Hitler, avvertì Roosevelt che gli scienziati nazisti stavano studiando la fisica atomica per creare un'arma di straordinaria potenza. Il Presidente autorizzò un imponente programma segreto anglo-americano, escludendo i Sovietici, per produrre la bomba atomica. Nel 1942 gli scienziati riuscirono ad avere una reazione atomica controllata ed acquisirono le conoscenze necessarie per costruire la bomba. Nel 1945 il Manhattan Engineering District terminò le due prime bombe atomiche, che vennero sperimentate il 16 luglio 1945 nel deserto nei pressi di Alamogordo, Nuovo Messico, dando il via all'età atomica. Al progetto presero parte più di 120.000 persone e furono spesi quasi due miliardi di dollari di allora.
[219] Cfr. Bamford, Body of Secrets, op. cit., p. 356.
[220] Ibidem.

La prima funzione, pertanto, consta nell'intercettare, con i propri mezzi o con l'ausilio di quelli dei quattro alleati, le comunicazioni straniere e nazionali di qualsiasi tipo (telegrafico, telefonico, telex, ed oggi anche e-mails), di crittoanalizzare il materiale ottenuto, cioè decifrare gli eventuali codici crittografici utilizzati per la cifratura, tradurlo ed infine analizzare e valutare il contenuto del traffico intercettato per fini politici, militari ed economici[221].
La National Security Agency non ha, pertanto, nessun carattere operativo, nessuna operazione può essere intrapresa di propria iniziativa in base a quello che si è scoperto: essa deve svolgere solo un'attività di intelligence "passiva", il suo unico compito consiste nel trasmettere le informazioni alle responsabili autorità governative le quali le valuteranno.
La seconda mansione dell'agenzia di Fort Meade è quella di proteggere le comunicazioni del Governo degli Stati Uniti, dei suoi vari dipartimenti e delle altre agenzie d'intelligence, come la CIA, per evitare che un paese potenzialmente ostile possa impossessarsi del contenuto dei messaggi inviati.
La sicurezza delle comunicazioni è pertanto una responsabilità della NSA.
Queste sono solo una parte delle capacità dell'agenzia: il contrammiraglio Mario de Arcangelis, uno dei più esperti conoscitori di guerra elettronica, nel suo libro *La storia dello spionaggio elettronico* illustra pienamente le potenzialità e le capacità che la National Security Agency possiede, le quali evidenziano i progressi che quest'agenzia ha compiuto dalla sua nascita ad oggi :"...la NSA conosce giorno per giorno in che luogo si trova ogni alto esponente dell'Unione Sovietica, i nomi di tutti i piloti militari russi distaccati nei reparti operativi in Europa ed in Estremo Oriente, i loro nominativi radio, il numero distintivo scritto sui fianchi dei loro aerei. La NSA conosce l'esatta posizione di ogni sommergibile nucleare sovietico nel suo punto di agguato, di tutte le località dell'Unione Sovietica in cui sono installati i missili intercontinentali, l'ubicazione di ogni unità terrestre, dal corpo d'armata al battaglione, i nomi dei comandanti, ecc. L'intercettamento e la goniometria delle emissioni radio sovietiche consentono alla NSA di conoscere con esattezza l'intero schieramento della difesa aerea sovietica, le tattiche impiegate dagli aerei intercettori ed i loro tempi d'intervento, e di valutarne, così, l'efficienza e la prontezza operativa. Dalla NSA sono stati escogitati metodi per registrare il timbro della voce nel corso delle trasmissioni radio dei piloti militari russi e di poterli così riconoscere uno per uno pur nell'intrecciarsi dei messaggi dei vari operatori radio in volo. Il personale addetto al settore ELINT (ELectronic INTelligence, è la raccolta di emissioni radar provenienti da un paese potenzialmente ostile) della NSA è persino capace di ricostruire un radar russo dopo averne intercettato le emissioni elettromagnetiche per un certo lasso di tempo"[222].
Le capacità dell'agenzia di Fort Meade e dei suoi partner erano e sono tuttora impressionanti, e le loro potenzialità aumentano anno dopo anno.
Lo sviluppo che ha avuto la tecnologia negli ultimi cinquant'anni è stato impressionante, rendendo possibile all'uomo di raggiungere mete impensabili

[221] Cfr. De Arcangelis, La storia dello spionaggio elettronico, op. cit., p.37.

[222] Ibidem, p.34.

solo pochi anni fa le quali hanno influenzato ogni settore dell'attività umana, compreso quello dei servizi di intelligence, soprattutto quello dell'intelligence delle comunicazioni, che fa un ampio uso della tecnologia.
Difatti, tecnologie innovative hanno dato la possibilità di compiere grandi progressi in questo settore, soprattutto in quello relativo ai servizi SIGINT, i quali si basano appunto su un impiego estensivo della tecnologia.
Progressi che non solo hanno permesso di cogliere, e spesso vincere, nuove sfide, ma che hanno anche dato la possibilità di creare impressionanti apparati adibiti allo spionaggio delle comunicazioni.

4. L'avvento delle nuove tecnologie.

L'intercettamento delle comunicazioni che la National Security Agency otteneva grazie alle proprie basi ed a quelle degli alleati era solo un passaggio dell'*intelligence* delle comunicazioni.
In effetti esso rappresenta solo un primo passo nel processo dell'attività COMINT: qualora si fosse entrati in possesso di un messaggio, il passaggio seguente sarebbe stata l'operazione di crittoanalisi, cioè decifrare il messaggio, cifrato tramite un codice di crittografia, e riportarlo al suo stato originale, "in chiaro".
Una volta decifrato, il messaggio doveva essere tradotto e, successivamente, analizzato.
Questa operazione consisteva nell'interpretare e valutare il messaggio o la comunicazione, ed ottenere dati, informazioni, notizie riguardanti altri Paesi, od anche singoli potenzialmente, ma non necessariamente, ostili al fine di ottenere un vantaggio per i propri interessi militari, diplomatici e politici.
L'elaborazione del materiale acquisito veniva effettuato dalle agenzie stesse.
Per effettuare tale attività esse necessitavano di appositi calcolatori per elaborare con precisione il materiale a disposizione.
Era infatti praticamente impossibile gestire una mole di messaggi, comunicazioni e notizie così elevata basandosi solo sulle capacità umane: solo per decifrare il codice utilizzato dalla Germania per cifrare i propri messaggi i servizi COMINT inglesi avevano impiegato anni e vi avevano preso parte centinaia dei migliori crittologi dell'epoca.
L'avvento dei sistemi informatici rese il lavoro più rapido e preciso, in quanto permetteva di compiere un numero di operazioni matematiche e di immagazzinare un volume di dati impressionante per quel periodo.
Il primo computer adibito all'attività SIGINT lo ottenne proprio la NSA nel 1958 e fu soprannominato "ATLAS"[223]: esso rappresentò la nuova frontiera degli elaboratori di dati, in grado di memorizzare 16.384 parole, cifra straordinaria per l'epoca.
Il calcolatore riusciva a immagazzinare ed elaborare una elevata quantità di dati, provando tutte le combinazioni possibili per decifrare i codici crittografici dei

[223] Ibidem.

messaggi nemici, riducendo notevolmente i tempi.
Bisogna considerare, però, anche il rovescio della medaglia di questa evoluzione: se i computer hanno senza dubbio fornito dei vantaggi alla decrittazione di un messaggio, essi hanno concesso gli stessi vantaggi a coloro che cifrano lo stesso messaggio, in quanto ha reso possibile utilizzare combinazioni sempre più complesse.
Prima dell'avvento dei computer, le agenzie di intelligence delle comunicazioni utilizzavano macchine cifranti convenzionali: quando si voleva decrittare una comunicazione era necessario, innanzitutto, individuare quei gruppi di cifre o di numeri che ricorrevano più frequentemente e che corrispondevano a determinate parole standard e frasi di sicuro significato, come quelle che indicavano la data, l'ora o il fuso orario, le quali erano abitualmente utilizzate.
Basandosi su questi supposizioni, era possibile cercare di "rompere" il codice utilizzato per cifrare il codice, si cercava cioè di ricostruire il codice utilizzato partendo da lettere cifrate le quali corrispondevano a parole di cui si conosceva il significato.
Inoltre, i computer permettevano di classificare una quantità enorme di dati ed informazioni, velocizzando le operazioni sia di archiviazione e di recupero nel caso fosse stato necessario confrontarli con altri nel futuro.
Con l'ausilio dei computer, tutte queste operazioni venivano svolte automaticamente e molto più velocemente, riducendo inoltre il margine di errore: paragonate all'attività umane, i computer erano in grado di eseguire operazioni che, se compiute solo qualche anno prima nella *Black Chamber* o a *Bletchley Park* avrebbero richiesto oltre 200.000 persone.
Nel giro di pochi anni, i progressi dei computer sarebbero stati così elevati che ciascuno di essi sarebbe stato in grado di effettuare il lavoro equivalente a quello di cinque milioni di crittoanalisti[224].
La NSA americana, il GCHQ inglese, il CSE canadese, il DSD australiano GCSB neozelandese compresero pertanto come i computer aprissero nuovi orizzonti per quanto riguardava i servizi COMINT e, più in generale, ogni settore dell'intelligence.
ATLAS fu considerato un'esperienza assolutamente positiva e si comprese ben presto che questa era la strada giusta da percorrere: James Killian, un professore dell'Università di Harvard, in un suo studio sulla possibile vulnerabilità degli Stati Uniti in caso di un attacco a sorpresa, concluse che il 90% degli attacchi di guerra sarebbero stati captati dall'intelligence dei segnali elettronici.
Ma, egli precisò, dal momento che un un attacco nucleare può essere lanciato in pochi minuti, era assolutamente necessario per la sicurezza nazionale velocizzare le capacità di intercettamento, decifrazione ed elaborazione dell'intelligence degli Stati Uniti[225].
Da allora in poi, la priorità dei servizi SIGINT sarebbe stata la velocità.
L'industria informatica americana diventò il miglior cliente della *National Security Agency*, la quale cominciò a richiedere computer dalle capacità sempre più potenti per soddisfare le esigenze che, giorno dopo giorno, si facevano più

[224] Ibidem, p.39.
[225] Cfr. BAMFORD, *Body of Secrets*, op. cit., p. 582.

impegnative.
Nel 1957 il Presidente Eisenhower approvò un programma di sviluppo e ricerche informatiche da applicare all'intelligence delle comunicazioni, il "Programma Lightning" allo scopo di creare un sistema di computer collegati tra loro aventi una capacità di memoria ed una velocità di elaborazione dati dieci volte maggiore al più potente computer esistente all'epoca.
Il programma fu praticamente una gara per aggiudicarsi il prestigioso, e remunerativo appalto, competizione alla quale parteciparono le maggiori industrie informatiche americane, come Honeywell, IBM, General Electric, Philco, RCA, oltre ad alcune tra le più importanti università americane, come il MIT, il Massachussets Institute of Technology[226].
Il primo innovativo computer, dal nome in codice di "Harvest", fu consegnato alla *National Security Agency* nel 1962, rappresentando la macchina più evoluta tra tutte quelle esistenti al mondo: rispetto ai computer precedenti, questo era almeno cinque anni più avanti del più potente computer disponibile nel settore commerciale civile.
Le industrie americane avevano progettato e realizzato per l'agenzia un gioiello della tecnologia: durante la seconda guerra, la macchina per decifrare i codici nemici in dotazione alla marina degli Stati Uniti, soprannominata "Bombe", era in grado di effettuare operazioni ad un ritmo di 1.300 caratteri al secondo.
In altre parole, effettuava 1.300 differenti tentativi ogni secondo, cercando la chiave, cioè il codice giusto per decifrarlo.
Con Harvest la velocità era stata aumentata al ritmo di tre milioni di caratteri al secondo, un aumento del 230.000 per cento: ogni secondo, pertanto, la NSA era in grado di attaccare un codice provando tre milioni di chiavi differenti.
Questa sorprendente tecnologia permetteva di effettuare un'operazione assolutamente innovativa: se prima bisognava aspettare di decifrare un messaggio per comprenderne il contenuto, rendendo il compito eccessivamente lungo nel caso si stesse cercando qualcosa di specifico, ora era possibile, già durante l'operazione di decifrazione, basare l'elaboratore per una ricerca di messaggi dal contenuto particolarmente rilevante.
Era sufficiente impostare la decifrazione utilizzando parole chiavi di particolare importanza, come nomi di leader politici o comandanti militari, parole che avrebbero permesso agli operatori di indirizzare l'operazione di decifrazione verso un soggetto di particolare interesse, avviando una ricerca più veloce e più precisa ed ottenendo così un risultato finale più vicino alla domanda iniziale.
Harvest era in grado di effettuare questa operazione su un gruppo di 7.075.315 messaggi, ciascuno di essi lungo 500 parole, decifrandoli ed estrapolando quelli che contenevano anche solo una delle 7.000 parole o frasi contenute nella "watch list", la lista contenente parole chiavi di particolare importanza[227].
Harvest fu un successo per l'*intelligence* delle comunicazioni degli Stati Uniti, e fu utilizzato senza interruzione per 14 anni, fino al 1976, quando l'agenzia passò ad un sistema più avanzato e potente, il computer CRAY-1.
Progettato da un'industria informatica di Chippewa Falls, Wisconsin, CRAY-1

---

[226] Ibidem, p. 583.

[227] Ibidem, p. 587.

era in grado di effettuare da 150 a 200 operazioni al secondo, con una capacità di memoria capace di analizzare 320 milioni di parole al secondo, l'equivalente di 2.500 libri di 300 pagine ciascuno[228].
Il CRAY-1 rimase in dotazione alla NSA, la quale lo utilizzò allo scopo di decrittare e decifrare messaggi in codice, cioè crittati, fino al 1983, quando i progressi e le nuove scoperte dell'industria informatica permisero la creazione del suo successore, il CRAY X-MP.
Dal peso di sei tonnellate, questo elaboratore conteneva al suo interno più di 70 kilometri di fili collegati a due microprocessori, i quali lavoravano in parallelo.
Questo innovativo sistema quintuplicò la velocità del CRAY X-MP rispetto al suo predecessore[229].
Questi due processori paralleli rappresentarono la chiave di svolta dell'intero sistema COMINT, cioè l'*intelligence* delle comunicazioni basato sull'utilizzo di elaboratori elettronici: il programma *Strategic Computing Program* sviluppato dall'agenzia DARPA (*Defence Advanced Research Projects Agency*) arrivò a collegare fra loro, ed a farli lavorare contemporaneamente e congiuntamente, più di 1000 processori, dato strabiliante se si pensa che nei primi anni '80 il mercato dell'informatica era pressochè agli albori[230].
Il CRAY X-MP venne sostituito negli anni seguenti da versioni sempre più potenti e sempre più sorprendenti che permettevano di ottenere risultati eccellenti nel campo della crittografia e delle crittoanalisi, come per esempio attaccare un codice utilizzando algoritmi di decifratura ad un ritmo compreso tra i 2 ed i 4 miliardi di tentativi al secondo.
Ma i campi delle scienze informatiche e matematiche non sono gli unici nei quali la NSA eccelle a livello mondiale: basti pensare che già nella seconda metà degli anni '80 si utilizzava, allo scopo di raffreddare i circuiti di questi supercomputers, dei liquidi speciali, una sorta di sangue artificiale denominato "Bubbles", che scorreva attraverso i processori, all'interno degli elaboratori.
La NSA stava contemporaneamente crescendo al suo interno: in effetti, il settore ricerca e sviluppo era basato prevalentemente sulla collaborazione con industrie esterne private, come la IBM o il Cray Research.
Per motivi di sicurezza, era pertanto necessario sviluppare maggiormente il settore interno dell'agenzia stessa, evitando così di appoggiarsi ad aziende esterne, le quali potevano rappresentare una sorta di crepa nell'impenetrabile muro di segreti della communità di intelligence statunitense.
La struttura, superfluo dire *top secret*, preposta a questo fu chiamata SRC: *Supercomputer Research Center*.
Il SRC ha in programma di realizzare entro il 2006 i Blue Gene, computer 500 volte più veloci degli attuali computer che la NSA stessa utilizza, in grado di compiere operazioni a velocità tali che hanno necessitato di terminologie *ad hoc*, come petaflop, cioè un milione di miliardi al secondo, raffreddati da una

---

228 Ibidem, p. 591.
229 Ibidem, p. 592.
230 Oggigiorno la NSA dispone di computer che utilizzano quasi un milione di processori collegati.

turbina a gas delle dimensioni di un motore di un aereo a reazione.
Per ottenere un paragone con le macchine che utilizziamo al giorno d'oggi, tali computer saranno 2 milioni più veloci degli attuali personal computer[231].
Ma gli obiettivi che la NSA ha intenzione di raggiungere non si fermano a Blue Gene: le velocità che si vogliono acquisire come standard per le loro macchine hanno nomi sconosciuti quasi come i risultati che offrono.
Basti pensare che collegando fra loro vari Blue Gene, il progetto è di arrivare a velocità per attaccare messaggi crittografati nell'ordine di 10^{24} operazioni al secondo, o yottaflop. Un messaggio codificato con il sistema standard DES, per esempio, potrà venire decifrato in meno di 5 minuti[232].

[231] 26 Cfr. Bamford, Body of Secrets, op. cit., p. 608.
[232] 27 Ibidem.

Capitolo Dodicesimo

IL CLIPPER CHIP

SOMMARIO: 1. Il *Clipper Chip*. - 2. L'*Escrowed Encryption Standard*. - 3. L'Operazione *Shamrock*. - 4. Il funzionamento del *Clipper Chip*. – 5. *Clipper Chip* e *privacy*.

1. *Il Clipper Chip*.

Nel 1987, con l'emanazione del *Computer Security Act*, il Congresso degli Stati Uniti d'America conferì al *National Bureau* of *Standards*[233] la responsabilità di garantire la sicurezza dell'infrastruttura tecnologica americana e, in particolare, di definire gli *standard* di crittografia per le comunicazioni ai quali aderire, mansione che fino ad allora apparteneva alla *National Security Agency*, l'agenzia di *intelligence* adibita all'intercettazione ed alla sicurezza delle comunicazioni[234].
Il motivo di questo cambiamento era duplice: da un punto di vista morale e sociale, il trasferimento era stato invocato da vari gruppi per la difesa delle libertà civili, i quali non vedevano di buon occhio l'ingerenza di un'agenzia del governo statunitense in un settore delicato come la *privacy* e la sicurezza delle comunicazioni, a maggior ragione se tale agenzia faceva parte della *community* dello spionaggio degli Stati Uniti d'America.
Ma tale trasferimento non era stato fatto solo per accontentare le richieste, per quanto legittime, di cittadini americani interessati alla loro *privacy*: ciò era stato compiuto in quanto, per citare le parole del Senatore Patrick Leahy, "il business USA non ama particolarmente che sia la NSA a dettare gli standard. Gli interessi che la NSA persegue in materia di sicurezza informatica non sono gli stessi interessi che gli uomini d'affari perseguono"[235].
I compiti della *National Security Agency* si possono riassumere in due attività differenti, ma tra loro strettamente collegate: la prima è quella di intercettare e decrittare le comunicazioni di molteplici soggetti, siano un cittadino straniero (per l'intercettazione di comunicazioni di cittadini americani la competenza, almeno in teoria, spetterebbe all'FBI), un terrorista, un narcotrafficante o un soldato nemico, e da queste intercettazioni ricavare materiale utile, in gergo "fare un'attività di intelligence", e fornirlo al governo americano, o a dipartimenti ed agenzie che ne abbiano fatto richiesta, come la CIA, la principale agenzia di spionaggio degli Stati Uniti d'America, o il DOD, il

---

233 Il *National Bureau of Standards* era il precursore dell'odierno NIST (*National Institute for Standards and Technology*).
234 Cfr. S. LEVY, *Crypto – Secrecy and privacy in the new code war*, Allen Lane - The Penguin Press, 2000, p. 182.
235 Cfr. S. LEVY, *op.cit.*, p. 182.

Dipartimento della Difesa.
Il secondo compito è quello di garantire al Governo americano (oltre a tutti i suoi dipartimenti, enti, agenzie, ecc..) la sicurezza delle comunicazioni, cioè rendendole assolutamente indecifrabili, qualora esse vengano intercettate, tramite l'utilizzo di codici di crittografia talmente elevati, matematicamente parlando, da rendere pressochè impossibile una loro decifrazione e, di conseguenza, una loro effettiva comprensione[236].
Fino al 1987, lo *standard* di cifratura utilizzato era il *Data Encryption Standard*, DES, un sistema di crittografia sviluppato dalla IBM, certificato e standardizzato a livello internazionale il quale aveva garantito una buona sicurezza in passato, ma cominciava a risultare vulnerabile in virtù dei progressi che si stavano compiendo nel campo dell'informatica e della crittoanalisi, cioè la pratica di attaccare un codice e di renderlo "chiaro", cioè comprensibile[237].
Per garantire pertanto la sicurezza delle comunicazione, il Governo impose la realizzazione di un nuovo *standard* di cifratura che si sarebbe andato a sostituire all'ormai obsoleto DES.
Le preoccupazioni in materia di sicurezza ed invulnerabilità erano accompagnate ad altri fattori, meno evidenti all'opinione pubblica ma di notevole importanza se consideriamo i soggetti coinvolti, cioè il Governo americano e le sue agenzie di intelligence.
In effetti, il Governo era preoccupato che la vulnerabilità del sistema DES potesse provocare un *gap* nel settore dell'*information security*, mettendo in moto, di conseguenza, una fuga delle aziende operanti nel settore delle comunicazioni verso prodotti più efficaci di derivazione non governativa.
Questa migrazione avrebbe così pregiudicato tutto il sofisticato sistema di intercettazioni e decrittazioni utilizzato dalle agenzie di *intelligence* ed dagli uffici federali investigativi americani nello svolgimento dei loro quotidiani compiti per preservare l'ordine pubblico e la sicurezza nazionale, in quanto il Governo americano avrebbe perso la sua supremazia nel settore della crittografia sia in termini di qualità, cioè il possesso e la conoscenza della crittografia più forte, sia in termini di quantità, cioè il fatto che tale crittografia non sarebbe più stato il sistema *standard* usato in ogni parte del mondo[238].
Il *National Institute for Standards and Technology* contattò la NSA, affinchè sviluppasse un nuovo sistema di crittografia, sofisticato e forte a tal punto da garantire l'assoluta sicurezza delle comunicazioni non solo del Governo degli Stati Uniti d'America, ma anche dei singoli cittadini.
Tale sistema, però, essendo sviluppato da un'agenzia governativa, avrebbe permesso all'agenzia stessa, su ordine del Governo, di 'rompere' il codice e di decifrarne il contenuto, permettendo così alle forze dell'ordine di mantenere una sorta di controllo nel settore delle telecomunicazioni.
Questo punto è fondamentale per capire la duplicità delle intenzioni del Governo statunitense in questo settore, e del perché la crittografia sia considerata alla stregua di un'arma, pertanto sottoposta ad una rigida

---

236 Cfr. S. LEVY, *op. cit.*, p. 228.
237 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *Segreti spie codici cifrati – Crittografia: la storia, le tecniche, gli aspetti giuridici*, Milano, Apogeo, 1999, p. 17.
238 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *op. cit.*, p. 190.

regolamentazione in materia di esportazioni proprio come lo sono i prodotti di carattere bellico. Gli Stati Uniti d'America necessitano di una crittografia forte allo scopo di proteggere le loro comunicazioni, garantendo così ai cittadini onesti e rispettosi della legge il diritto alla *privacy* ed alla riservatezza delle proprie comunicazioni, difendendo inoltre l'economia degli Stati Uniti d'America (la crittografia è assolutamente necessaria in materia di transazioni commerciali e per evitare tentativi di spionaggio industriale, per esempio).
La crittografia, però, è un'arma a doppio taglio, in quanto le possibilità che offre potrebbero essere utilizzate per fini illeciti: tramite tale sistema, in effetti, i criminali potrebbero comunicare liberamente tra di loro via telefono o posta elettronica, senza che le forze dell'ordine possano tenere sotto controllo le loro comunicazioni.
Per ovviare a ciò, il NIST, su ordine del Governo americano, incaricò la NSA, la più importante agenzia americana (e mondiale) nei campi della crittografia e della crittoanalisi, di sviluppare un sistema più sicuro del DES, indecifrabile se non dal Governo USA stesso.

2. L'*Escrowed Encryption Standard*.

Il risultato fu il cosiddetto EES (*Escrowed Encryption Standard*) basato su *Skipjack*, un algoritmo a doppia chiave da utilizzare con un apposito microprocessore, il *Clipper* per la telefonia, il *Capstone* per i computer.
Tale strumento sarebbe stato installato nei telefoni o nei computer direttamente dalle aziende produttrici, le quali diventavano a tutti gli effetti collaboratori delle agenzie di *intelligence* americane, come era già avvenuto per le principali compagnie telefoniche americane.
In effetti, questo sistema era una medaglia a due facce, o meglio, trattandosi di crittografia una spada a due lame (secondo l'interpretazione del Governo americani la crittografia era da considerarsi come un'arma): in effetti, mentre tale strumento sarebbe servito a proteggere le comunicazioni, avrebbe contemporaneamente permesso al governo americano, tramite agenzie preposte, di decrittarle, adducendo motivi di prevenzione e repressione del crimine e per esigenze di sicurezza nazionale.
Per rendere possibile ciò, il *Clipper chip* utilizzava un sistema cosiddetto di "Key Escrow": si basava su due *keys*, due chiavi di 80 *bit* ciascuna, contenenti gli algoritmi di crittazione, i quali consentono di crittare il messaggio e, al contempo, di decrittarlo[239].
Queste due chiavi erano la garanzia della *privacy* dei cittadini americani.
Ad ogni telefono si assegnava un apposito *chip*, il quale conteneva le due chiavi, entrambi assolutamente indispensabili per decrittare il messaggio.
Queste due chiavi venivano separate e depositate presso due "key escrow"[240]

---

[239] Cfr. Sito web del *Center for Democracy & Technology*", http://www.cdt.org, pagina Encryption - U.S. Encryption Policy, "Clipper Chip" (Escrowed Encryption Standard): April 16, 1993.
[240] Il verbo *To Escrow* si può tradurre letteralmente dall'inglese all'italiano con *"consegnare qualcosa a qualcuno, dare qualcosa in consegna a qualcuno"*.

database differenti, e solo la loro eventuale combinazione avrebbe permesso la decifrazione di un messaggio crittato: se anche si possedeva una delle due chiavi, essa era inutile ed era necessario procurarsi anche l'altra chiave complementare.
I due agenti depositari delle chiavi Escrow erano stati individuati nel NIST stesso (il quale opera all'interno del Dipartimento del Commercio), e nell'*Automated Systems Division* (ASD) del Dipartimento del Tesoro[241], scelti per la loro competenza e capacità nel trattamento e nella salvaguardia di informazioni delicate.
Questi due agenti dovevano agire nel rispetto di rigide procedure allo scopo di garantire la sicurezza dei componenti delle chiavi in loro possesso e il loro rilascio sono nei casi previsti dalla legge e dietro una specifica autorizzazione.
Essi sarebberro stati responsabili della conservazione delle *keys*: per ogni singolo *chip*, un agente ne avrebbe conservato una parte, mentre l'altra metà sarebbe stata custodita dall'altro agente.
Entrambi gli organismi avrebbero rilasciato le chiavi in loro possesso unicamente ad agenzie governative autorizzate ad entrarne in possesso, e comunque, per ottenere una chiave, era necessario che l'agenzia governativa che ne facesse richiesta (la CIA, l'FBI o l'NSA, per esempio) ottenesse l'autorizzazione da parte del governo americano, e che la conseguente attività di intercettazione si svolgesse nel rispetto della legalità e delle leggi federali in materia di intercettazioni.
Il sistema *Clipper Chip* doveva in ogni caso sottostare alle regole vigenti in materia di spionaggio che regolano, limitano ed autorizzano le agenzie governative nelle loro attività di intelligence[242].
La procedura per ottenere le chiavi consisteva in una richiesta scritta da parte di un'agenzia governativa autorizzata da presentare ai due agenti, NIST e ASD; tale richiesta era obbligatoria e serviva a: identificare l'agenzia responsabile dell'attività di intercettamento delle comunicazioni e chi sarebbe stato oggetto di tale attività; assicurare la liceità dell'intercettazione da parte dell'agenzia; specificare la provenienza dell'autorizzazione dell'intercettazione e la sua durata; specificare il numero seriale del *chip* di crittazione che viene decrittato mediante l'unione delle due *key-escrow*. In ogni caso, il procuratore legale coinvolto in questa attività ha l'obbligo di assicurare ai due agenti che rilasciano le chiavi che tutta l'operazione si stia svolgendo nel rispetto della legge e dietro una preventiva autorizzazione[243].
Per effettuare un controllo più capillare delle comunicazioni, già dal 1945 la *Armed Forces Security Agency*, e più tardi la *National Security Agency*, aveva cominciato e gestito un programma per intercettare le comunicazioni non solo in entrata ed in uscita dagli Stati Uniti d'America, ma anche quelle che avvenivano all'interno del Paese stesso.

---

241 Cfr. Comunicato Stampa Department of Justice, *"Attorney General makes key escrow encryption announcements"*, AG (202) 616-2771, 4 febbraio 1994.
242 Ibidem.
243 Cfr. Comunicato Stampa Department of Justice, op. cit., AG (202) 616-2771, 4 febbraio 1994.

3. L'Operazione *Shamrock*.

Il programma, dal nome in codice di "Operazione Shamrock", prevedeva che le maggiori compagnie telefoniche americane permettessero alla AFSA ed alla NSA l'accesso al traffico da loro gestito, e, sovente, erano le compagnie stesse a fornirlo.
Dal settembre 1945, le tre principali compagnie telefoniche degli Stati Uniti d'America, la ITT Communications, la Western Union e la RCA Communications (le quali gestivano quasi tutto il traffico telefonico americano), presero parte a questo programma illegale e passarono ogni giorno all'intelligence americana microfilm contenenti copie di tutti i telegrammi spediti da ed all'interno degli Stati Uniti d'America[244]. Questo sistema progredì ulteriormente quando le compagnie telefoniche cominciarono a registrare il traffico da loro gestito su nastri magnetici, caratteristica che permetteva all'agenzia di analizzare tutto questo materiale attraverso il potente sistema Harvest.
Questo computer permetteva di avviare una ricerca basata su specifiche parole chiave, frasi, mittenti o destinatari, persino una loro combinazione: attraverso questo efficace sistema la NSA riusciva ad ottenere ed analizzare circa 150.000 messaggi al mese.
Nel 1966, la NSA, in collaborazione con la CIA, istituì un centro, dal nome in codice di LPMEDLEY[245] preposto unicamente alla gestione del materiale Shamrock: la sede di questa nuova struttura era localizzata in *Lower Manhattan*, New York, proprio di fronte agli uffici delle tre compagnie telefoniche.
Nel 1975, Il direttore della NSA Lew Allen testimoniò ed ammise che la NSA aveva condotto il Progetto Shamrock e, durante la sua attività dal 1952 al 1974, intercettò, analizzò e trasmise a FBI e CIA ed al Dipartimento delle Difesa le comunicazioni private riguardanti oltre 75.000 cittadini americani e 1.690 organizzazioni, le quali condussero a più di 3.900 rapporti investigativi[246].
Il sistema utilizzato nel passato per intercettare le comunicazioni dei cittadini era abbastanza semplice, anche perché in quegli anni la maggior parte delle comunicazioni era in chiaro, non decrittate, oppure utilizzavano algoritmi di cifratura relativamente deboli.
Ma nei primi anni '90, la crittografia aveva compiuto notevoli progressi, ed il sistema che la NSA aveva ideato poteva essere considerato lo stato dell'arte del COMINT[247]: l'agenzia aveva creato un forte sistema per la crittazione delle telecomunicazioni, talmente sicuro che le aziende americane l'avrebbero inserito nei loro prodotti destinati non solo al mercato americano, ma anche ai mercati esteri. L'opinione pubblica sarebbe stata così soddisfatta dall'elevato

---

244 Cfr. J. BAMFORD, *The Puzzle Palace - Inside the National Security Agency, America's most secret intelligence organization*, Penguin Books, New York, 1983, p. 305.
245 Cfr. il sito web di P. S. POOLE, *ECHELON: America's Secret Global Surveillance Network* (sito Web visitato il 12 marzo 2001).
246 Cfr. BAMFORD, *The Puzzle Palace*, *op. cit.,* p. 381
247 COMmunications INTelligence, lo spionaggio delle comunicazioni.

grado di sicurezza che *Skipjack* avrebbe fornito, non conoscendo però l'altra faccia della medaglia di questo strumento.
Nel maggio del 1993, una associazione per la tutela dei diritti civili, la *Computer Professional for Social Responsibility* (CPSR), accedendo a documenti e materiale declassificato grazie al *Freedom of Information Act* (FOIA)[248], scopre che durante la progettazione dell'*Escrowed Encryption Standard* (EES) la NSA era riuscita nell'intento di impedire all'opinione pubblica ed alle associazioni per la difesa dei diritti civili di conoscere meglio ed esaminare in dettaglio tale progetto.[249]
In effetti, non è necessario essere esperti in materia di spionaggio delle comunicazioni per rendersi conto che il Clipper Chip è una spada a due lame, spada che il governo americano impugna e punta sui propri cittadini.

4. Il funzionamento del *Clipper Chip*.

Se esaminiamo il funzionamento del *Clipper Chip*, infatti, risulta immediatamente chiara la dualità del sistema, che rispecchia proprio la dualità della crittografia: da una parte la crittografia aiuta a proteggere la *privacy* dei cittadini onesti e fornisce all'economia un valido strumento per concludere affari e trasmettere dati in tutta sicurezza, allo stesso tempo, però, fornisce uno scudo, una sorta di protezione a criminali e terroristi.
Il governo degli Stati Uniti d'America aveva visto nel *Clipper Chip* la soluzione a questo problema: si permetteva ai cittadini rispettosi della legge l'uso della crittografia, ed allo stesso tempo se ne impediva un uso improprio ai criminali che ne avrebbero fatto uso come espediente per nascondere le loro attività illegali[250].
Il Presidente degli Stati Uniti, all'epoca Bill Clinton, raccomandò alle agenzie implicate nel progetto di creare una *policy ad hoc* per il Clipper Chip, la quale ne avrebbe regolato il suo utilizzo.
Gli aspetti più importanti che tale *policy* doveva regolare erano: la privacy dei cittadini; la capacità degli ufficiali autorizzati a procedere alle intercettazioni, le quali dovevano essere autorizzate; come tale sistema dovesse contribuire a costruire una rete delle comunicazioni efficiente allo scopo di promuovere la crescita economica e la competitività dell'industria americana nel mercato globale.
Questa sorta di lista "politically correct" mostra come il *Clipper Chip* rappresentasse una minaccia non solo per la privacy dei cittadini, come varie associazioni per la difesa dei diritti civili avevano già sottolineato (FOIA, alla quale si aggiunse l'*Electronic Frontier Foundation*) ma anche come tale sistema

---

248 Il *Freedom of Information Act* è la legge che permette l'accesso da parte dei cittadini agli atti ed ai documenti dell'amministrazione americana. Alcuni documenti, però, possono rimanere classificati qualora il governo li ritenga estremamente riservati per motivi concernenti la sicurezza nazionale.
249 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *op. cit.*, p. 191.
250 Cfr. Comunicato Stampa Department of Justice, op. cit., AG (202) 616-2771, 4 febbraio 1994.

correva il rischio di diventare un ostacolo per l'economia degli Stati Uniti d'America, in particolare per le aziende del settore.
In effetti, le aziende che producevano gli apparecchi contenenti il *Clipper Chip* erano giustamente preoccupate delle reazioni della clientela straniera: sarebbe stato arduo commercializzare un prodotto all'estero il quale, al suo interno, avesse contenuto un sistema per permettere ad agenzie di spionaggio americane di intercettare le comunicazioni che proprio quell'apparecchio rendeva sicure ed "inespugnabili".
Si acquistava un prodotto per rendere sicure le proprie comunicazioni, ma il prezzo da pagare per quella sicurezza era una sorta di cavallo di Troia che avrebbe vanificato gli sforzi per preservare la propria privacy e riservatezza delle comunicazioni.
Questa dualità era quello che i funzionari delle agenzie di *intelligence* americane avevano sempre voluto attuare, e questa volta non avrebbero dovuto agire ai margini della legalità, in quanto il *Clipper Chip* sarebbe stato un sistema assolutamente legale e rispettoso delle leggi americane.
Già nel luglio 1991, Clint Brooks, assistente del Direttore della *National Security Agency*, durante un *meeting* con l'FBI disse che "[il Clipper Chip] sarebbe stato un traguardo nazionale che avrebbe soddisfatto il bisogno di una buona sicurezza crittografica commerciale e non, proteggendo altresì gli interessi e le responsabilità di sicurezza nazionale e delle organizzazioni che sovrintendono all'applicazione delle leggi. Il termine per il raggiungimento di quel traguardo era "Nirvana".[251]
Se l'obiettivo dell'*intelligence* degli Stati Uniti d'America era il raggiungimento del cosiddetto "Nirvana della crittografia", il *Clipper Chip* rischiava di turbare i sogni di pace eterna del governo americano.
In effetti, i problemi che l'eventuale utilizzo di questo sistema comportava si possono suddividere in due fattori, ciascuno fondamentale e di grande impatto sull'opinione pubblica americana: il fattore privacy ed il fattore business.
Per quanto riguarda l'economia, il *Clipper Chip* avrebbe dovuto essere la soluzione dei contrasti tra il Dipartimento del Commercio e le aziende produttrici di *software* per la crittografia.
In effetti, il Governo degli Stati Uniti d'America considerava la crittografia, e tutti i sistemi per produrla, alla stregua di un'arma, pertanto le esportazioni internazionali di tali prodotti dovevano sottostare ad un rigido controllo federale.
Questo controllo limitava le vendite internazionali delle aziende produttrici dei software di crittografia,[252] limiti per di più di scarsa efficacia e comprensione in quanto gli Stati Uniti d'America, per quanto all'avanguardia nel settore delle tecnologie informatiche, non detenevano certo il monopolio assoluto su scala mondiale della produzione di tali tecnologie.
Inoltre, limitare il mercato internazionale di tali prodotti, avrebbe causato un proliferare del mercato nero di tali prodotti.

---

[251] Cfr. LEVY, *op. cit.*, p. 250.
[252] Cfr. LEVY, *op. cit.*, p. 246.

Questa limitazione avrebbe frenato anche lo sviluppo dell'*e-commerce*, che in quel periodo[253] stava cominciando a diventare un settore cruciale e dalle grandi possibilità per l'economia degli Stati Uniti d'America.
L'amministrazione Clinton decise di giocare la carta della morale e pose l'opinione pubblica di fronte all'eterno, e tuttora irrisolto, dilemma in materia di privacy/strumenti di controllo: "siete disposti a sacrificare vite umane, in cambio di un po' di ricchezza e meno privacy, anche se voi cittadini onesti non avete nulla da temere? La vita di migliaia di cittadini valgono aumentare del 10% la ricchezza di Bill Gates?" La risposta era ovvia[254].
Ma il *Clipper Chip* era un argomento delicato, e presentava più di un problema, i quali non si potevano risolvere facendo unicamente leva sulla morale dell'opinione pubblica americana.
Un'altra questione da risolvere era la funzionalità che il *Clipper Chip* avrebbe avuto sul mercato internazionale.
Se questo sistema di controllo delle comunicazioni americano non fosse stato globale, sarebbe stato inefficace e la sua operatività non avrebbe garantito alle agenzie di *intelligence* degli Stati Uniti d'America un valido strumento per implementare la sicurezza nazionale.
Se all'estero i consumatori non avessero avuto fiducia in questo "prodotto", l'avrebbero rifiutato.
E le stesse aziende estere non avrebbero visto di buon occhio la commercializzazione di un prodotto per la sicurezza delle comunicazioni, sicurezza che era garantita, fornita e gestita unicamente dal governo degli Stati Uniti d'America?
E comunque, sarebbe stata un'ardua impresa commercializzare un prodotto in mercati *extra*-americani delicati, come la Cina o il Medio-oriente, che avesse contenuto un *chip* tramite il quale il governo statunitense poteva ascoltare le comunicazioni.
Una soluzione poteva essere rappresentata dalla stipula di una sorta di accordi multi o bi-laterali, ma anche in questo caso come ci si doveva comportare con i Paesi che non avessero accettato? E quelli favorevoli, invece, avrebbero richiesto di entrare in possesso dei *Key Escrow* per utilizzare loro stessi il sistema *Clipper Chip*?
Il ruolo dei governi delle altre nazioni era fondamentale: essi avrebbero consentito ai loro cittadini di acquistare prodotti attraverso i quali la CIA poteva ascoltare le comunicazioni? Ovviamente no.
E se non per tutelare i diritti dei propri cittadini, almeno per impedire ad un'agenzia di *intelligence* di un Paese straniero la possibilità di accedere alla propria rete di comunicazioni senza la possibilità di apporre alcun tipo di controllo, se non quello di entrare in possesso anch'essi degli algoritmi di decifratura sui quali si basa il *Clipper Chip*, anche se in questo modo il governo degli Stati Uniti d'America avrebbe perso il controllo egemonico del sistema[255].
Una convincente soluzione a questi quesiti non venne mai data né dall'amministrazione Clinton-Gore, né dalle agenzie di intelligence degli Stati

---

253 Primi anni '90, precisamente il 1993.
254 Cfr. LEVY, *op. cit.*, p. 247.
255 Cfr. LEVY, *op. cit.*, p. 247.

Uniti d'America, né dai creatori e promotori del *Clipper Chip*:[256] a queste irrisolte problematiche, anzi, se ne aggiungevano altre concernenti la privacy dei cittadini e la riservatezza delle comunicazioni.
Molte associazioni erano già insorte contro il progetto del Clipper Chip, come il CPSR, *Computer Professional for Social Responsibility* e l'EFF, l'*Electronic Frontier Foundation*, arrivando ad un vero e proprio scontro con l'amministrazione degli Stati Uniti d'America.
Se l'amministrazione Clinton aveva cercato l'appoggio dell'opinione pubblica facendo leva sulla necessità di garantire e difendere la sicurezza nazionale, queste associazioni, coadiuvate da giornalisti e "cypherpunks", attuarono una campagna di informazione, incentrandola sulle libertà fondamentali dei cittadini, come la privacy e la riservatezza delle comunicazioni, diritti fondamentali ed inalienabili garantiti dalla Costituzione americana.
Le loro argomentazioni erano semplici quanto efficaci: "Lascereste una copia delle chiavi della vostra casa" dissero "presso la stazione di polizia locale?".[257]
Jerry Barman dell'EFF affermò che il Clipper Chip "avrebbe permesso al governo di avere le chiavi per aprire tutti i nostri lucchetti, ancor prima che qualcuno fosse accusato o sospettato di aver commesso un crimine. Questo non è tollerabile in America"[258].
Chi avrebbe permesso al governo degli Stati Uniti d'America un accesso diretto, immediato alle proprie informazioni?
L'esito di questa campagna anti-Clipper fu una sorta di boicottaggio da parte di alcune aziende che affermarono l'intenzione di utilizzare al posto dell'EES (l'*Escrowed Encryption Standard* basato su *Skipjack*, l'algoritmo a doppia chiave), l'algoritmo RSA, sistema per la crittografia creato dalla RSA *Data Security*, robusto come l'ESS ma senza alcuna possibilità di "rottura" da parte dell'intelligence americana[259].
Il doppio aspetto della *privacy* è qui ben evidente: se il Governo americano aveva domandato "ma cosa avete da nascondere se siete cittadini onesti?", che rappresenta l'esigenza di sacrificare la propria privacy per esigenze di sicurezza nazionale, la risposta "non sono affari vostri!" aveva rappresentato l'altro aspetto, cioè che i cittadini non desideravano affatto perdere i propri diritti costituzionali a causa di un "Big Brother Chip"[260].

5. *Clipper Chip* e *privacy*.

Il già precario rapporto tra la *privacy* e la sicurezza era stato ulteriormente indebolito dal progetto *Clipper Chip*, in quanto tale sistema comportava più di una problematica al riguardo.
I punti salienti da tenere in considerazione sono diversi.

---

256 *Ibidem*, pp. 247 e 251.
257 Cfr. LEVY, *op. cit.*, p. 251.
258 *Ibidem*, p. 252.
259 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *op. cit.*, p. 192.
260 Cfr. LEVY, *op. cit.*, p. 252.

Il *Clipper Chip* violava i diritti degli individui in materia di *privacy*.
Non esisteva una politica chiara ed adeguata a riguardo dell'utilizzo di tale sistema, inoltre alcuni punti non erano stati adeguatamente regolati, come la durata dell'attività di intercettazione ed i limiti all'uso delle informazioni carpite[261].
L'uso del *Clipper Chip* poteva ritorcersi contro il Governo statunitense stesso, in quanto i principali utilizzatori rimanevano pur sempre le due agenzie di intelligence, CIA e NSA, e l'agenzia federale d'investigazione, l'FBI.
Vi era il rischio di far nascere uno spionaggio nello spionaggio[262], in quanto tale sistema era gestito solo da una parte della vasta macchina governativa degli Stati Uniti d'America, e vi era il rischio di un abuso del suo utilizzo[263].
Non menzionata, inoltre, era la tutela che si offriva all'altra parte della comunicazione, cioè all'individuo soggetto dell'intercettazione solo perché si trovava in rapporti con la persona sospettata[264].
Se si intercettavano le comunicazioni di un determinato individuo, era ammissibile sottoporre ad attività di spionaggio un estraneo, magari in rapporti del tutto legali con il sospettato? [265]
L'algoritmo utilizzato per la cifratura delle comunicazioni, il cosiddetto "Skipjack", fu sviluppato segretamente dalla *National Security Agency*, e non era stata data la possibilità di testare la sua robustezza ad esperti "civili", non implicati direttamente nella comunità di *intelligence* USA, in modo da assicurare che le comunicazioni sarebbero state effettivamente sicure ed inaccessibili[266].
Il *Clipper Chip* violava i principi contenuti nel *Computer Security Act*.
Questo atto, approvato dal Congresso americano nel 1987, limitava il ruolo della NSA nello sviluppo di standard per le comunicazioni civili.
Nonostante questa legge, la NSA aveva progettato il *Clipper Chip* proprio allo scopo di utilizzarlo per attività di intercettazione di comunicazioni civili[267].
L'epilogo avvenne il 4 febbraio 1994: il Presidente Clinton dispose che l'ESS diventasse il *Federal Information Processing Standard*, lo *standard* federale per le comunicazioni telefoniche, ma grazie agli sforzi delle associazioni per la tutela dei diritti civili, le quali avevano fatto fronte comune contro questo progetto governativo unendosi nel *Digital Privacy and Security Working Group*[268], non si sancì l'uso obbligatorio del *Clipper Chip* nel settore privato.

---

261 Cfr. pagina Web *"Encryption – U.S. Encryption Policy"* del *Center for Democracy & Technology*, http://www.cdt.org (sito consultato il 10 luglio 2002)..
262 Il caso *Watergate*, per esempio, fu un caso di spionaggio avvenuto all'interno del Governo stesso degli Stati Uniti d'America.
263 Cfr. pagina web *"Encryption – U.S. Encryption Policy"* del *Center for Democracy & Technology* http://www.cdt.org (sito consultato il 10 luglio 2002).
264 Si ricordi, a questo proposito, il già citato caso SHAMROCK, nel quale l'*intelligence* degli Stati Uniti d'America intercettò le comunicazioni di migliaia di cittadini onesti, solo perché si trovavano in rapporti con persone sospettate, e di come l'attività di intercettazione si era allargata a dismisura.
265 Cfr. pagina web *"Encryption – U.S. Encryption Policy"* del *Center for Democracy & Technology*, http://www.cdt.org (sito consultato il 10 luglio 2002).
266 *Ibidem*.
267 *Ibidem*.
268 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *op. cit.*, pp. 192 e 206.

PARTE TERZA

CRITTOGRAFIA E CASI GIUDIZIARI

Capitolo Tredicesimo

IL CASO DI DANIEL BERNSTEIN

SOMMARIO: 1. Crittografia e casi giudiziari. – 2. Il caso Bernstein.

1. Crittografia e casi giudiziari.

Negli ultimi anni l'*encryption* ha rappresentato un fertile e difficile terreno di disputa che ha visto confrontarsi aspramente più parti. *In primis* il Governo degli Stati Uniti d'America e le multinazionali del settore informatico, vista anche l'importanza delle conseguenze sul settore del commercio elettronico, ma anche associazioni a tutela della *privacy* e della libertà di parola.
Le sentenze e le considerazioni, poste in essere alla luce dei casi giudiziari che si andranno ad analizzare, sono il frutto del lungo cammino ancora in corso verso una completa regolamentazione del fenomeno della crittografia; solo attraverso l'analisi di esse si potrà avere una migliore panoramica dei diversi punti di vista e delle diverse esigenze che caratterizzano tali questioni.
Per anni i programmi di 'encryption' sono stati considerati, come già abbiamo visto e come vedremo meglio in seguito, 'armi da guerra' e di conseguenza, tra i limiti imposti agli stessi, spiccava il divieto di varcare le frontiere nazionali.
Il 16 settembre 1999 la Casa Bianca, in una conferenza stampa dei Ministri della Giustizia Janet Reno, della Difesa William Cohen e del Commercio William Daley, ha annunciato un deciso cambio di direzione a riguardo, allentando, di fatto, i divieti e le restrizioni all'uso e all'esportazione dei *software* di crittografia
In realtà, alcuni divieti preesistenti non saranno affatto smorzati: in pratica, le *software house* che possono già esportare i programmi di cifratura con chiavi fino a 64 *bit*, dovranno essere espressamente autorizzate dal Governo statunitense nel caso vogliano esportare programmi più potenti con chiavi a 128 *bit*.
Condizione ulteriore ed imprescindibile consiste nel divieto di vendita, riferita ai prodotti in questione, nei confronti dei Paesi considerati a rischio di terrorismo anti-americano[269], oltre alla possibilità di vendere le stesse tecnologie esclusivamente a utenti finali.
Più che alla risoluzione delle problematiche legate al mondo della *web-economy*, il cui principio di libera circolazione delle merci rischia di essere compresso in nome della 'sicurezza' nella circolazione delle informazioni, gli Stati Uniti d'America hanno dimostrato, sin dall'inizio, maggiore attenzione nei confronti di questioni legate alla sicurezza nazionale.

[269] In particolare Corea del Nord, Cuba, Iran, Iraq, Libia, Siria e Sudan.

L'utilizzo 'normale' della crittografia dovrebbe essere infatti la chiave che apre le porte al commercio elettronico: impedire a terzi di intercettare i propri dati personali (si pensi ai numeri di carte di credito) quando essi viaggiano attraverso Internet significa, in pratica, incentivare le transazioni in Rete.
Allo stesso tempo, però, è necessario considerare, da parte del Governo statunitense, la paura da sempre manifestata e combattuta di essere 'spiati dal nemico'; in particolare, attraverso la globalizzazione della tecnologia crittografica, il timore è quello di vedere facilmente intercettati dati importanti per la sicurezza stessa degli Stati Uniti d'America.
La situazione descritta ha portato la Casa Bianca a considerare, includendola in tale *species*, la 'crittografia forte' tra le armi da guerra, su cui vige il divieto assoluto di esportazione.
In realtà questa decisione è andata a scontrarsi con gli interessi dei grandi produttori di *software* e degli operatori dell'*e-commerce*.
Le situazioni che si andranno ad analizzare attraverso le controversie giuridiche di coloro che vedono nella crittografia un indispensabile strumento tecnologico a tutela della *privacy* e della libertà di opinione rappresentano altrettanti casi che, per le problematiche in essi delineate, si porranno probabilmente come altrettanti *leading cases*.
Tempo fa, ad esempio, il giudice federale Betty Fletcher ha emesso una storica sentenza che riconosce i *software* come opere dell'ingegno, qundi protette dal Primo Emendamento della Costituzione degli Stati Uniti. Nel caso di specie, la norma che considerava i programmi di *encryption* come armi belliche non poteva essere applicata in quanto "…nessuna legge può proibire la libertà di parola".
Il caso, sul quale si tornerà tra breve, era quello di Daniel Bernstein, un matematico che, nel 1996, pubblicò in Internet le formule per la ralizzazione di un programma di crittografia e, per questo, fu accusato dal Governo di avere esportato armi da guerra.
La stessa accusa fu contestata qualche anno prima, precisamente nel febbraio del 1993, anche a Phil Zimmerman, 'colpevole' anche lui di un comportamento analogo: aver diffuso, rendendolo gratuitamente disponibile in Rete, il risultato del proprio lavoro, cioè il famoso ed utilizzatissimo *software* denominato PGP.
Dal 14 gennaio 2000 gli Stati Uniti d'America hanno comunque cambiato, almeno in parte, il proprio atteggiamento a riguardo: quello che secondo le *International Traffic Arms Regulations* (ITAR[270]), era considerato un gravissimo reato consistente nell'esportazione di materiale bellico, oggi è un diritto riconosciuto e costituzionalmente garantito.
John Yung[271], un architetto newyorchese, ha immediatamente messo alla prova le nuove regole, immettendo nella Rete, disponibile per il *download*, proprio PGP.
Da questo momento in poi, Internet è stata letteralmente invasa da *upload* e *download* inerenti a programmi analoghi; sui *forum* e sui siti specializzati è

---

[270] *International Traffic Arms Regulation*, promulgato quale implementazione dell'AECA (*Arms Export Control Act*) (in Internet all'indirizzo http://www.smdc.army.mil/FDOP/Home.html e http://www.pmdtc.org/, siti Internet consultati il 15 giugno 2002).
[271] Curatore del sito Web http://www.jya.com (sito Internet consultato il 15 giugno 2002).

aumentata considerevolmente la quantità e la qualità delle informazioni di pubblico dominio sull'argomento crittografia[272].
La nuova legge prevede che per l'esportazione dei programmi di crittaggio forte sia comunque necessaria una notifica al *Bureau of Export Administration*[273].
In realtà tale atto è stato, fino ad ora, scarsamente considerato e, al massimo, assolto mediante l'invio di *e-mail* all'indirizzo dell'organo preposto[274].

2. Il caso Bernstein.

Il Professore Daniel Bernstein era ancora un giovane matematico e studente dell'università di Berkeley quando, nel 1992, si trovò implicato, suo malgrado, in una situazione sgradevole e, per certi versi, paradossale: in quanto esperto in crittografia, desiderava discutere e diffondere, secondo l'uso e la tradizione in particolare delle università americane, le proprie ricerche con i colleghi attraverso la Rete.
Egli inviò, a tal fine, un semplice programma di crittografia nel *newsgroup* 'sci.crypt', violando, in tal modo, le rigide norme previste all'epoca dall'ITAR (e recentemente modificate).
Il programma in questione, che si chiamava 'Snuffle', era definito dallo stesso Bernstein come "zero-delay private-key encription system", quindi un vero e proprio sistema per la crittografia.
Il matematico decise di articolare il suo progetto in due rami ben distinti: da un lato, uno scritto accademico in lingua inglese intitolato "The Snuffle encryption system", dall'altro i codici sorgente scritti in C (che denominò rispettivamente "Snuffle.C" e "Unsnuffle.C" fornendo, altresì, dettagliate informazioni sulle relative operazioni di crittaggio e decrittaggio), linguaggio di programmazione *high-level*.
L'intervento della *National Security Agency* e quello, successivo, del Dipartimento di Stato, impedirono di fatto al giovane scienziato di perseverare nella distribuzione del suo *software*.
L'impedimento si basava, nelle intenzioni di chi lo pretese, sulla considerazione che qualsiasi dibattito pubblico svolto tramite Internet fosse da assimilare ad un'esportazione presentando, di conseguenza, potenziali pericoli riferiti, in particolare, alla sicurezza nazionale.

---

272 Ad esempio alla pagina Web http://www.shmoo.com/crypto/Cracking_DES/ (sito consultato il 10 giugno 2002) viene spiegato come 'crackare' l'algoritmo DES, fra i più utilizzati nell'ambito del commercio elettronico.

273 Su Internet all'indirizzo http://www.bxa.doc.gov (sito consultato il 10 giugno 2002).

274 Per quel che riguarda i programmi *open source* che fanno uso di algoritmi di crittografia robusta, il discorso cambia nel caso in cui il sorgente venga reso pubblico e non vengano richiesti diritti di *copyright*. Infatti, in tal caso, il sorgente non risulta più soggetto alle restrizioni previste per l'esportazione. In tale ambito rientra anche PGP, anche se non è classificabile come programma *open source*, ma "free for non-commercial use". In tal modo i gestori di http://www.pgpi.com non saranno più costretti a esportare i sorgenti del PGP in forma cartacea e a passarli allo *scanner*, unica soluzione che fino a poco tempo fa consentiva il passaggio dei confini americani per programmi di crittografia. In ogni caso, il sorgente del *software* che si intende esportare (o l'indirizzo di una pagina Web dove esso è disponibile) deve essere ugualmente inviato al Governo degli Stati Uniti d'America per il citato 'controllo'.

La NSA e il Dipartimento di Stato cominciarono, in nome del Governo degli Stati Uniti d'America, una guerra contro la crittografia che oggi, a distanza di molti anni, ha portato ad una situazione legislativa che, sebbene possa considerarsi molto più permissiva (nei confronti di studiosi ed utenti), presenta notevoli zone d'ombra.
Bernstein non fu però solo nel corso della battaglia legale. Il suo infatti non era un problema unicamente 'personale', legato cioè agli impedimenti imposti nei confronti dei lavori accademici e di programmazione dello stesso matematico; molto più in generale, il vero problema si riferiva ad una situazione legislativa che, di fatto, impediva a chiunque di diffondere le proprie opinioni ed il risultato del proprio lavoro in tema di crittografia.
L'*Electronic Frontier Foundation* si affiancò, dunque, allo studioso, offrendogli collaborazione e sostegno e denunciando, al tempo stesso, il governo per la violazione dei suoi diritti civili. In particolare, ciò che si riteneva inibita era la libertà d'espressione.
In senso più generale, l'EFF accusò il Governo di incoerenza, dato che la cifratura si pone quale soluzione, o comunque come strada perseguibile per la soluzione, di tanti altri problemi che normalmente riguardano uno Stato (ed, in particolare, gli aspetti legati alla sicurezza dello stesso), garantendo la riservatezza di tutti i tipi di informazione. Quegli stessi *software* che il Governo voleva rendere praticamente illegali avrebbero garantito maggiore protezione in riferimento a truffe e atti di vandalismo.
La diatriba si aprì quando a Bernstein vennero inibiti, sulla base del Regolamento ITAR, tutti gli atti di divulgazione relativi tanto al *software*, inteso quale codice sorgente, quanto alla documentazione riguardante istruzioni, algoritmi e pensiero scientifico.
Il Regolamento di cui si tratta è applicato dal Dipartimento di Stato attraverso l'ODTC (*Office of Defense Trade Control*).
Il *Bureau of Political-Military Affaires* disciplina, tra l'altro, l'importazione e l'esportazione di articoli militari dei servizi connessi alla fornitura di difesa[275].
A tal fine è redatta la USML[276] (*United States Munition List*).
Anche i sistemi *software* per la crittografia (sia forte sia debole) erano compresi in tale lista e necessitavano di una apposita licenza da parte del Governo che ne autorizzasse importazione o esportazione.
Il 30 giugno dello stesso anno Bernstein si sottomise alle decisioni indicate dal Dipartimento di Stato attuate attraverso *Comodity Jurisdiction* (CJ). In tale sede si stabiliva che Snuffle 5.0 (comprendente Snuffle.C e Unsnuffle.C), insieme alla documentazione accademica che descriveva il sistema, avrebbe dovuto essere sottoposto ad un controllo di conformità rispetto alle previsioni dell'ITAR.
L'ODTC stabilì che Snuffle 5.0 era da considerare uno strumento di difesa compreso nella "Category XIII" dell'ITAR (in particolare dell'USML) e di conseguenza necessitava, prima di essere esportato, dell'apposita licenza da parte del Dipartimento di Stato[277].

---

275 *Arms Export Control Act* 22 U.S.C. § 2778(b 2)
276 *Arms Export Control Act* 22 U.S.C. § 2778(a 1)
277 In particolare l'ODTC considerò il tutto come "stand-alone cryptographic algoritm which is not incorporated into a finished software product", e il 20 agosto 1992 informò Bernstein della

Pur obbedendo dal 2 agosto alle limitazioni poste alla sua libertà di comunicare, pubblicare, discutere con altri le proprie teorie sulla crittografia e sul suo programma, Bernstein decise di sfidare l'AECA e l'ITAR sul presupposto di una violazione, da parte degli stessi, del Primo Emendamento della Costituzione americana, relativo alle fondamentali libertà civili delle quali nessun individuo può essere spogliato.
Nel corso dell'estate 1993 Bernstein e ODTC si scambiarono copiosa corrispondenza riferita all'applicazione della licenza prescritta nell'agosto del 1992; in particolare, l'attenzione era qui rivolta alla risoluzione dei dubbi riguardanti il trattamento da riservare agli scritti accademici del matematico.
Bernstein si sottopose, quindi, ad un'ulteriore CJ nel luglio del 1993 dove la richiesta consisteva in una determinazione separata di ogni questione relativa al suo caso[278].
Nell'ottobre dello stesso anno però l'ODTC notificò a Bernstein che tutto quanto analizzato rientrava nella "Category XIII (b 1)" dell' ITAR.
Il 29 giugno 1995, già nel cuore della battaglia legale che si sta descrivendo, l'ODTC comunicò che le limitazioni imposte dal proprio CJ riguardavano solo Snuffle.C e Unsnuffle.C, chiarendo così l'esclusione dello scritto "The Snuffle Encryption System".
Infatti si sottolineò, in tale sede, come lo scritto in questione non rientrasse nella definizione di "technical data" che era necessaria per farlo rientrare nella medesima disciplina prevista e voluta per il resto del materiale[279].
La Corte[280] notò che Bernstein aveva avuto, in effetti, tutti i motivi per essere dubbioso fino a quella data e stabilì che, per questo, necessitava di una determinazione inequivocabile circa la qualificazione dei suoi scritti.
Le risposte ai dubbi dello studioso arrivarono in una comunicazione datata 26 luglio 1996 nella quale William Lowell, Direttore dell'ODTC, dichiarò di abbandonare le posizioni assunte il 29 giugno 1995, quando, cioè, decise di sottoporre lo scritto alle medesime limitazioni poste ai sorgenti di Snuffle.
Nel rispetto dei concetti di "technical data" presenti all'interno dello stesso ITAR e del USML, Lowell chiarì che gli scritti in questione non avrebbero dovuto subire limitazioni se non l'apposizione di una licenza nel caso in cui la loro esportazione avesse perseguito scopi di assistenza a soggetti stranieri nella creazione di *software* di cifratura.
In realtà quello che voleva Bernstein era solo pubblicare e comunicare le proprie idee circa la crittografia.

---

possibilità di inserire il proprio programma in una distribuzione commerciale di software, così da escludere ad un tempo lo stesso dalla sottoposizione del controllo del Dipartimento di Stato e consentire inoltre una nuova "comodity jurisdiction request".

278 Le singole questioni da affrontare avrebbero riguardato: a) gli scritti denominati "The Snuffle Encription System"; b) Snuffle.C; c) Unsnuffle.C; d) la manualistica in lingua inglese relativa all'utilizzo di Snuffle; e) La descrizione in lingua inglese delle operazioni di programmazione necessarie alla macchina per utilizzare il *software*.

279 Si veda il documento http://www.eff.org/Privacy/ITAR_export/Bernstein_case/Legal/961206.decision (sito consultato il 10 luglio 2002).

280 Vedi anche http://cr.yp.to/export/dishonesty.html e http://cr.yp.to/export/1996/0415-order.txt (siti Internet consultati il 10 luglio 2002).

Egli sosteneva, ancora una volta, di non essere libero di trasmettere ad altri la conoscenza dell'algoritmo di Snuffle, di parlare dello stesso nel corso di conferenze accademiche o di pubblicarlo in giornali e gruppi di discussione *on-line*.
In particolare, Bernstein sosteneva che la licenza, così come formulata dall'ITAR, imponesse restrizioni incostituzionali rispetto alla diffusione della crittografia.
Inoltre egli contestò l'imprecisione del documento e la violazione del Primo Emendamento della Costituzione degli Stati Uniti d'America.
Dall'altra parte si argomentò, al contrario, che l'ITAR rispettava la norma costituzionale in questione nelle sue previsioni riguardanti la crittografia; anzi, secondo la difesa del Governo, erano le richieste di Bernstein ad essere eccessive, in quanto le precedenti disposizioni non riguardavano gli insegnamenti di carattere accademico e scientifico.
La difesa oppose, in particolare, la considerazione che un eventuale giudizio sulla violazione del Primo Emendamento si sarebbe, al massimo, potuto riferire al caso particolare di esportazione del sistema o di sue componenti.
La Corte accolse tale impostazione quale punto di partenza per lo studio del caso, ma il 15 aprile 1996 il Giudice Patel dichiarò per la prima volta un concetto di fondamentale importanza giuridica: il codice sorgente, in quanto linguaggio (nel senso di forma espressiva del pensiero), è costituzionalmente protetto dal Primo Emendamento[281].
Inoltre, utilizzando documentazione riguardante casi riferibili al Pentagono come precedenti giuridici, il Giudice stabilì che "non sono sufficienti i soli interessi di sicurezza nazionale a giustificare restrizioni preventive".
Patel sostenne poi che il sistema di licenze utilizzato dal Governo non garantiva affatto la sicurezza auspicata costituendo anzi, così come applicato alla Category XIII(b)(1) dell'ITAR, una chiara violazione del Primo Emendamento.
Dalle argomentazioni del Giudice si può evincere anche che le restrizioni poste dai controlli all'esportazione di informazioni debbono riguardare il contenuto delle stesse e solo quello.
Anche se, in effetti, la Category XIII(b)(1) dell'ITAR si riferisce alla ricerca scientifica applicata allo scambio di informazioni sull'argomento della crittografia, nel caso di specie era stata posta una limitazione alla circolazione delle informazioni in quanto tali e non, come appunto stabilisce la norma, per quanto in esse eventualmente contenuto di pericoloso per la sicurezza nazionale.
Una ulteriore, importante precisazione caratterizzò il già consistente intervento del Giudice.
Tale precisazione definì l'ITAR "vago" notando, infatti, che lo stesso non chiariva adeguatamente come informazioni definibili di pubblico dominio in virtù della loro importanza scientifica e didattica e quindi della ricerca e del progresso industriale dovessero subire il controllo prima della loro esportazione.

---

[281] http://cr.yp.to/export/1996/0415-order.txt (sito consultato il 10 luglio 2002).

Questo, secondo la Corte, impedisce a chiunque di avere una "reasonable opportunity" di conoscere quanto è proibito[282].
Lo stesso giudizio riceve anche la definizione fornita dall'ITAR di "defense article".
Gli effetti immediati della decisione assunta dal Giudice Patel consentirono a Bernstein di continuare a svolgere liberamente le proprie attività.
Così egli fu libero di pubblicare su Internet i propri materiali e di discutere con altri studiosi le proprie ricerche, con la certezza di non violare l'ITAR[283].
Il 15 novembre 1996, il presidente Clinton diede un ordine particolare.
Tutta la disciplina riguardante la crittografia, che fino ad allora era stata competenza del Dipartimento di Stato, doveva immediatamente essere trasferita sotto il controllo del Dipartimento del Commercio.
Tale operazione comportò che le decisioni assunte dal Giudice Patel il 6 dicembre (con efficacia decorrente dal 16 dello stesso mese), che avrebbero dovuto impedire in fatto ed in diritto al Dipartimento di Stato di imporre agli americani licenze governative per la pubblicazione di informazioni e *software* di crittaggio, ricevessero quale risposta "politico-istituzionale" la pubblicazione di un nuovo regolamento del Dipartimento del Commercio[284].
Questo ripresentava, in pratica, tutti gli stessi problemi posti dal precedente redatto dal Dipartimento di Stato e già condannato in giudizio da Patel.
In una lettera datata 3 dicembre 1996 i legali di Bernstein chiesero al Governo quantomeno di attendere nell'applicazione della normativa predisposta, almeno fino al momento del vaglio di legittimità costituzionale effettuato dalla Corte Distrettuale, e chiesero contemporaneamente al Giudice di inibire fino allo stesso termine le imposizioni dettate dal nuovo regolamento.
Nelle intenzioni dei legali di Bernstein era forte la volontà di estendere con certezza l'eventuale ed auspicata soluzione favorevole della causa a tutto il territorio nazionale.
A ben vedere, le spinte in tale direzione non mancavano, provenendo anzi da diverse direzioni: sia l'industria sia il Parlamento degli Stati Uniti d'America avrebbero gradito l'eliminazione delle imposizioni contro cui si agiva.
Da più parti è stata sostenuta nel tempo l'utilità della crittografia; in particolare si è detto della sua importanza ai fini dello sviluppo di Internet, con particolare riferimento alle problematiche legate alla *privacy*, alla sicurezza delle transazioni commerciali e di dati, oltre alla sicurezza riferita al "contenuto informativo" di ogni singola macchina.
Secondo l'industria, imposizioni come quelle create dal Governo non permettevano la realizzazione di "prodotti sicuri" ed inoltre rischiavano di far

---

[282] In Internet all'indirizzo http://www.eff.org//Privacy/ITAR_export/Bernstein_case/Legal/961206.decision (sito consultato il 20 luglio 2002).

[283] In realtà, come venne presto alle luce, non era stato chiarito un dubbio. In particolare, non era chiaro l'ambito territoriale in cui le previsioni del Giudice Patel avrebbero espresso la loro efficacia. Patel aveva giurisdizione nel *Northen District of California* (in pratica San Francisco e Silicon Valley), quindi si discuteva circa la validità della sentenza al di fuori di tale territorio. In quel periodo i controlli alle esportazioni di *software* eseguibili continuarono ad essere effettuati. Fra gli altri subì tale sorte, ad esempio, anche il *broswer* Netscape

[284] In particolare dal *Bureau of Export Administration*.

perdere agli Stati Uniti d'America la *leadership* nel mercato dei computer e della *communication tecnology*.
Al contrario, dall'altra parte della barricata (NSA e FBI in testa) si argomentava che la tecnologia è troppo pericolosa per consentire a chiunque di utilizzarla in quanto, ad esempio, consente di mantenere la *privacy* anche a criminali oltre che ai comuni cittadini.
Il 18 giugno 1997 Daniel Bernstein, attraverso una conferenza stampa, decise di rendere pubbliche le problematiche relative al suo caso. Ciò avvenne alla presenza dei suoi legali e dei rappresentanti dalla *Electronic Frontier Foundation*.
Il 25 agosto 1997 la *Federal District Court*, presieduta ancora dal Giudice Patel, affrontò nuovamente tutte le questioni[285].
In tale occasione il giudice spiegò che, trasferendo una regolamentazione non conforme alla Costituzione degli Stati Uniti d'America da un Dipartimento all'altro, il Governo non aveva affatto risolto i problemi di legittimità emersi nel giudizio precedente.
In particolare, il Giudice sottolineò, ancora una volta, la violazione del Primo Emendamento da parte delle nuove regole, in quanto risultava ancora evidente la 'compressione' di diritti, quali quello di creare, usare e sviluppare *software* di crittografia, che discendevano direttamente dal novero generale dei diritti civili spettanti ad ogni individuo in merito alla libertà di espressione, pensiero e stampa.
Il cuore della sentenza specificava come l'imposizione di licenze per i *software* di crittaggio e decrittaggio e per la relativa manualistica informativa costituisse una chiara violazione del Primo Emendamento.
Di conseguenza, anche il regolamento del Dipartimento del Commercio doveva considerarsi incostituzionale.
Ancora una volta Bernstein ebbe la sensazione di essere libero di poter svolgere tutte le attività che potesse ritenere importanti ai fini della diffusione del profrio pensiero e delle proprie creazioni.
Ad avvalorare questo sentimento, anche l'invito della Corte, rivolto al Governo, di ricorrere alle Corti di Giustizia e non ad arbitrarie decisioni per futuri casi analoghi.
Seguì, inoltre, l'igiunzione da parte della stessa Corte, e ancora rivolta al Governo, a non minacciare, perseguitare, scoraggiare, ostacolare o, comunque, interferire in ogni modo con il lavoro svolto da Bernstein e da altri operanti nello stesso campo, in quanto tutti questi soggetti avrebbero agito nell'ambito dei propri diritti.
Il 28 agosto 1997, in risposta ad una "emergency motion" del Governo degli Stati Uniti d'America,[286] lo stesso Giudice Patel decise che la maggior parte

---

285 Si veda http://www.eff.org/Privacy/ITAR_export/Bernstein_case/Legal/970825.decision (sito consultato il 20 luglio 2002).
286Si vedano http://www.eff.org/Privacy/ITAR_export/Bernstein_case/Legal/970827_stay_motion.images/index.html e http://www.eff.org/Privacy/ITAR_export/Bernstein_case/Legal/970827_stay.motion (siti consultati il 20 luglio 2002).

delle ingiunzioni statuite potessero aspettare fino alla decisione della 9th *Circuit Court of Appeals*.
Comunque parte di esse conservarono intatta l'efficacia, così da consentire a Bernstein, l'otto settembre dello stesso anno, la pubblicazione di Snuffle 5.0 su Internet.
Il 6 maggio 1999 la Corte d'Appello confermò le decisioni assunte nel precedente giudizio dinanzi a Patel, stabilendo quindi l'incostituzionalità delle restrizioni sul crittaggio.
La Corte riconobbe, in *primis*, l'importanza e la 'criticità' della situazione conseguente alla connessione delle tecnologie crittografiche alla società moderna, non potendo non considerare, in tale ambito, le inevitabili implicazioni riguardanti i diritti garantiti dal Primo Emandamento.
Inoltre la Corte fa riferimento alla crittografia anche per sottolineare che il suo impiego ai fini del mantenimento della riservatezza e della segretezza sulle attività svolte da qualsiasi soggetto, implica anche il richiamo e lo studio del Quarto Emendamento, che si riferisce appunto alla *privacy*.
Considerazioni altrettanto importanti riguardano il rapporto tra le nuove tecnologie ed il Primo Emendamento negando, in tal caso, la Corte che il semplice fatto di utilizzare mezzi di comunicazione tecnologicamente avanzati e linguaggi differenti da quelli comuni comportasse l'esclusione di espressioni del primo tipo dalla tutela garantita attraverso il Primo Emendamento.
La sentenza in sé rappresentò un grande successo per Bernstein e per tutti coloro che si trovavano in analoghe situazioni.
Nel giugno 1999, però, un ulteriore intervento del Governo chiese la revisione delle decisioni della *9th Circuit Court of Appeals* e, contestualmente, la sospensione delle misure conseguenti alle stesse.
La richiesta si basava sulla superficialità presunta attribuita al lavoro della 9th Corte d'Appello nella assegnazione del giudizio di incostituzionalità dato dalla stessa Corte nei confronti delle restrizioni alla crittografia.
In particolare, si contestava che tali restrizioni, oltre ad essere utili ed indispensabili per la sicurezza dello Stato, per risultare efficaci avrebbero dovuto necessariamente agire anteriormente rispetto al momento divulgativo di informazioni e codici sorgenti.
Il 30 settembre 1999, la *Ninth Circuit Court of Appeals* annunciò l'accoglimento della richiesta di revisione presentata dal Governo.
Il 5 ottobre fu deciso che tutti i ventuno membri della Corte dovevano essere chiamati ad esprimersi nel giudizio per il quale si stabilì la data del 16 dicembre.
In quello stesso periodo, la stessa "encryption export regulation" oggetto della disputa in atto era anche in via di revisione da parte del Dipartimento del commercio: il 16 dicembre 1999, infatti, l'amministrazione Clinton aveva annunciato un nuovo indirizzo istituzionale in tema di crittografia. Risultava necessario, quindi, l'adeguamento della normativa preesistente.
Il Dipartimento per il Commercio annunciò la propria intenzione di rivedere le regole in questione entro il 15 dicembre 1999 (un giorno prima di quello fissato per il giudizio di revisione sul caso Bernstein).

La Corte decise, a questo punto, di concedere un maggiore intervallo di tempo prima di assumere la propria decisione.
In tal modo si consentiva la possibilità di valutare, sia da parte della Corte sia delle parti in causa, l'impatto delle modifiche apportate al regolamento anche per mezzo di brevi "supplimental brief" che argomentassero in riferimento alle modifiche apportate al regolamento dell'EAR.
Fu così deciso per un rinvio della causa al 21 marzo 2000. Per tale data fu accolta infatti la "Motion to Reschedule Oral Argument" del Governo.
Nonostante la stesura delle nuove norme, resa pubblica il 14 gennaio 2000, Bernstein ed i suoi legali si ritrovarono nuovamente a contestare i problemi di sempre: sia, cioè l'incostituzionalità delle disposizioni in sé, sia la non considerazione del codice sorgente quale forma espressiva degna di essere tutelata dal Primo Emendamento e, quindi, quale "vicolo informativo" liberamente utilizzabile per comunicare, trasmettendo istruzioni, tramite Internet.
Ulteriore problema era, poi, costituito dalla doppia notificazione che risultava necessario eseguire nei confronti della BXA e dell'NSA in riferimento ai codici spediti in forma elettronica, quando per gli stessi risultava, invece, consentita la pubblicazione cartacea.
Ed ancora, dubbi furono posti su come dovevano essere considerati i sorgenti distribuiti mediante supporti fisici e su altre questioni procedurali previste, ma non adeguatamente regolate, dalla nuova disciplina.
I difensori di Bernstein decisero, quindi, di rivolgersi alla Corte, richiedendo una nuova revisione dei fatti che però, date le novità apportate dal nuovo regolamento, sarebbe stato opportuno, sempre secondo la difesa del matematico, riportare al giudizio della Corte distrettuale di prima istanza.
Nel gennaio 2002 le parti si sono ritrovate dinanzi alla *Federal District Court* per quella che sembra essere diventata l'ennesima battaglia di una guerra ad armi impari eppure combattutissima.

Capitolo Quattrodicesimo

IL CASO DI PHIL ZIMMERMANN

SOMMARIO: 1. I fatti. – 2. L'intervento della *Electronic Frontier Foundation* e le argomentazioni giuridiche. – 3. Il 'caso Zimmermann'. – 4. La fine del procedimento.

1. I fatti.

Phil Zimmermann è, oggi, uno dei massimi conoscitori delle questioni tecniche legate alla crittografia e, suo malgrado, anche delle questioni legali che ad essa si accompagnano[287]. Il suo lavoro nell'ambito della crittografia ha ricevuto, nel corso degli anni, numerosi attestati di riconoscimento[288].
Zimmermann deve, però, almeno parte della sua fama proprio alle questioni legali sollevate dal programma di crittografia PGP da lui creato.
Quando, nel 1991, *Pretty Good Privacy* venne diffuso in tutto il mondo gratuitamente[289], il Governo degli Stati Uniti d'America ritenne che fossero

---

[287] Prima di creare il famoso software PGP (*Pretty Good Privacy*) nel 1991, Zimmermann ha lavorato, dopo essersi laureato in informatica presso la Florida Atlantic University, per oltre venti anni come ingegnere, specializzandosi in crittografia e sicurezza dei dati, data communications e sistemi *real-time embedded*. Quando è stato redatto questo capitolo, Zimmermann era *Senior Fellow* presso *Network Associates* e consulente indipendente per questioni legate alla crittografia. Fra i suoi clienti si ritrovano nomi legati alla produzione e alla distribuzione di hardware e software su scala mondiale: *Silicon Graphics*, *Sun Microsystems*, TCI, *Cable Labs*, *Reuters*, *Nike*, *Hewlett-Packard*, *Huges*, *Allied Signal*, *First Virtual Holdings*, *FTP softwar*e, *Deston-Fearing* e molti altri.

[288] Tra questi il *Lifetime Achievement Award* da parte di *Secure Computing Magazine* (1998); il *Norbert Wiener Award* da parte di *Computer Professionals for Social Resposability* (1996) per promuovere un uso responsabile della tecnologia; il *Crhrysler Award* (1995); il *Pioneer Award* da parte di *Electronic Frontier Foundation* (1995), il *PC Week IT Excellence Award* (1996); il *Network Computing Well-Connected Award* (1996). *Pretty Good Privacy* venne selezionato da *Information Week* come uno dei migliori dieci prodotti del 1994, e Zimmermann nel 1995 venne inserito da *Time Magazine* nei 'Net 50', tra le cinquanta persone più importanti dell'IT. Zimmermann è membro della *International Association for Cryptologic della Research*, *Association for Computing Machinery*, della *League for Programming Freedom*, e della *Union of Concerned Scientists*. È inoltre nel consiglio direttivo di *Computer Professionals for Social Responsability* e nel *Advisory Panel of American for Computer Privacy*.

[289] Zimmermann decise di regalare il programma, viste anche le intenzioni censorie e restrittive che sembravano animare l'operato del Congresso degli Stati Uniti d'America con riferimento al destino di PGP. Zimmermann ha sempre sostenuto che, attraverso tale atteggiamento, non intendeva in alcun esportare il *software*, ma semplicemente distribuirlo agli amici. Ha poi sempre sostenuto di essersi costantemente raccomandato, con chiunque lo ricevesse ed utilizzasse, di distribuirlo solo negli Stati Uniti d'America.

state violate le leggi di restrizioni all'esportazione di *software* crittografico[290]; come immediata conseguenza, il lavoro di Zimmermann divenne oggetto di indagini da parte delle autorità.
Lo studioso aveva, in realtà, distribuito PGP negli Stati Uniti d'America a titolo di *software freeware*, e non aveva in senso letterale 'esportato' il *software*. Il problema primario fu però che il programma si trovò ad essere oggetto di un *upload* anonimo su un sito ftp[291]. In tal modo il programma fu disponibile per il *download* da ogni angolo del mondo.
Da questi fatti partono le accuse mosse contro Philip Zimmerman[292] che, nel 1993, portarono all'apertura di una inchiesta nei suoi confronti[293].

2. L'intervento della *Electronic Frontier Foundation* e le argomentazioni giuridiche.

Nel corso della sua battaglia legale, lo studioso si è ritrovato al suo fianco persone ed associazioni, con la *Electonic Frontier Foundation* in prima fila, che da tempo si battono in nome del rispetto dei diritti civili nel ciberspazio[294].
In particolare, le argomentazioni giuridiche portate dalla EFF su questo caso si basano sostanzialmente sulla considerazione che quella del Governo americano è una 'guerra' senza un nemico determinato, combattuta esclusivamente contro l'utilizzo e l'esportazione delle tecnologie legate alla crittografia stessa.
Le risposte della EFF agli atteggiamenti assunti dal Governo durante l'indagine sono indirizzate, principalmente, in tre direzioni: da un lato l'appoggio economico a Zimmermann e la raccolta di fondi per la copertura delle spese legali per le cause riguardanti la crittografia, da un altro lato lo svolgimento di investigazioni - sia con riferimento al caso in questione sia con riferimento ad

---

290 Tale attività è regolata negli Stati Uniti d'America dal già accennato ITAR.
291 Le accuse mosse a Zimmermann prendono spunto dall'*upload* del *software* su Usenet. Con riferimento alle definizioni di Internet ed alla loro rilevanza giuridica sia consentito il rinvio a G. ZICCARDI, *Il diritto dell'era di Internet*, Mucchi, Modena, 1999.
292 In realtà, ad essere coinvolte nelle questioni legali di cui ci si occupa in questo capitolo, furono anche le due società *ViaCrypt* di Phoenix e *Austin Code Works* di Austin, che commercializzavano versioni di PGP preparate per la vendita.
293 Il 21 settembre 1993, la *Associates Press* annuncia per prima che è in corso una investigazione federale che ha ad oggetto "un programma controverso", ed in particolare si preannuncia la nascita di un caso giudiziario che influenzerà il futuro della distribuzione in Rete di software di questo tipo. L'annuncio originale è ancora reperibile su Internet all'indirizzo http://www.eff.org/Legal/Cases/PGP_Zimmermann/ap_subpoena.article (il sito è stato consultato il 15 luglio 2002).
294 La più nota delle associazioni che si occupa di questi temi è, appunto, la *Electronic Frontier Foundation*, fondata da Mitch Kapor, multimilionario *ex* proprietario della *Lotus*, e dal musicista-imprenditore-visionario John Perry Barlow. La EFF, che gode dell'appoggio di molte aziende contrarie all'ingerenza 'selvaggia' dell'autorità statale nella regolamentazione di Internet, ha organizzato raccolte di fondi o direttamente finanziato la difesa in molti processi che le autorità statunitensi hanno intentato contro presunti *hacker* e giovani programmatori accusati di pirateria telematica o di diffusione illegale di software considerato di valore strategico, oltre ad effettuare una attività di informazione e di pressione. Il sito Web di questa organizzazione è all'indirizzo http://www.eff.org.

altri casi giudiziari legati alle medesime problematiche - e, in ultimo, l'organizzazione di una campagna di sensibilizzazione che si preoccupi di evidenziare e combattere atteggiamenti non aderenti al dettato costituzionale contenuti in testi normativi in materia di crittografia, campagna finalizzata anche alla sensibilizzazione dei 'potenti' e dei politici al fine di mutare il volto della normativa sulle esportazioni.
La EFF contesta poi, essenzialmente, l'inadeguata e, per certi aspetti, inesistente protezione dei diritti civili offerta dalle istituzioni ai cittadini americani negli ambiti correlati ad Internet ed al ciberspazio: gli interessi in gioco, in effetti, risultano fortemente influenzati, soprattutto nel settore *de quo* da atteggiamenti che definire ostruzionistici risulterebbe quantomeno riduttivo.
In primis il pericolo riguarda il rispetto costante del diritto alla libertà di espressione e di quello alla *privacy*; altrettanto importanti appaiono, poi, altri obiettivi da perseguire, riferendosi in questo senso ad ulteriori diritti inderogabili propri di ogni individuo, riguardanti la possibilità di accedere a sistemi di crittografia sicura per il trasferimento di proprie informazioni o documenti, il diritto di pubblicare liberamente opere digitali e, non ultimo, il diritto ad essere giudicati equamente ed in assenza di condizionamenti di alcuna sorta[295].

3. Il 'caso Zimmermann'.

Le indagini sul caso Zimmermann, iniziate nel 1991 ed aperte formalmente nel 1993, si conclusero l'11 gennaio 1996.
In tale data, il Giudice M. J. Yamaguchi, del *Northen District of California*, decise che non sussistevano le ragioni necessarie a fare proseguire le indagini nei confronti di Zimmermann[296].
Il giudice non motivò la propria decisione, ma allo stato degli fatti possono riconoscersi, tra le ragioni che hanno portato alla chiusura dell'indagine, almeno due considerazioni che il giudice deve necessariamente avere affrontato: *in primis*, non fu mai provato che Zimmerman avesse reso disponibile personalmente PGP *on-line*, così come non era chiaro e pacifico che tale atto potesse esse considerato equivalente ad una esportazione vera e propria[297].

---

[295]Il testo dell'annuncio della EFF è reperibile su Internet all'indirizzo:
http://www.eff.org/Legal/Cases/PGP_Zimmermann/usatty_pgp_011196.announce (il sito è stato consultato il 15 luglio 2002).
[296] Per precisione di termini, nel caso di specie non si può parlare di 'assoluzione' in quanto Zimmermann ancora non era stato formalmente rinviato a giudizio.
[297] Tale aspetto presenta, come è facilmente intuibile, profili delicati. Sentenze che sostengono e appoggiano le questioni sollevate da Zimmermann e da altri casi analoghi, se da un lato consentono il superamento delle barriere poste alla divulgazione della conoscenza e limitano le facoltà di espressione, dall'altro potrebbero, in assenza di ogni limite, aprire la via ad un utilizzo pericoloso di Internet (istruzioni per fabbricare armi, segreti militari, preparazione di azioni terroristiche sono solo alcuni degli esempi di un tale impiego di questo peculiare mezzo di comunicazione).

Inoltre lo stesso giudice intuì, e tenne probabilmente conto, delle reali motivazioni che spingevano il Governo[298] ad impegnarsi in questa ed in altre analoghe battaglie legali.
La Corte riconobbe come unico vero scopo di queste azioni quello della indiscriminata opposizione alla creazione e alla distribuzione di *software* e documentazione riguardante la crittografia, perseguita per mezzo di atti che potessero condurre anche all'inibizione delle stesse azioni. La preoccupazione delle istituzioni era (ed è), come noto, legata a questioni di sicurezza nazionale.
Di conseguenza, tutto ciò che non poteva essere facilmente decodificato doveva considerarsi illegale o, comunque, soggetto a restrizioni forti.
Nel caso di specie, i fatti fondamentali furono individuati dalla EFF proprio nel mancato rispetto dei diritti sopra descritti.
A Zimmermann ed altri coinvolti in questi fatti fu richiesto di fornire documentazione riguardante PGP[299], alla *Austin Code Works* fu anche chiesto, da parte del Dipartimento di Stato e su indicazione dell'NSA, di registrarsi presso le apposite Autorità come 'commercianti di armi'.
Interessante risulta l'analisi del caso contenuta in un articolo di John Markoff, pubblicato sul *New York Times*[300] il 21 settembre 1993.
Markoff si preoccupa di analizzare e commentare la questione toccando, dalla sua posizione in linea di principio 'neutrale' e oggettivamente critica di giornalista, tutti i punti fondamentali e le implicazioni della vicenda.
In primo luogo viene particolarmente evidenziato il rapporto che intercorre tra crittografia, libertà di parola (*free speech*), privacy e sicurezza nazionale.
L'attenzione viene poi portata sul coinvolgimento nella vicenda legale anche delle due *software house* che risultavano in 'rapporto' con la distribuzione di PGP, e in particolare sulla sanzione pecuniaria (*Federal subpoena*) inflitta a *ViaCrypt*, la già vista società di Phoenix che intendeva vendere una versione licenziata di PGP e alla società di Austin, che intendeva fornire ad altri sviluppatori di software che avrebbero poi incorporato PGP nei loro programmi.
Dal 9 settembre 1993 tanto *ViaCrypt* quanto *Austin Code Works* avrebbero dovuto fornire al Governo tutta la corrispondenza ed i *records* correlati alla distribuzione di PGP, nonchè tutte le altre informazioni che riguardassero in ogni modo la crittografia[301].
In questa disposizione si ravvisa ancora una volta l'ennesimo atto di una lunga guerra compiuta dal Governo, ed in particolare dall'NSA, nel tentativo di bloccare l'adozione pubblica e l'implementazione di tecnologie 'pericolose' per la sicurezza nazionale.

---

298 Intendendo, in particolare, gli uffici dell'FBI della CIA e dell'NSA.
299 Il *Federal Grand Jury*, su richiesta dell'*Assistant U.S. Attorney* William Keane, chiese la produzione obbligatoria di documentazione riservata sulla crittografia sia a Zimmermann sia a *ViaCrypt* e *Austin Code Works*.
300 Il testo dell'articolo è reperibile in Internet all'indirizzo http://www.eff.org/Legal/Cases/PGP_Zimmermann/nyt_subpoena.article (sito cconsultato il 15 luglio 2002).
301 Per ulteriori approfondimenti, e per consultare tutta la documentazione correlata a questo caso, è interessante consultare l'indirizzo http://www.eff.org/Legal/Cases/PGP_Zimmermann (sito consultato il 15 luglio 2002).

Inoltre è necessario considerare che le restrizioni poste ad ogni tentativo di divulgazione di materiale concernente la crittografia hanno, nel tempo, colpito ed 'irritato', oltre che ricercatori informatici e matematici, anche numerose *software-house*.
Alcune di queste, rappresentate dalla *Software Publisher Association*, nel 1992, avevano trovato un accordo con l'NSA che permetteva l'esportazione di *software* contenente determinate (tassativamente) funzioni di *coding*.
In realtà, la realizzazione di tale accordo altro non era che uno strateggemma attuato dalla NSA con lo scopo di mantenere il pieno controllo della situazione.
Non è difficile immaginare, infatti, come la *National Security Agency* intendesse riservarsi la possibilità di accedere a dati crittati in ogni momento attraverso una sorta di 'chiave universale' detenuta dallo stesso ente.
PGP, a causa delle novità tecniche che presentava, costituì sin dall'inizio un duro ostacolo che si poneva sulla strada dell'NSA.
Il Professor Eben Moglen, della *Columbia University* di New York, inquadrando il problema nell'ottica dei diritti civili e criticando aspramente le intenzioni dell'NSA, commentò che "il diritto di parlare con la lingua di PGP è identico al diritto di parlare la lingua Navajo. Il Governo non ha alcun particolare diritto di prevenire che si parli in maniera tecnica, anche se non ha modo di comprendere quello che si dice".
La formula di PGP[302], considerata da molti capace di proteggere ogni informazione anche dall'attacco dei computer dell'NSA, ha generato ulteriori ed interessanti dibattiti oltre a quelli incentrati sui dettami e sulla relativa violazione del Primo Emendamento alla Costituzione degli Stati Uniti d'America.
Alcuni di questi hanno riguardato aspetti tecnici, come quello volto a stabilire la rilevanza e le conseguenze giuridiche assunte dalla descrizione degli algoritmi e dal rapporto di questi con il codice sorgente[303].
Interessante è anche la questione sollevata e discussa in un articolo[304] del *Boardwatch Magazine*.
In questa sede viene oggettivamente analizzata la questione relativa alla diffusione di PGP, considerando che l'accusa mossa nei confronti di Zimmermann riguarda l'esportazione del *software*. Il programma in questione, secondo l'articolo, non ha mai attraversato i confini degli Stati Uniti d'America a seguito di una diretta e volontaria azione di qualcuno, ma è stato semplicemente 'postato' su siti Internet locali.
La conseguenza fu però che, in una decina di minuti, PGP era già diffuso in tutto il mondo.

---

302 Sviluppata alla sua base da tre noti informatici: Ronald Rivest, Adi Shamir e Leonard Adelman.
303Si veda, con riferimento al dibattito su questi punti http://www.eff.org/Legal/Cases/PGP_Zimmermann/itar_aeca_caaa_implication.debate (sito Internet consultato il 15 luglio 2002).
304 il testo dell'articolo è consultabile all'indirizzo http://www.eff.org/Legal/Cases/PGP_Zimmermann/rickard_pgp_nii.article (sito Internet consultato il 15 luglio 2002).

Questo episodio, più che confermare una diffusione non autorizzata del *software*, sottolinea l'estrema difficoltà, se non l'impossibilità di fermare la diffusione della crittografia su scala mondiale.
La tecnologia, ed in tale accezione la trasmissione telematica, sono mezzi che ben poco si prestano agli scopi, in molti casi persecutori e limitativi, caldeggiati ed attuati da CIA, FBI e NSA. Anzi, Internet costituisce il mezzo ideale per costruire la libertà proprio perché l'ambiente virtuale che ne costituisce l'essenza difficilmente si presta all'esercizio di un controllo globale sul suo contenuto.
Le intenzioni sostenute da Zimmermann, che più volte aveva dichiarato il suo favore alla possibilità che i cittadini americani potessero proteggere la propria *privacy*, portarono, in effetti, conseguenze diverse.
Il programma 'finito' in Internet era stato scaricato da milioni di utenti contravvenendo così alle disposizioni che regolando le esportazioni (di armi).
La pena per tale reato, che lo stesso Zimmermann rischiava in conseguenza dell'accusa che gli era stata rivolta, prevedeva una condanna da tre a cinque anni ed una multa fino ad un massimo di un milione di dollari.
Quando nel 1996 il Dipartimento di Giustizia lasciò cadere le accuse e le relative investigazioni, Zimmermann fondò *PGP Inc*, che nel dicembre 1997 venne acquistata da *Network Associates*. Recente è stato l'annuncio della cessazione dello sviluppo di PGP.
PGP ha, nel tempo, assolto a numerose funzioni ed è stato oggetto di altrettanti riconoscimenti.
Lo stesso Zimmermann ha continuato a ricevere lettere ed attestati di riconoscenza in particolare da gruppi di attivisti che si battono in tutti i Paesi del mondo per il rispetto dei diritti umani[305]. Il lavoro di PGP nelle intenzioni del suo creatore protegge l'innocente e il debole[306].

4. La fine del procedimento.

Il lungo procedimento legale svoltosi contro Zimmermann si è risolto, in realtà, in un buco nell'acqua per il Governo americano[307]:
Da un lato, i Tribunali hanno finito per assolvere lo scienziato (le cui ingenti spese di difesa sono state coperte da una sottoscrizione che ha coinvolto migliaia di utenti della rete); dall'altro, l'ingiunzione a rendere disponibili attraverso Internet solo versioni di PGP fornite della cosiddetta *backdoor* — basate cioè su un algoritmo di cifratura del quale le istituzioni di sicurezza

---

[305] Ad esempio in Guatemala l'*International Center for Uman Right Research* utilizza PGP per cifrare i *database* ogni notte per il timore che una 'squadra della morte' attacchi i suoi uffici. (i *database* contengono i dati anagrafici di testimoni che altrimenti correrebbero immenso pericolo). Così anche nel resto del mondo, come nei balcani e nell'est europeo dove PGP ha protetto *file* contenenti dati e identità di gruppi e soggetti impegnati in ambiti umanitari e portato anche alcuni soggetti in carcere pur di non rivelare *password* e chiavi di PGP

[306] Casi concreti di questa concezione possono trovarsi all'indirizzo http://www.philzimmermann.com/letters.shtml (sito consultato il 15 luglio 2002).

[307] Nel maggio 1999, la sentenza che decide (per ora) il caso Bernstein, conferma la sconfitta subita dal Governo americano.

possedessero una delle chiavi — è stata vanificata dal fatto che le versioni 'depotenziate' di PGP immesse in rete in America sono state largamente ignorate dalla popolo della Rete, al quale bastava collegarsi ad un sito europeo per scaricare una versione 'sicura' del programma.
In ultimo, non può trascurarsi un aspetto della questione che riguarda ancora la riservatezza del messaggio scambiato in Rete.
Tale caratteristica dovrebbe, infatti, riguardare ogni tipo di comunicazione e non solo quelle considerate 'sensibili'; inoltre bisogna anche riconoscere che lo stesso diritto alla riservatezza, di per sé privo di conseguenze negative se non correttamente impiegato, può causare il sorgere di problematiche inevitabilmente connesse.
Ci si riferisce, tra l'altro, alla diffusione attraverso la Rete di materiale pedo-pornografico, ai proclami di gruppi violenti o terroristici, alle informazioni militari o riservate.
Si tratta di questioni problematiche, vista anche la difficoltà di classificare una determinata informazione in maniera univoca. Tale analisi comporta giudizi di valore, e assunti morali, la cui considerazione può variare radicalmente da Paese a Paese, da cultura a cultura, da persona a persona, e che possono comunque essere facilmente aggirati dalla natura sovranazionale, o meglio ultraterritoriale, di Internet.
Molti Governi, con in testa quello degli Stati Uniti d'America, di fronte a questi fenomeni hanno cercato di intraprendere la via della censura e della repressione, ma hanno forse sottovalutato tanto le potenzialità della Rete quanto quelle dei suoi utenti.
Ad esempio, il *Communication Decency Act* e il *Child On-line Protection Act*, predisposti con il fine di controllare e gestire la trasmissione telematica di determinate informazioni, si sono rivelati per il Governo pericolose armi a doppio taglio in considerazione dei relativi provvedimenti giudiziari che li hanno riguardati.
Proprio episodi di questo tipo portano a comprendere come debba ritenersi auspicabile, al fine di evitare nuovi interventi eccessivamente autoritari da parte delle istituzioni nazionali, che la stessa comunità della rete individui in molti settori i meccanismi di autocontrollo[308].
In ambito europeo, anche in seguito all'emissione di alcune normative comunitarie, come la Direttiva CEE 90/388 (modificata dalla 96/19 CE), relativa alla concorrenza nei mercati dei servizi di telecomunicazioni[309], si è accesa la discussione attorno alle medesime problematiche sino ad ora descritte.
In particolare, uno dei punti che provoca i maggiori problemi riguarda la normativa di controllo sulle trasmissioni telematiche e le questioni riguardanti le eventuali responsabilità dei gestori dei sistemi telematici e dei fornitori

---

[308] In questo senso si muove, ad esempio, la tecnologia PICS.
[309] Per una panoramica della normativa vigente in Unione Europea ed in Italia è consigliabile consultare l'indirizzo: http://www.agcom.it/arg_tlc.htm (sito Internet consultato il 20 luglio 2002).

dell'accesso alla Rete relativamente alle informazioni immesse nella Rete dai propri utenti.
Una soluzione che avesse accolto la tesi di una responsabilità diretta di questi soggetti avrebbe, sicuramente, condotto ad una forma di controllo dei predetti contenuti (compresa la corrispondenza) in palese contrasto con l'art. 15 della Costituzione italiana.
Al contrario, la soluzione inversa, accompagnata comunque dalla possibilità-necessità per i gestori dei suddetti servizi di identificare gli utenti (ad esempio previa richiesta della autorità giudiziaria) non impedirebbe totalmente un accesso anonimo alla rete e alle possibilità divulgative da questa offerte; d'altro canto sarebbe controproducente continuare sulla strada della repressione anche in seguito ad una ulteriore ed importante considerazione: così come avviene anche in altri ambiti, ed ancora di più in Internet vista la peculiarità del mezzo, repressione ed eccessive restrizioni più che 'disciplinare' il sistema rischiano di provocare reazioni incontrollabili.

Capitolo Quindicesimo

IL CASO DI DMITRY SKLYAROV

SOMMARIO: 1. Il *Digital Millenium Copyright Act* e la crittografia. – 2. Il caso Sklyarov. – 3. Il DMCA in rapporto alla normativa europea: considerazioni.

1. Il *Digital Millenium Copyright Act* e la crittografia.

Il *Digital Millenium Copyryght Act* (DMCA) è la legge adottata nel corso della amministrazione Clinton nel 1998 in accoglimento delle osservazioni e delle richieste della WIPO (*World Intellectual Property Organization*).
La sua funzione è quella di regolare e proteggere il diritto d'autore nell'era digitale. In particolare, l'attenzione delle disposizioni, suddivise in cinque articoli, è rivolta alle modalità attraverso le quali è possibile utilizzare i mezzi di trasmissione telematica allo scopo di fruire di informazioni ed inoltre, con lo stesso atto, si sono poste numerose e pesanti restrizioni alla condivisione delle stesse.
Analizzando più da vicino il DMCA si nota come il primo articolo dello stesso, riferendosi alle problematiche derivanti dall'impiego delle nuove tecnologie telematiche rispetto alla tradizionale tutela del diritto d'autore, introduca nuove fattispecie di reato che si traducono, nella pratica, nelle misure relative alla violazione delle misure di protezione tecnologiche (*Circumvention of Technological Protection Measures*)[310], e alla violazione dell'integrità delle informazioni riguardanti il *copyright management* (*Integrity of Copyright Management Information*).
In pratica, per mezzo del DMCA risulta inibita la produzione e la vendita di apparecchiature o servizi tesi alla violazione dei divieti sopra descritti[311].
In verità nessun veto è posto ai produttori di *hardware*[312], ma la situazione concreta vede numerosi "accordi privati" tra aziende tesi allo sviluppo di protocolli segreti (e crittografati) atti ad impedire qualsiasi copia, e quindi anche di quella "personale" prevista come diritto dalla legge, di prodotti protetti dal diritto d'autore.

---

310 Previsione che a sua volta distingue tra aggiramento di misure che inibiscono l'accesso non autorizzato a lavori protetti dal *copyright* e quello relativo alle misure che impediscono la copia non autorizzata di lavori protetti dallo stesso *copyright*.
311 La normativa relativa al *copyright* prevede, comunque, che in determinati casi la copia può essere considerata "fair use" rispetto al lavoro protetto.
312 Una interessante lettura sull'argomento è reperibile all'indirizzo http://www.toad.com/gnu/whatswrong.html (sito consultato il 15 luglio 2002).

Il DMCA, in concerto con i suddetti accordi, ha in pratica contribuito a privare gli utenti di quel "far use" che al contrario deve essere, in quanto diritto legittimo, riconosciuto e protetto per legge.
Quanto alla seconda fattispecie di reato introdotta dal DMCA, essa si riferisce al contrassegno elettronico (CMI) che contiene le informazioni relative al lavoro a cui lo stesso viene apposto. Il CMI contiene, ad esempio, le informazioni relative all'autore, al detentore dei diritti, ed altre informazioni dello stesso tenore[313].
A riguardo le misure previste si rivolgono a due differenti condotte riferibili alla violazione del CMI: una riguarda la falsificazione del CMI, l'altra la rimozione o l'alterazione dello stesso contrassegno.
Il primo reato riguarda la creazione e la distribuzione di CMI falsi intenzionalmente tesi alla violazione della legge; il secondo prevede misure penali per chi sempre intenzionalmente altera o rimuove lo stesso contrassegno compresa l'eventuale distribuzione di copie contraffatte.
Nelle previsioni di reato contenute nel DMCA è compresa anche la diffusione di informazioni che abbiano lo scopo di facilitare o consentire l'alterazione e la rimozione del DMCA.

2. Il caso Sklyarov.

Dmitry Sklyarov è un cittadino russo che lavora alle dipendenze della Elcomsoft, società con sede a Mosca. Egli, mettendo in pratica quanto esposto nella propria tesi di laurea, realizza un *software*, denominato *Advanced eBook Processor* (AEBPR), che consente l'aggiramento delle misure tecnologiche ideate dalla ADOBE a tutela del proprio formato *eBook* consentendo, attraverso operazioni di decrittaggio, la trasposizione delle informazioni nel differente formato PDF (*Portable Document Format*), sempre di proprietà della ADOBE, ma distribuito liberamente come "reader".
Nel raccontare quanto messo in atto dal programmatore russo, non può trascurasi una considerazione.
Il sistema ideato da Sklyarov funziona esclusivamente con eBook regolarmente acquistati sul mercato[314].

---

313 È però espressamente vietato che il CMI possa comprendere informazioni relative al mero utilizzatore e/o detentore dell'oggetto.

314 Il sistema di sicurezza ideato da Adobe da solo non fornisce la cifratura dei libri elettronici: a tale scopo soccorrono *plug in* di terze parti, come *WebBUy*, che, appunto, siedono dentro l'infrastruttura di Adobe per garantire cifratura e decifratura; il sistema di Adobe si preoccupa, invece, di gestire le varie restrizioni all'uso che gli editori possono decidere di abilitare o disabilitare. Le ricerche condotte da Sklyarov si sono preoccupate proprio di individuare e sfruttare le debolezze presenti nella infrastruttura del sistema di Adobe nonchè di quelle relative alle relazioni della stessa infrastruttura con i vari *software* di *plug in*. Il risultato di tale sforzo è la trasformazione nel diverso ed accessibile formato PDF. In pratica AEBPR intercetta la versione non cifrata del libro elettronico dopo il passaggio della stessa attraverso i *plug in*. In questo momento, il *file* intercettato e decifrato è libero dalle restrizioni all'uso che vengono aggiunte dall'*e-Book reader* e può quindi essere aperto da qualsiasi lettore PDF.

L'utilità di questo *software* si concretizza, infatti, nella possibilità di "trasportare" da un computer all'altro o da un computer ad un supporto esterno il contenuto del file acquistato legalmente nel formato *eBook* di Adobe.
Allo stesso modo in cui, ad esempio, è possibile leggere un libro in formato tradizionale in luoghi diversi, o ascoltare lo stesso Cd musicale a casa o con il lettore dell'auto, le intenzioni di Sklyarov e, conseguentemente, quelle commerciali della Elcomsoft, sono rivolte a creare la possibilità di rendere usufruibile un *E-book*, quando regolarmente acquistato e scaricato sul proprio Personal Computer, anche in situazioni diverse da quelle che prevedono l'impiego della stessa macchina.
In realtà, ciò che si acquista mediante lo scaricamento dalla rete del *file* di Adobe, non è il libro, ma solo il permesso di leggerlo. Infatti il *file* che si ottiene è inutilizzabile, in quanto crittografato, se non è accompagnato dal meccanismo di "autorizzazione alla lettura" consistente in una serie di transazioni tra vari *server* (quello del distributore autorizzato, quello di Adobe e quello dell'utente finale).
Il risultato di tali operazioni è quindi il "permesso" di leggere il libro solo ed esclusivamente sul computer che ha partecipato all'operazione di transazione. Naturalmente l'utente usufruisce dell'*e-book* senza rendersi conto della complessa operazione che lo ha consentito.
Skyliarov, per conto della *Elcomsoft*, ha messo effettivamente a punto AEBPR allo scopo di aggirare le protezioni tecnologiche utilizzate dalla Adobe per i propri *Ebook*; da un altro punto di vista però, egli ha creato uno strumento capace di consentire quel "fair use"[315] garantito dalla normativa sul diritto d'autore[316].
Inoltre egli ha fatto tutto ciò in Russia, dove, oltre ad essere un simile *software* perfettamente legale, il DMCA con le sue previsioni non può arrivare per ovvie ragioni di ambito territoriale.
Si è già detto in precedenza di come, nelle previsioni legislative degli USA, ed in particolare proprio nel DMCA, sia considerato un grave reato ("felony") ogni atto di diffusione di sistemi, *software* o informazioni, che abbiano lo scopo di aggirare le misure poste a tutela del *copyright*.

---

[315] Il concetto di "fair use" indica, nell'esperienza americana, il punto di riferimento culturale per l'applicazione giuridica delle eccezioni al *copyright* destinate a salvaguardare il diritto alla copia privata ad uso personale e di studio, e in alcuni casi, anche all' utilizzo all'interno di biblioteche per consultazioni a carattere scientifico e didattico. Un ottimo riferimento per la pubblicistica relativa a tale concetto è il sito Web: http://fairuse.stanford.edu (consultato il 15 luglio 2002).

[316] Oltre alla possibilità di lettura in luoghi diversi da quello in cui risiede la macchina che contiene il file, AEBPR consente ai legittimi acquirenti di *e-Book* di esercitare utilizzazioni libere, legittime ma altrimenti impossibili con il formato originale di Adobe. Ad esempio, il programma consente la lettura del *e-Book* anche sul proprio "laptop", su un PDA, inoltre permette di continuare a lavorare anche se il formato cambia o se il computer sul quale è caricato il *file* ha problemi; ancora offre la possibilità di effettuare una stampa su carta, e di continuare ad usufruire di quanto acquistato anche utilizzando un sistama operativo diverso (come ad esempio il diffusissimo ed ottimo Linux). ABEPR consente anche la possibilità di copiare parte del *e-Book* in un progetto di studio scolastico, o in uno scientifico; inoltre, non ultimo, il software in questione facilita la letture degli *e-Book* a persone con problemi di vista.

A Skylyarov, in realtà, non è stata mossa alcuna accusa riguardante la violazione del *copyright*, inteso come sfruttamento del diritto derivante dalla creazione o dalla detenzione dei diritti sull'opera; anche perché, come già evidenziato, AEBPR funziona esclusivamente con *e-book* regolarmente acquistati nel formato proprietario.
La questione legale che ha costretto il programmatore russo ad un prolungamento forzato del proprio soggiorno americano, si riferisce invece alla violazione di differenti norme che, se fosse stata confermata in sede di giudizio[317], avrebbe costretto Sklyarov alla detenzione per un periodo di almeno cinque anni (e fino a 25) ed al versamento di una considerevole somma in denaro, da 500.000 fino ad 1.000.000 di dollari[318].
Una prima accusa riguardava la violazione delle previsioni "anti-traffiking" della section 1201 (b)(1)(A) del 17 USC, diventata poi legge nel 1988 con l'emanazione del DMCA; una ulteriore riguardava invece quanto previsto dal 18 USC 2, e cioè gli atti di "aiding" e di "abetting" puniti dalla stessa norma.
La Section 1201(b)(1)(A) pone il veto ad "ogni persona" di costruire, importare, offrire al pubblico, fornire, o comunque trafficare con ogni tecnologia, prodotto, servizio, device, componente, e con qualsiasi altro mezzo che abbiano il proposito di circonvenire le protezioni fornite da misure tecnologiche poste a tutela del diritto del detentore del *copyright* su un lavoro o su una parte dello stesso[319].
Il 18 USC 2 prevede invece che ogni persona che aiuti, impartisca consigli o ordini, induca o comunque procuri un'offesa agli Stati Uniti d'America, sia giudicato e punito come il principale autore dello stesso fatto.
Sklyarov fu quindi accusato di aver creato, 'spacciato' e fornito al pubblico *software* che permette l'aggiramento delle misure tecnologiche sopra descritte[320].

---

317 Le accuse nei confronti di Sklyarov sono, come si vedrà, successivamente cadute quando la Adobe, per fermare il boicottaggio dei suoi prodotti messo in atto dai sostenitori della "libertà digitale" ha ritirato la propria denuncia favorendo così il rilascio su cauzione del programmatore.

318 Si tratta infatti di una indagine criminale regolata nella sezione 1204 del 17 USC.

319 Si veda il sito http://www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html

320 da http://www.eff.org/Cases/US_v_Elcom/us_v_sklyarov_faq.html "Prosecution Questions: What is Dmitry charged with? Two counts. First, with violating the anti-trafficking provision in section 1201 (b)(1)(A) of 17 USC , which was made law by the 1998 Digital Millennium Copyright Act (the DMCA), and secondly, with "aiding and abetting" under 18 USC 2. Section 1201(b)(1)(A) prohibits any person from manufacturing, importing, offering to the public, providing or otherwise trafficking in "any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof". 18 USC 2 provides that any person who aids, abets, counsels, commands, induces or procures the commission of an offense against the United States or "willfully causes an act to be done" by himself or another person which would be an offense against the United States, is punishable as a principal offender. Sklyarov is accused of "trafficking" in or providing to the public, software that can circumvent technological protection on copyrighted material under the DMCA's anti-circumvention provisions (section 1201(b)(1)(A)). He's also charged with aiding and abetting. The Complaint doesn't identify the factual basis of that charge, but people have speculated that the US government would claim that Dmitry, as an employee of ElcomSoft Co. Ltd., aided and

Il caso che si sta esaminando, pone tra l'altro l'accento sulla sospetta incostituzionalità caratterizzante le nuove norme del DMCA, di cui Sklyarov appare come la prima vittima ufficiale; anche se in realtà in materia sono state affrontate numerose altre questioni, ma sempre in sede esclusivamente civile[321].
Per molto tempo la Adobe e l'FBI hanno cercato un sistema per fermare la diffusione del programma AEBPR e delle informazioni che lo riguardavano.
Il limite territoriale del DMCA e, più in generale, quelli di giurisdizione[322] del Governo degli Stati Uniti d'America e, quindi, del proprio apparato giudicante, costrinsero l'FBI ad una paziente attesa che si protrasse fino al momento in cui Sklyarov, varcando i confini americani, partecipò a Las Vegas alla DEF CON[323] per presentare la propria relazione dal titolo "*e-Book security: Theory and pratice*".
Nel corso della conferenza si discusse in particolare di questioni legate alla "sicurezza elettronica" ed è in tale sede che Sklyarov evidenziò, ridicolizzandoli al tempo stesso, i problemi relativi ai *bug* prsenti nella tecnologia alla base del software *Adobe e-Book*.
Il problema, e forse anche il motivo del particolare impegno, da parte di Skyliarov e dai sostenitori della sua causa con in testa la solita EFF, nel combattere questa battaglia contro il governo degli Stati Uniti d'America[324],

---

abetted the company to manufacture and distribute software that circumvents a technological protection that effectively protects a copyrighted work".

321 Con riferimento agli aspetti correlati al copyright si legga da http://www.eff.org/Cases/US_v_Elcom/us_v_sklyarov_faq.html "The Affidavit sworn by FBI Special Agent O'Connell filed in support of the Complaint alleges that Dmitry was the holder of the copyright in Elcomsoft's Adobe eBook Processor (AEBPR) program. The ElcomSoft website claims that Dmitry simply developed the algorithms on which the AEBPR program is based. Is Dmitry accused of copyright infringement? No. Copyright infringement is not an issue in this case and Dmitry is not accused of infringing anyone's copyrights. And ElcomSoft claims that its Advanced eBook Processor software can't be used by anyone except for people who have already lawfully purchased the right to view the eBooks from eBook retailers. Instead this case hinges on new, and constitutionally-suspect provisions that were added to copyright law by the DMCA. The provision (see above for details) do not address copyright violation, but rather the distribution of tools and software that can be used for copyright infringement. Is it illegal under the DMCA's anti-circumvention provisions for people in the US to use the software Dmitry wrote? The DMCA anti-circumvention provisions don't prohibit the mere possession or use of a section 1201(b)1) circumvention technology, so (assuming for the purpose of argument that AEBPR would be found to be such a tool), it's legal to use AEBPR in a non-infringing way. Paradoxically, the DMCA makes it illegal for someone to write a program or develop a tool and provide it to people so that they can remove a technological protection and exercise fair use rights, but it is not illegal for people to use that tool for purposes that don't infringe copyright (such as fair use).

322 http://www.eff.org/Cases/US_v_Elcom/us_v_sklyarov_faq.html : " Can the US even have jurisdiction over Dmitry and/or Elcomsoft for developing software in Russia that is perfectly legal to distribute in Russia?".

323 La DEF CON è una delle più importanti "technical conference" che si tiene da 10 anni raccogliendo più di 4000 partecipazioni da parte di esperti, non solo professionisti, di sistemi di sicurezza, crittografia e programmazione. Maggiori informazioni sulla "DEFense CONdition of the Country", comprese quelle riguardanti le misure di sicurezza relative al rischio di una guerra nucleare, sono reperibili all'indirizzo http://www.defcon.com/ (sito consultato il 15 luglio 2002) .

324 Sklyarov non poteva non conoscere i problemi che il suo intervento alla DEF CON avrebbe causato. A tale conferenza partecipa infatti un grande numero di "professionisti della

consisteva nella punibilità, prevista nel primo articolo del DMCA, dell'atto di diffusione di informazioni relative alla rimozione o all'alterazione del CMI.
Dalla parte del programmatore si sostenne, tralaltro, che l'affermazione normativa che programmi come AEBPR possano facilitare e consentire comportamenti illeciti, quale ad esempio la duplicazione abusiva dell'*e-Book* di Adobe, è inesatta: in casi simili, la legge dovrebbe infatti prevedere sanzioni esclusivamente a carico di chi, di tali strumenti faccia un eventuale uso illecito.
Fatto sta che il 16 luglio 2001 gli agenti dell'FBI, una volta che Sklyarov ebbe concluso il proprio intervento, ponendo così in essere la tanto attesa violazione delle norme americane nei confini territoriali degli stessi Stati Uniti d'America, effettuarono l'arresto del programmatore mentre questi rientrava in albergo[325].
Fino al 6 agosto egli rimase detenuto e solo l'intervento di Robin Gross, legale della EFF, e di Joe Burton, difensore di fiducia dello stesso Sklyarov, uniti all'immediato interesse per la questione sorto nell'opinione pubblica della Rete, ne consentirono la liberazione previo versamento di una cauzione di 50.000 dollari.
In realtà, l'arresto non conseguì direttamente al contenuto del suo intervento al DEF CON, anche se quest'ultimo costituiva comunque un grave punto a suo sfavore.
L'azione fu invece intrapresa nei confronti dell'informatico così da consentire, attraverso la sua presenza fisica, l'instaurazione del giudizio sulla questione in territorio americano[326].
Anche se la *ElcomSoft* era una società russa, e Sklyarov un programmatore che lavorava in Russia, l' affidavit dell'FBI sostenne che la stessa *ElcomSoft* vendeva il *software* attraverso un sito statunitense[327] inviando, dopo la conferma dell'acquisto, una chiave elettronica all'acquirente[328]. Il vero obiettivo delle istituzioni americane era quindi chiaramente la Elcomsoft[329].

---

tastiera" che, una volta venuti in possesso delle preziose informazioni fornite dallo stesso Sklyarov, non hanno avuto problami a metterle in pratica.

325 Swklyarov subì la persecuzione del Dipartimento di Giustizia americano dietro la spinta del Governo degli Stati Uniti; in particolare, tutto ha avuto origine da un "complaint" depositato dall'agente speciale dell'FBI Daniel J O'Connell di San Jose (che è anche sede della AdobeSystem Inc.). Nel documento si evince che l'accusatore principale di Sklyarov è Joseph Sullivan e Scott Frewing, *Assistant U.S. Attorneys* con l'assistenza di Lauri Gomez. Ulteriore documentazione su questi aspetti è consultabile agli indirizzi http://www.cybercrime.gov/Sklyarov.htm e http://www.eff.org/ (sito consultato il 15 luglio 2002).

326 Il programmatore aveva in realtà sviluppato gli algoritmi che sono alla base del programma e scritto parte dello stesso non prendendo parte in alcun modo alla distribuzione di AEBPR.

327 Cfr. http://www.regnow.com (sito consultato il 15 giugno 2002).

328 Il 3 luglio la ElcomSoft, dopo l'invio da parte della Adobe di una lettera di diffida che sosteneva, tra l'altro, che la distibuzione attuata dalla società russa soddisfaceva i requisiti del reato di "trafficking", interruppe la vendita di AEBPR sul sito statunitense

329 Con riferimento al radicamento del procedimento: da http://www.eff.org/Cases/US_v_Elcom/us_v_sklyarov_faq.html: "It's not clear. As part of his work for ElcomSoft Co Ltd. in Russia, Dmitry allegedly developed the algorithms on which the AEBPR program is based and allegedly wrote some of the AEBPR program. The Complaint alleges that software was available for purchase until late June at www.regnow.com, a site based in Washington D.C and is available at the ElcomSoft company's site. The prohibition in section 1201(b)(1)(A) of the DMCA is against "any person" from

Il 30 agosto 2001, dopo la prima udienza fissata per il 23 dello stesso mese, Skyliarov comparve davanti ai giudici americani gravato di tutte la accuse in precedenza descritte.
A Sklyarov, lasciato a piede libero dopo quasi un mese passato in cella, fu ritirato il passaporto e, contestualmente gli fu inibito di oltrepassare i confini della California, dove avrebbero avuto luogo le udienze preliminari relative al suo caso.
Più che da convinzioni di probabile innocenza, per altro mai chiaramente assunte dalla Corte degli Stati Uniti, il rilascio del programmatore fu la conseguenza del ritiro della denuncia sporta nei suoi confronti dalla Adobe, in considerazione, soprattutto, dei riscontri di mercato estremamente negativi causati dal boicottaggio[330] dichiarato in Rete nei confronti della stessa *software house*[331].
Il 13 dicembre 2001 il Giudice della Corte Federale Ronald White, firmò finalmente l'ordine che permise a Sklyarov di fare ritorno a casa dopo cinque mesi di soggiorno forzato negli Stati Uniti.
Tale atto, se da un lato può definirsi "dovuto" ed ovvio da parte di chi considera con altri parametri l'utilizzo di tecnologie che consentono principalmente usi legittimi, dall'altro è invece conseguito ad un accordo intercorso tra Sklyarov e la giustizia americana. In pratica, in cambio della testimonianza[332] resa dal programmatore contro la società per cui lavorava, tutte le accuse mosse nei suoi confronti furono cancellate.
Una volta caduta l'accusa nei confronti di Sklyarov, il governo statunitense ritenne ancora che la società russa *ElcomSoft* dovesse essere considerata responsabile criminalmente per aver creato AEBPR.

---

manufacturing, importing, providing, offering to the public or otherwise trafficking in a circumvention technology. On the assumptions (which of course are by no means proved) that AEBPR would be found to be a circumvention device under section 1201(b)(1) and that it would be found that that program was distributed within the US, it could be argued that Dmitry assisted his employer in manufacturing such a tool in Russia. However, the DMCA anti-circumvention provisions would not likely be triggered by manufacture in Russia, and it is EFF's understanding that manufacturing such a tool is not illegal in Russia. EFF also understands that Dmitry was not involved in distributing the program in any way. People have speculated that action was taken against Dmitry because he was on US soil for the Def Con conference, and his physical presence would make it easier for the government to establish jurisdiction under US law. According to the Affidavit filed by the FBI Special Agent in support of the criminal Complaint, the FBI appear to have arrested Dmitry on the basis that they believed that he (and not ElcomSoft) was the person who owned the copyright rights in the AEBPR program. The FBI's Affidavit (para 20) and the Department of Justice's Press Release on 17 July both refer to Dmitry's ownership of the copyright. The current version of AEBPR (2.2) appears to list ElcomSoft Co. Ltd. as the copyright holder on its opening window".

330 Fu addirittura creto allo scopo un sito: http://www.boycottadobe.org (sito consultato il 15 giugno 2002) .

331 Numerosi siti Web, gruppi di attivisti (soprattutto quelli legati al *software* libero ed *open source* e alle altre comunità *hight.-tech*), esercitarono notevoli pressioni volte ad ottenere la liberazione di Sklyarov, e contestualmente l'armonizzazione delle norme chiaramente incostituzionali poste in materia ed applicate dalle Corti statunitensi. In varie città americane, fra cui San Francisco, Boston, New York, Washington e San Josè, furono organizzati cortei di protesta: il 6 agosto, ad esempio furono in molti ad attendere davanti ai cancelli della Corte, proprio a San Josè, la decisione sulla richiesta di rilascio presentata dalla difesa di Sklyarov.

332 Si veda http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20020204_eff_elcom_pr.html

Anche se in parte l'obiettivo dell'EFF era stato raggiunto con la liberazione di Sklyarov, rimanevano irrisolti i "veri" problemi che si ponevano alla base di tutta la questione.
Il 4 febbraio 2002, infatti, la EFF depositò una memoria amichevole alla Corte Distrettuale Federale nella quale si chiedeva che il DMCA fosse dichiarato incostituzionale a causa del suo conflitto con alcune libertà fondamentali, *in primis* la libertà di parola, garantite appunto dalla Carta Costituzionale. Inoltre, il contenuto della memoria sottolineava quanto lo stesso DMCA nuocesse allo sviluppo delle nuove tecnologie ponendo ostacoli giudiziari insormontabili.
Secondo la EFF, il formato ideato ed applicato dalla Adobe per proteggere gli e-Book, oltre a porre gravi ostacoli al pieno e corretto utilizzo del bene acquistato, impone all'utente un unico impiego dello stesso, per altro totalmente "controllato" dagli editori.
Il Primo Emendamento dovrebbe, sempre secondo l'EFF, proteggere i diritti degli acquirenti degli *e-Book*, e non solo gli editori e le società che cercano di "bloccare" i formati in questione.

3. Il DMCA in rapporto alla normativa europea: considerazioni.

Il 22 maggio 2001 Parlamento e Consiglio Europeo hanno approvato la Direttiva 2001/29/CE sulla "armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione"[333].
Con l'accoglimento delle norme in essa comprese, ed in particolare dell'art. 6, in Europa si recepisce una tutela giuridica delle misure tecnologiche di protezione delle opere digitali che si pone sostanzialmente sulla scia del DMCA americano[334].
L'art. 6 pone a carico degli Stati membri l'obbligo di prevedere una protezione giuridica "adeguata", non solo allo scopo di evitare l'aggiramento delle predette misure, ma anche diretta ad impedire il traffico di dispositivi tecnologici e dei servizi atti ad aggirarle.
L'art. 7, invece, prevede la punibilità giuridica di chiunque compia, consapevolmente e senza averne diritto, atti tesi alla rimozione, alterazione di qualsiasi informazione elettronica sul regime dei diritti[335] (comma 1, lett. a)).

---

333 Il testo della Direttiva è reperibile al link http://europa.eu.int/comm/internal_market/en/intprop/news/index.htm

334 Da considerare come i due testi legislativi siano entrambi ispirati ai trattati della WIPO del 1996 ed alla Convenzione di Berna del 1971 in materia di diritto d'autore.
http://clea.wipo.int/lpbin/lpext.dll/clea/LipEN/46e4b/48c86?f=file[document.htm]#JD_754ab

335 Nel secondo comma è chiarito che la locuzione "informazione sul regime dei diritti" corrisponde, ai fini della Direttiva, qualunque informazione, fornita dai titolari dei diritti, che identifichi l'opera o i materiali protetti dal diritto sui generis di cui al capIIIdella Dir. 96/9/CE circa i termini e le condizioni d'uso dell'opera o di altri materiali nonché aqualunque numero o codice che rappresenti tali informazioni; l'autore o qualsiasi altro titolare dei diritti; "comunque" qualsiasi informazione circa i termini e le condizioni d'uso dell'opera o di altri materiali; qualsiasi numero o codice che rappresenti tali informazioni;

Inoltre, lo stesso articolo, condanna anche altre azioni, consistenti nel distribuire o importare ai fini della distribuzione, nel diffondere per radio o televisione, e nel comunicare o mettere a disposizione del pubblico opere o altri materiali protetti ai sensi della stessa direttiva o del capitolo III della Direttiva 96/9/CE dalle quali siano state rimosse o alterate, senza averne diritto, le informazioni elettroniche sul regime dei diritti (comma 1, lett. b)).
Come è facile immaginare, proprio a causa della accentuata similitudine delle norme in questione con quelle del DMCA, i problemi che, nelle relative materie, inevitabilmente si porranno in Europa saranno simili a quelli sempre più spesso caratterizzano le liti in materia nelle Corti americane.
Così, rifacendosi a quanto più volte sottolineato dalla EFF e da altre organizzazioni, con in testa quelle che sostengono il software libero, possono individuarsi, quali problematiche fondamentali, i pesantissimi (ed insormontabili) limiti imposti da simili impostazioni legislative tanto alla ricerca scientifica e tecnologica, quanto all'innovazione ed al progresso conseguenti.
Risulta inoltre necessario chiedersi, sempre sulla base di quanto è accaduto ed ancora continua ad accadere in America, quale sarà l'impatto della Direttiva in questione e delle altre norme che la hanno seguita o che verranno in futuro, su quello che negli USA è definito "fair use".
In Europa il problema rischia, anzi, di risultare ancora più grande. Infatti, anche e soprattutto a causa della immancabile pressione delle potenti lobby, tali problematiche vanno a toccare direttamente anche un'altra importante questione: quella della brevettabilità del software[336].
In pratica, come sottolineato anche da Lessig[337], tanto le pressioni lobbystiche, quanto le attuali norme in materia, costituiscono niente altro che una "intimidazione". In particolare Lessig sottolinea come il diritto di testare la sicurezza delle protezioni elettroniche anti-pirateria ed il fatto di lavorare per cercare soluzioni che vadano a migliorarne i punti deboli, "dipende dal proprio datore di lavoro". Se si lavora per l'industria, ricerca ed innovazione sono un diritto; in caso contrario, lo stesso esercizio dello stesso diritto diviene una grave violazione di legge, perseguibile tanto in sede civile quanto in quella

---

[336] Attualmente a livello istituzionale solo da parte della Francia, ed in particolare dalla voce del segretario di Stato Christian Pierret, si è voluta affermare con forza la contrarietà al regime del brevetto imposto al software; ciò, sempre secondo il segretario, anche in considerazione dell'incoraggiamento offerto dalla formula del brevetto al "terrorismo giuridico", inteso come grande aumento dei processi chiesti dai grandi operatori commerciali contro le piccole software house e contro le giovani e brillanti menti che "non vogliano" eventualmente lavorare per le stesse grandi imprese preferendo diverse soluzioni professionali. Anche in altri paesi parte delle istituzioni hanno fatto sentire la propria voce in materia di brevetto. In Germania, dove come in Francia ed in altri Paesi è lecito l'impiego di software libero nell'ambito della Pubblica Amministrazione, i partiti politici hanno dichiarato la propria contrarietà all'applicazione di tale modello per la tutela dei *software*. Nei Paesi Bassi il parlamento ha imposto una chiara presa di posizione sull'argomento, mentre in Danimarca forti associazioni di professionisti si oppongono fermamente alla medesima questione.

[337] In particolare, sull'argomento si consiglia la lettura dell'intervista di Richard Koman a Lawrence Lessig (il cui testo completo è reperibile al link http://www.openp2p.com/pub/a/p2p/2001/08/07/lessig.html sito consultato il 10 luglio 2002).

penale. Il risultato di tale operazione, sottolinea ancora Lessing, non può che essere la concentrazione del potere di ricerca, e quindi di innovazione tecnologica, nelle mani di poche e potenti società che, occupandosi di "digital rights management", favoriscono spudoratamente gli interessi della grande industria.
Tanto in Europa quanto negli Stati Uniti d'America, la disciplina del diritto d'autore nasce come compromesso e quindi da un delicato bilanciamento di interessi (totalmente contrapposti) che, tralasciando in questa sede tutte le altre questioni attinenti, si concretizza, dal punto di vista dell' utente con la previsione di un (limitato, anzi limitatissimo) diritto di libera riproduzione delle opere regolarmente acquistate o comunque possedute.
Proprio le protezioni tecnologiche poste a tutela delle opere e così previste dalle norme di legge, rischiano poi di non consentire nemmeno questo limitato godimento di diritti, ricordiamolo ancora, regolarmente acquisiti.
Interpretando alla lettera l'art. 6 della Direttiva, che introduce una ulteriore ipotesi di reato che non riguarda la violazione dei diritti esclusivi degli autori o dei titolari dei diritti connessi, si evince infatti che il solo utilizzo di un dispositivo, di qualsiasi natura, idoneo a bypassare la protezione di un'opera digitale, indipendentemente dal tipo di utilizzazione che riguarderà l'opera copiata, costituisce reato.
Naturalmente tale impostazione normativa coinvolge anche attività che, volendo accogliere il concetto americano di "fair use", dovrebbero invece rimanervi escluse.
Il DMCA, proprio in relazione a questo problema, precisa che l'aggiramento delle misure tecnologiche di protezione è illecito esclusivamente quando abbia ad oggetto l'elusione di sistemi che controllino l'accesso ad opere protette, mentre risulta lecito quando riguarda misure poste allo scopo di impedire la riproduzione delle medesime.
Se, in America questo spiraglio è da considerarsi un riconoscimento, seppure minimo ed interpretabile, di interessi diversi da quelli delle grandi aziende, in Europa la situazione rischia dia apparire anche più grave. Infatti, nel vecchio continente, non è stata stabilita a riguardo alcuna distinzione. Anzi il regime ivi previsto richiede, per la realizzazione di una copia per uso privato effettuata da una persona fisica, il percepimento da parte dei titolari dei diritti, di un "equo compenso che tenga conto dell'applicazione o meno delle misure tecnologiche (di protezione)".
Questo quadro normativo si pone però in chiaro contrasto con quanto stabilito nell'art. 6 al par. 3., dove agli Stati membri è richiesta, "in deroga alla tutela giuridica del paragrafo 1, e in mancanza di misure volontarie prese da titolari […], di prendere provvedimenti adeguati affinché i titolari mettano a disposizione del beneficiario di un'eccezione[338] i mezzi per fruire della stessa".

[338] Tra cui rientra "l'uso privato".

Capitolo Sedicesimo

IL CASO DECSS

Sommario: 1. Introduzione. - 2. 2. I precedenti sulla legge sul diritto d'autore negli Stati Uniti. - 3. I recenti sviluppi nella vicenda Deccs: *DVD Copy Control Ass. v. Andrew Bunker.* - 4. Conclusioni.

1. Introduzione.

La digitalizzazione dei brani musicali e delle pellicole cinematografiche dal loro precedente formato analogico[339] ha rivoluzionato il modo di distribuire i prodotti sottoposti a copyright da parte dell'industria dell'intrattenimento[340]. Il formato digitale è ormai lo standard con il quale vengono distribuite sia le nuove che le vecchie registrazione di audio e video.
Tuttavia, così come negli anni ottanta la riproduzione non autorizzata di audio e video cassette aveva costituito una vera e propria minaccia per l'industria dell'intrattenimento così il formato digitale sta creando simili preoccupazioni[341].
I primi segnali in tal senso, furono rilevati dalla giurisprudenza americana nel caso *Sony Corporation of America v. Universal City Studios*[342]. In quell'occasione infatti la Corte Suprema giudicò che la commercializzazione del Video Tape Recorders prodotto dalla Sony, usato per le registrazioni e successive riproduzioni ad uso domestico dei programmi televisivi sottoposti a copyright, costituiva un caso di "*fair use*"[343]. In quel caso la Corte rilevò inoltre che un fabbricante non poteva essere ritenuto responsabile per la vendita di 'staple article of commerce' il quale sia 'capable of commercially significant [or substantial] noninfringing uses'[344].
Il caso Sony è il caso che ha segnato la strada per quelle che oggi sono conosciute, in common law, come le regole giurisprudenziali del "*fair use*" e del

---

339 Tecnicamente la procedura prevede l'utilizzo di un ADC, acronimo di **A**nalog To **D**igital **C**onverter, un convertitore analogico/digitale. Come il nome lascia intendere, è appunto un circuito che trasforma il segnale analogico in forma numerica campionandolo parecchie volte al secondo *(procedura di campionamento)*, assegnando un valore a ciascuno di questi campioni *(quantizzazione)* e restituendoli in uscita in forma di numeri binari *(codifica)*.

340 Cfr. Charles L. Simmons Jr., *Digital Distribution of Entertainment Content -- The Battle Lines Are Drawn,* July/August 2000 - Maryland Bar Journal, 32 anche all'URL http://www.gandwlaw.com/articles/ent_cont.html.

341 Sull'argomento si veda Benton J. Gaffney, *Copyright Statutes that Regulate Technology: A Comparative Analysis of The Audio Home Recording Act and the Digital Millennium Copyright Act*, 75 Wash. L. Rev. 611, 629 (April 2000).

342 Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417

343 Il *fair use* (o come diremo noi il "uso corretto – giusto utilizzo") è un concetto sociale, civile e giuridico formulato negli Stati Uniti, una teoria e prassi delle eccezioni al profitto derivante da diritti d'autore in quei contesti istituzionali di utilizzo pubblico ed educativo delle risorse altrimenti sottoposte a copyright. Vedasi diffusamente <http://fairuse.stanford.edu> vero e proprio punto di riferimento per la pubblicistica relativa al f*air-use.* Dopo il caso Sony la dottrina del *fair use* è stata codificata nella sezione 107 del Copyright Act (17 U.S.C. 107).

344 Cfr. Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 p. 442.

"staple article of commerce"[345]. Entrambi i principi sono metodi di difesa che possono essere invocati per una violazione del diritto d'autore che impone l'onere della prova a carico dell'imputato della violazione.
Circa 15 anni dopo la sentenza "Sony" la digitalizzazione dei contenuti dei video tape, dalla videocassetta al DVD, è esplosa sul mercato. Oggi infatti, l'industria cinematografica distribuisce la maggior parte dei propri prodotti sottoposti a diritto d'autore proprio in formato digitale su DVD, un disco che può essere letto e visualizzato attraverso appositi apparecchi di lettura (DVD player) o personal computer[346]. Un sistema di criptazione anticopia per i file contenuti all'interno di un DVD, conosciuto come Content Scrambling System (Sistema di Cifratura del Contenuto o "CSS"), dovrebbe proteggere le pellicole dell'essere decriptate, copiate o semplicemente viste senza un opportuno decodificatore (hardware o software) che conosca il sistema di decriptazione[347]. I DVD messi in commercio dalle Major americane hanno perciò al loro interno delle informazioni che identificano univocamente il continente (o una "regione" del mondo) nel quale tali DVD devono essere venduti[348]. I lettori, a loro volta, sono in grado di leggere i soli DVD della regione nella quale essi stessi sono stati venduti in quanto possiedono l'appropriato algoritmo che ne permette la decodifica. Tuttavia, sebbene i DVD possano essere copiati senza perdita di qualità, il procedimento di copia e distribuzione non autorizzata preoccupa l'industria cinematografica assai meno di quanto accadde in seguito all'introduzione dei Video Tape Recorders della Sony: infatti i DVD non contengono una sofisticata tecnologia di compressione. Di conseguenza il trasferimento digitale ed integrale delle pellicole comporta l'occupazione di grosse quantità di "spazio disco" e dunque copiare è meno fattibile perchè i tempi di download e di trasferimeto sono enormi[349].

2. I precedenti sulla legge sul diritto d'autore negli Stati Uniti.

---

345 Letteralmente: "dottrina del prodotto fondamentale del commercio".

346 Di fatto i lettori di DVD sono l'equivalente funzionale dei Video Tape Recorders (i.e. videoregistratori). Si veda in tal senso Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d at 310.

347 Per una spiegazione sullo sviluppo della tecnologia del Content Scrambling System si veda Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d p. 308.

348 La DVD Content Control Association [http://www.dvdcca.org/] sostiene che tale codifica regionale è stata messa a punto per impedire che qualcuno possa ad esempio comprare un DVD negli U.S.A. tramite internet e vederlo in Italia prima che questo sia uscito nelle sale cinematografiche (insieme all'ulteriore pericolo di una distribuzione illegale addirittura anticipata). La codificazione regionale dei DVD permetterebbe infatti ad una pellicola di essere diffusa su DVD in una regione anche se ancora in programmazione nelle sale di un' altra regione perché la codificazione regionale assicura che non interferirà con la programmazione cinematografica. Senza codificazione regionale, tutti i fruitori "domestici" dovrebbero attendere fino al momento in cui la pellicola non abbia completato la relativa distribuzione nelle sale di tutto il mondo prima di avere a disposizione il relativo DVD.

349 Per una dettagliata analisi della procedura di veda Charles L. Simmons Jr., *Digital Distribution of Entertainment Content -- The Battle Lines Are Drawn,* Maryland B.J., Vol. XXXIII, Number 4, July/August 2000, p. 33.

La necessità di una legge sulla protezione del diritto d'autore trova la propria origine nel periodo coloniale come una risposta alle leggi britanniche di censura e all'invenzione del torchio tipografico[350]. Sin dall'inizio, la legge sul diritto d'autore ha cercato di equilibrare l' esigenza della libertà d' espressione con il desiderio di incoraggiare i miglioramenti tecnologici [351]. Attualmente la legge sul diritto d'autore del 1976[352] (the "Copyright Act" o il "1976 Copyright Act") stabilisce che "copyright protection subsists ... in original works of authorship fixed in any tangible medium of expression, now known or later developed"[353].
Generalmente, i diritti d'autore sulle pellicole e sui brani musicali sono ripartiti fra gli autori ed i produttori. Gli artisti ed i membri della RIAA[354] (l'associazione delle case discografiche americane) sono compensati per il loro lavoro creativo dalla vendita delle registrazioni e dalle tasse di concessione (*license fees*)[355]. Nel caso degli attori e della Motion Picture Association of America (MPAA)[356], la compensazione viene dalla vendita e dal noleggio dei videos, delle vendite dei biglietti nelle sale cinematografiche e dalle tasse di concessione[357].

A norma del Copyright Act del 1976, ai titolari di diritto d'autore sono riconosciuti diritti esclusivi: il diritto di riprodurre l'opera protetta, il diritto di distribuire copie dell'opera al pubblico e il diritto di rendere pubblica l'opera protetta[358]. In qualsiasi caso questi diritti esclusivi non siano rispettati, si incorre in uno dei casi di violazione del diritto d'autore.
Il diritto statunitense infatti riconosce tre tipi diversi di responsabilità per violazione del Copyright: il primo tipo di responsabilità è quella attribuita al soggetto che ha direttamente compiuto la violazione (*direct liability*)[359]. La responsabilità per fatti causati da terzi è invece distinta in due differenti tipologie: la responsabilità da concorso colposo (*contributory liability*)[360], che si ha

---

350 Si veda in tal senso Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 p. 430 n.12.
351 Ibidem
352 Il Copyright Act of 1976 fu promulgato il 19 ottobre del 1976, Public law number 94-553, 90 Stat.*2541* (titolo 17 del United States Code § 101).
353 Cfr. 17 USC § 102 (a).
354 Recording Industry Association of America.
355 Cfr. Ariel Berschadsky, *RIAA v. Napster: A Window Onto the Future of Copyright Law in the Internet Age*, 18 J. Marshall J. Computer & Info. L. 755, 762 (2000).
356 Le aziende che fanno parte del MPAA (www.mpaa.org) includono: Universal City Studios, Inc., Paramount Pictures Corporation, Metro-Goldwyn-Mayer Studios, Inc., Tristar Pictures, Inc., Colombia Pictures Industries, Inc., Time Warner Entertainment Co., L.p., Disney Enterprises, Inc. e ventesimo Century Fox Film Corporation.
357 Per una semplice analisi sul sistema dell'industria dell'intrattenimento si veda John Jackson, *Royalty Securitization: Taking Cabs to Bankruptcy Court*, 21 T. Jefferson L. Rev. 209, 212 (2000)
358 17 USCS § 106
359 Per la *direct liabilty* il titolare del diritto deve provare: "(1) valid copyright ownership of a work; (2) the work was, in fact, copied; and (3) the copying of work was illegal under copyright laws." Vd. Marshall Leaffer, *Understanding Copyright Law*, 2 ed., N.Y., 1995.
360 Per la *contributory liability* il titolare del diritto dovrà provare "(1) a direct infringement occurred[;] (2) the defendant knew or had reason to know of the infringing activity[;] and (3) the defendant substantially participated in the infringement by inducing, causing, or materially

quando il soggetto responsabile, pur non essendo il diretto esecutore della violazione, contribuisce in un qualche modo alla sua realizzazione e ne è a conoscenza (*actual knowledge*) o comunque ha motivo di esserlo (*reason to know*), e la responsabilità indiretta (*vicarious liability*)[361], che si verifica quando il soggetto responsabile ha il compito e la possibilità di controllare (*the right and ability to supervise*) l'attività svolta dal terzo che ha direttamente commesso la violazione e quando, a seguito di questa, tragga un vantaggio economico. In quest'ultimo caso nessun valore è dato al fatto che il responsabile indiretto conoscesse o meno il comportamento illecito del terzo.

Nel dicembre del 1996 due trattati furono adottati dall'Organizzazione Mondiale per la Proprietà intellettuale (WIPO)[362]: WIPO Copyright Treaty[363] e WIPO Performances and Phonograms Treaty[364]. Questi trattati sono stati studiati per fornire alle nazioni contraenti, compreso gli Stati Uniti, una protezione legale efficace per gli autori di materiale protetto da diritto di Copyright contro atti di pirateria digitale commessi attraverso Internet. Come conseguenza del WIPO, il congresso degli Stati Uniti ha promulgato il Digital Millenium Copyright Act (DMCA)[365].

Questo è, sommariamente, lo scenario in cui si deve leggere la vicenda del cd. "Decss".
Nel settembre del 1999, infatti, un quindicenne norvegese di nome Jon Johansen e due, non ben identificati, individui da lui incontrati nel web, crearono un programma in grado di violare l'algoritmo di crittografia CSS, e quindi di "sproteggere" un DVD e copiarne il suo contenuto su un Hard Disk[366]. La giustificazione alla "violazione" della codifica nasceva tuttavia dal

---

contributing to its occurrence." Vd. Pollack Wendy M., Tuning in: *The future of Copyright Protection for Online Music in the Digital Millenium,* vol.78, Fordham L. Rev.,n. 6, 2000, p. 2456.

361 Per la *vicarious liability*, l'attore dovrà provare che il convenuto aveva "the right and ability to supervise the infringing activity and also has a direct financial interest in such activities" Vd. Ibidem

362 World Intellectual Property Organization

363 World Intellectual Property Organization Copyright Treaty, Dec. 20, 1996.

364 World Intellectual Property Organization Performances and Phonograms Treaty, Dec. 20, 1996.

365 Il DMCA si pone non solo come mera disposizione di attuazione dei sopraccitati trattati internazionali, ma come vera e propria miglioria degli stessi. In particolare esso mira ad una articolata disciplina della fruizione del materiale protetto da Copyright all'interno degli Stati Uniti e disponibile esclusivamente nel formato digitale. La norma si compone di cinque titoli: Titolo I: Implementazioni al vigente WIPO "Copyright and Performances and Phonograms Treaties"; Titolo II: "Online Copyright Infringement Liability Limitation Act"; Titolo III: "Computer Maintenance Competition Assurance"; Titolo IV: Una serie di previsioni varie, riguardanti in particolar modo l'ufficio del Copyright, l'educazione a distanza e le esenzioni dalle disposizioni di questa legge; Titolo V: "Vessel Hull Design Protection Act".

366 Il programma DeCSS si presenta come un' unica finestra in cui, in una sezione, vengono scelti il lettore DVD, il calcolo dello spazio sul disco, la possibilità di unire i file decriptati .VOB (l'estensione dei file presenti sul DVD-Video) e una finestra di stato; nell'altra sezione vengono elencati i file presenti sul DVD-Video in modo da scegliere solamente quelli che contengono sequenze video (in genere solo i file di grosse dimensioni, di circa 1 Gigabyte ciascuno). Scelti i file da decriptare, si sceglie il percorso di destinazione in cui memorizzare i

fatto che per l'ambiente Linux non esisteva alcun player DVD e quindi gli utenti non potevano fruire di questo nuovo standard emergente[367]: il DVD, infatti era programmato per funzionare solo su Windows e l'unico mezzo per consultarne il contenuto su un sistema operativo diverso, era quello di rompere il codice crittografico. Tuttavia Johansen non si era limitato a ciò, ma, pubblicando[368] sul proprio sito i sorgenti del programma, (come è prassi per tutto il software *open source*) ha reso disponibile al mondo intero il suo metodo di decodifica.

Nel Novembre del 1999, il convenuto nel giudizio Universal City Studios v. Reimerdes[369], Eric Corley, editore della rivista on-line *2600*[370] *"The Hacker Quarterly"* pubblicò i sorgenti del programma Decss sul proprio sito[371]. Da questo sito i visitatori erano in grado di fare direttamente il *download* del software o potevano essere invitati a farlo attraverso altri siti i cui *links* erano pubblicati in liste sulla stessa rivista[372]. Nell'ottobre del 1999 la MPAA incominciò a diventare cosciente dell'invio tramite internet del software di decriptazione e cercò di porvi rimedio inviando, ai siti in questione, lettere che invitavano a mettere fine a questo tipo pubblicazione. Poiché il sito *2600.com* non aderiva alle richieste, la MPAA, nel gennaio del 2000, intentò una causa contro Corley, al fine di costringere *2600.com* a cessare la pubblicazione (*posting*)

---

file sul disco, quindi si può iniziare il trasferimento. Il processo è abbastanza veloce, bastano circa 10 minuti su un sistema a 500 MHz, tenendo presente che occorre però molto spazio sull'hard disk: un unico DVD-Video infatti può arrivare ad occupare mediamente 4 o 5 Gigabyte. Una volta copiati e decifrati, i file possono essere riprodotti proprio come se si stesse utilizzando un disco DVD, semplicemente utilizzando un qualsiasi player software. Il problema resta tuttavia quello che una volta copiato il contenuto del DVD sull'hard disk, questo occupa moltissimo spazio disco. Per ovviare a ciò esistono sistemi di compressione (e.g. DivX) che permettono di "riversare" il contenuto di un DVD in due CD-ROM.

367 Già alcune società hanno "lanciato" software DVD per il sistema operativo Linux. Vista la mancanza supporti DVD per Linux, alcuni utenti dei sistemi operativi *open source* (a sorgente libero) erano costretti ad installare sia Linux che Windows nei loro computer per poter avere giochi e film in DVD.

368 Attraverso un'attività di *Posting*, che significa "affiggere" cioè mettere un testo dove può essere letto pubblicamente (il termine è comunemente usato anche per indicare l'affissione di un articolo in una bacheca elettronica e talvolta ne nasce il neologismo italiano "postare").

369 Nelle corti statunitensi sono attualmente in discussione almeno tre casi che coinvolgono questioni inerenti il Decss: uno è il citato caso Universal City Studios v. Reimerdes (attualmente in appello di fronte alla Court of Appeals for the Second Circuit N.Y.), il secondo è il caso californiano DVD Copy Control Assoc. v. McLaughlin, Case No. CV 786804 (dove la DVD Copy Control Association ha denunciato 72 persone accusandole di appropriazione indebita dei segreti commerciali relativi al CSS e diffusione ostinata dello stesso attraverso l'attività di *linking*) ed infine, il meno conosciuto Universal City Studios, Inc. v. Hughes, Case No. 300CV72 RNC (un caso sempre basato sulla presunta violazione del titolo 17 U.S.C. § 1201).

370 www.2600.com

371 Universal City Studios v. Reimerdes, 111 F. Supp. 2d, 308-309.

372 Universal City Studios v. Reimerdes, 111 F. Supp. 2d, 311-312 "….defendants' web site began to offer DeCSS for download. It established also a list of links to several web sites that purportedly "mirrored" or offered DeCSS for download".

e successivamente l' "electronic civil disobedience" ovvero il *linking* ad altri websites che mettevano in rete la tecnologia DeCSS[373].
Nel caso *Reimerders* la MPAA ha sostenuto che l'attività di posting e linking del codice Decss da parte del convenuto 2600.com viola il paragrafo 1201(a)(2) del DMCA[374], ovvero la previsione relativa alle misure anti-raggiro (*anti-circumvention*) del copyright.

> *§ 1201. Circumvention of copyright protection system*
>
> (a) Violations regarding circumvention of technological measures.
>
> (1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter [enacted Oct. 28, 1998].
>
> (B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).
>
> (C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine—
>
> (i) the availability for use of copyrighted works;

---

373 La causa iniziale era stata intentata contro Corley ed altri due convenuti che successivamente hanno preso parte agli accordi con i querelanti.
374 La citazione esatta sarebbe: violazione del titolo 17 U.S.C. § 1201 (a)(2). Il titolo 17 U.S.C. 1201, introdotto dal DMCA, stabilisce delle sanzioni penali per l' aggiramento di una tecnologia che "effectively controls access" a materiale protetto da copyright, come pure il la fabbricazione o la messa a disposizione dei dispositivi pubblici finalizzati ad aggirare i meccanismi di controllo dell' accesso.

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;
(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and
(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

I convenuti hanno di contro sostenuto che le attività di *Linking* e *posting* aventi ad oggetto il codice Decss rientravano nella definizione di "*fair use*" prevista dal

Copyright Act[375]. Essi inoltre ipotizzarono una violazione del Primo Emendamento, sostenendo che il DMCA violerebbe la libertà d'espressione se applicato ai programmi per computer e ai loro codici.
Il giudice Kaplan, della U.S. District Court for the Southern District of New York, ha tuttavia sostenuto[376] che l'attività di *posting* e *linking* messa in pratica dal convenuto fosse una evidente violazione del DMCA disponendo a favore dei querelanti un risarcimento e un "*injuction and declaratory relief*"[377].
La Corte in primo luogo ha ritenuto che il Decss "clearly is a means of circumventing a technological access control measure". Secondariamente la Corte ha riconosciuto che il CSS effettivamente controlla l'accesso ai dati contenuti nei DVD dei querelanti e dunque questo sistema ricade nelle previsioni della sezione 1201 (a) (2) (A) poiché "in the ordinary course of its operation, [the measure] requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work"[378]. In terzo luogo, dato che il solo scopo per la creazione del DeCSS era la decriptazione del CSS, si può desumere che questo sia stato destinato soprattutto per "aggirare" il CSS[379]. Perciò la Corte ha sostenuto che attraverso l'invio del codice sulla rete nelle pagine di 2600.com, i convenuti hanno chiaramente violato la sezione 1201(a)(2)(A) del DMCA. Attraverso la stessa analisi, la corte ha concluso che i convenuti avevano egualmente violato la sezione 1202(a)(2)(B) perché lo scopo o l' uso primario del DeCSS era quello di aggirare il sistema di protezione CSS. Dall'altra parte gli accusati hanno cercato di sostenere che il DeCSS potesse rientrare tra le eccezioni all'aggiramento dei sistemi di protezione del Copyright[380] previste dallo stesso DMCA ovvero il c.d. "reverse engineering"[381], l' "encryption research"[382] e il "security testing"[383].

---

375 Vd. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 321-322.

376 "In the final analysis, the dispute between these parties is simply put if not necessarily simply resolved. Plaintiffs have invested huge sums over the years in producing motion pictures in reliance upon a legal framework that, through the law of copyright, has ensured that they will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure. Defendants, on the other hand, are adherents of a movement that believes that information should be available without charge to anyone clever enough to break into the computer systems or data storage media in which it is located. Less radically, they have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era. Each side is entitled to its views. In our society, however, clashes of competing interests like this are resolved by Congress. For now, at least, Congress has resolved this clash in the DMCA and in plaintiffs' favor. Given the peculiar characteristics of computer programs for circumventing encryption and other access control measures, the DMCA as applied to posting and linking here does not contravene the First Amendment. Accordingly, plaintiffs are entitled to appropriate injunctive and declaratory relief. SO ORDERED. Dated: August 17, 2000 Lewis A. Kaplan" - . Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 346.

377 Un provvedimento dichiarativo dell'illegalità dell'atto e al contempo di divieto nella continuazione dei comportamenti considerati illegali.

378 Vd. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 318.

379 Vd. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 318-319. 17 U.S.C. 1201(a)(2)(A).

380 17 U.S.C. 1201(f), (g)(4), e (j).

381 Il *reverse engineering* (definizione intraducibile in italiano "ingegneria dell'inversione") indica tutti quei procedimenti di manipolazione ed analisi di un software a partire dal suo codice

Tale linea di difesa era motivata dal fatto che il Decss "is necessary to achieve interoperability between computers running the Linux operation system and DVDs"[384]e dunque il *reverse engeneering* sarebbe stato motivato dalla necessità di identificare e di analizzare quegli elementi del programma necessari a realizzare la interoperatività di un programma destinato ad un determinato tipo di sistemi operativi con altri sistemi per i quali, precedentemente, non era stato messo a disposizione. Nel rigettare questo argomento, il giudice Kaplan ha dichiarato che l'eccezione di *reverse engeneering* si applica soltanto a coloro che realmente hanno acquisito le informazioni attraverso il procedimento di *reverse engeneering*. Pertanto questa eccezione non può essere fatta valere dai convenuti poiché essi non avevano creato il Decss ma si erano limitati a renderlo disponibile attraverso il web (*posting*) dopo che era stato creato o scoperto da qualcun altro. Inoltre anche se uno degli scopi degli sviluppatori del DeCSS era quello di creare un DVD player per Linux, il giudice Kaplan ha rilevato come ciò non fosse il solo scopo, così come sarebbe previsto per l'applicazione dell' eccezione di *reverse engineering*, perché il DeCSS è stato sviluppato sul sistema operativo Window, un sistema operativo ampiamente usato[385]. La corte ha poi egualmente rigettato le altre due eccezioni perché assolutamente non corrispondenti alle fattispecie astratte previste dal DMCA.
Per quanto poi riguarda il *linking*[386] ad altri siti web che pubblicano il Decss, la Corte ha ritenuto questa attività equivalente al rendere disponibile il codice del programma, direttamente dal proprio sito[387] in particolare se si è a conoscenza del contenuto di materiale che viola qualche legge[388].

---

finale senza bisogno dei sorgenti. Un programmatore infatti crea un software usando dei linguaggi di medio e altro livello ma vicini al suo linguaggio naturale (ad es: Java, C++, Visual basic etc), in seguito questi sorgenti vengono trasformati nel prodotto finale da un compilatore, che ha il compito di tradurre nel linguaggio della CPU le istruzioni del programma. Il prodotto finito (programma compilato) risulta direttamente eseguibile dalla macchina, ma non più comprensibile dall'uomo. Attraverso le tecniche di *reverse engineering* anche il più protetto dei programmi può essere decifrato ovvero è possibile sfruttare lo stesso codice o algoritmo creato da un'altra persona senza chiederne il diritto d'uso o la licenza al suo creatore.

382 L'*encryption research* comprende quelle attività necessarie per identificare ed analizzare i difetti e le vulnerabilità delle tecnologie di crittografia che si sono applicate prodotti coperti da Copyright, sempre ammesso che queste attività siano condotte per avanzare la condizione di conoscenza nel campo della tecnologia crittografica o per promuovere lo sviluppo di prodotti di crittografia.

383 *Security testing* significa accedere ad un calcolatore, ad un sistema di elaborazione, o ad una rete di calcolatori, solamente con lo scopo di procedere, in buona fede, a testare, studiare, o correggere, un difetto di sicurezza o una vulnerabilità, con l' autorizzazione del proprietario o del responsabile di tale calcolatore, sistema di elaborazione, o rete di calcolatore.

384 Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 320.

385 Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 320: "right to make information available extends only to dissemination 'solely for the purpose' of achieving interoperability as defined in the statute".

386 Nonostante spesso il link venga condannato e ritenuto illegale, non esiste affatto una posizione uniforme al riguardo, e alcuni giuristi ritengono che esso debba essere considerato lecito strumento di comunicazione, essenziale al sistema di comunicazione telematico e che quindi non possa essere mai vietato

387 Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 324: "Defendants are engaged in the functional equivalent of transferring the DeCSS code to the user themselves".

388 Ibidem, 341.

Un ulteriore tentativo di difesa da parte dei convenuti è stato il ricorso al Primo Emendamento della costituzione americana[389] sostenendo che il divulgare il codice (ovvero la forma nella quale il Decss esiste) che sta alla base di un programma costituisce libertà di espressione ("code is speech"), perciò non limitabile dalla legge ovvero dal DMCA. La limitazione della libertà d'espressione può infatti interviene non solo sul contenuto ma anche sul mezzo usato per veicolare il contenuto, ed avere lo stesso effetto limitativo della libertà d'espressione operata direttamente sul contenuto.
La Corte ha invece sostenuto che le regolamentazioni sul codice sono necessarie perché "the Constitution ... is a framework for building a just and democratic society ... not a suicide pact". Il Congresso dunque, possiede il potere di stabilire norme *content-neutral* che producono effetti sull'espressione come il codice di un programma. Perciò il DMCA applicato alle attività di *linking* e *posting* del Decss, non contravviene il primo Emendamento.
Il Primo Emendamento proibisce infatti al congresso di creare leggi che "abridging the freedom of speech."
La legislazione sul copyright interferisce chiaramente con determinati generi di espressione: essa impedisce il "publicity performing" o il "reproducing", senza permesso, di materiale sottoposto a diritto d'autore. In altre parole molti dei modi in cui è possibile esprimere il proprio pensiero sono stati dichiarati illegali dal Congresso[390]. E' dunque lecito affermare che la legge sul copyright nel suo insieme o, alcune sue specifiche applicazioni, debbano essere ritenute incostituzionali?
Le Corti statunitensi che si sono dovute confrontare con questa domanda hanno invariabilmente risposto in senso negativo.
Due giustificazioni sono comunemente offerte a sostegno della compatibilità del diritto di copyright e della "freedom of speech".
In primis, l'articolo 1, ottava sezione, clausola 8 della Costituzione americana[391] autorizza esplicitamente il Congresso a promuovere il progresso della scienza e delle arti "utili" fissando, per periodi limitati, agli autori ed agli inventori, il diritto esclusivo sui loro rispettivi scritti o scoperte. E non c'è alcuna indicazione data dai redattori del Primo Emendamento né da coloro che lo hanno ratificato nel senso di limitare o rendere nulla questa dichiarata potestà legislativa.
In secondo luogo, le regole giurisprudenziali sulla legislazione sul diritto d'autore operano in modo tale da assicurare che questa non interferisca eccessivamente con la capacità delle persone di esprimersi liberamente.
Specificatamente, il principio che soltanto il modo particolare in cui un opinione o un pensiero è espresso, possa essere protetto da copyright , e non il pensiero in se, garantisce che gli individui siano in grado di esprimere concetti,

---

389 "Congress shall make no law respecting an stablishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances".
390 James Boyle, "The First Amendment and Cyberspace: The Clinton Years," 63 Law & Contemporary Problems 337 (2000).
391 The Congress shall have Power "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"

fatti o argomenti senza alcuna limitazione. Ancora di più, il principio del "fair use" fornisce un porto sicuro a chi voglia fare usi ragionevoli di materiale sottoposto a Copyright per usi scientifici o didattici.
Queste considerazioni hanno condotto le Corti statunitensi ad aggirare di fatto ogni sfida costituzionale all'applicazione della legislazione sul Copyright.
Tuttavia proprio questi *cases*, scaturiti dai modi in cui la legge sul diritto d'autore è stata modificata ed applicata ad attività su Internet e quindi dall'emanazione del DMCA, hanno spinto un numero crescente di esperti di diritto e di parti in causa a suggerire che i sopraccitati metodi convenzionali per la riconciliazione tra la legge sul copyright e il Primo Emendamento necessitino di un riesame.

3. I recenti sviluppi nella vicenda Deccs: *DVD Copy Control Ass. v. Andrew Bunker*

Proprio circa un mese fa la Corte d'appello dello Stato della California, 6° distretto, in un caso scaturente dalla causa intentata dalla DVD Copy Control Association[392] (licenziataria della tecnologia CSS) contro McLaughlin ed altri, ha distolto l'attenzione degli addetti ai lavori dalla causa di New York, ribaltando la *preliminary injuction*[393] a favore dell'appellante (Andrew Bunner) proprio sulla base del Primo Emendamento.
Il fatto fa parte di quelle denuncie presentate sistematicamente alla Corte Californiana dalla DVD Copy Control Association contro decine di persone accusate di incoraggiare la pirateria poiché colpevoli di aver pubblicato su internet il programma Decss o semplicemente il codice sorgente dello stesso.
La difesa di Andrew Bunner è stata incentrata sull'assunto che il testo del Decss, ovvero il codice non compilato (e quindi non eseguibile) debba essere considerato un opera di libera espressione a prescindere dall'uso che, una volta "attivato", qualcuno può farne. In base a questa considerazione, impedire ad un sito di pubblicarlo, rappresenterebbe una palese violazione del primo emendamento del *Bill of Rights*. I giudici del tribunale d'appello hanno stabilito che allo stesso modo del software di cifratura dei contenuti (CSS), il Decss è un testo composto di codice sorgente informatico che descrive un metodo alternativo per decrittare DVD cifrati con il Content Scrambling System. Dunque, a prescindere da chi abbia scritto il programma, il Decss deve essere considerato un'espressione scritta delle idee e delle informazioni dell'autore circa la decrittazione dei DVD senza CSS. Perciò se il codice sorgente fosse compilato e quindi attivato e fatto funzionare, allora sì la risultante

---

[392] La DVD CCA si definisce "a not-for-profit corporation with responsibility for licensing CSS (Content Scramble System) to manufacturers of DVD hardware, discs and related products. Licensees include the owners and manufacturers of the content of DVD discs; creators of encryption engines, hardware and software decrypters; and manufacturers of DVD Players and DVD-ROM drives" Vd. www.dvdcca.org
[393] E' così detta negli Stati Uniti la decisione diretta a preservare lo *status quo* fino alla decisione della causa di merito.

composizione di zeri e di uno non sarebbe pensata per comunicare pensieri o idee[394].
La Corte ha perciò concluso affermando che "the source code is capable of such compilation, however, does not destroy the expressive nature of the source code itself. Thus, we conclude that the trial court's preliminary injunction barring Bunner from disclosing DeCSS can fairly be characterized as a prohibition of pure speech"[395].
La sentenza prevede dunque la cancellazione della *preliminary injuction* e il rimborso dei costi del ricorso in appello per Andrew Bunner.

Il 28 novembre scorso tuttavia La Corte d'appello di N. Y. , contraddicendo completamente questa importante decisione californiana, ha deciso all'unanimità di dar torto in appello a 2600.com e al suo editore, Eric Corley, sostenendo che il DeCSS consente all'utente di copiare il film in formato digitale e trasmetterlo istantaneamente in quantità potenzialmente infinite, di fatto riducendo le vendite dei produttori cinematografici. L'avvento di internet creerebbe dunque il potenziale per la distribuzione su scala mondiale di materiale copiato[396].

4. Conclusioni.

Sia in Europa (direttiva 29/2001/CE) che in Italia (legge 248/2000) sono state approvate due discusse leggi che vanno a sanzionare penalmente anche il solo scambio di informazioni legate ai sistemi di protezione hardware e software.
Sulla legge italiana hanno giocato, fra l'altro, le pressioni esercitate, tramite l'ambasciata di Roma, ma anche attraverso prese di posizione ufficiali, dal governo americano e dal Ministero del commercio estero Usa che ha a più riprese indicato l'Italia quale paese degno di figurare nella top list della pirateria; se nel 1998 eravamo nella Watch List, nel 1999 eravamo passati alla Priority Watch List. Soprattutto il governo Usa aveva dichiarato la ferma intenzione di deferire l'Italia al Wto (World Trade Organisation) per effettiva violazione degli impegni sottoscritti con i trattati Trips (Trade-related aspects of intellectual property).
Una situazione poco dignitosa con pesanti ricadute negative sulla credibilità politica e commerciale del nostro Paese, e da qui la necessità di un intervento normativo forse frettoloso.

IN REALTÀ, COME È GIÀ STATO DA PIÙ PARTI OSSERVATO, QUELLO CHE DOVREBBE ESSERE PUNITO È L'ABUSIVO SFRUTTAMENTO COMMERCIALE DI QUESTI SISTEMI E NON IL LORO SEMPLICE STUDIO.

---

394 "Like the CSS decryption software, DeCSS is a writing composed of computer source code which describes an alternative method of decrypting CSS-encrypted DVDs. Regardless of who authored the program, DeCSS is a written expression of the author's ideas and information about decryption of DVDs without CSS. If the source code were compiled to create object code, we would agree that the resulting composition of zeroes and ones would not convey ideas" DVD CCA, Inc. v. Andrew Bunner (11/01/01) 6th district Ct. of Appeals, CA.

395 "tuttavia il fatto che il codice sorgente possa essere così compilato non cancella la natura di espressione del codice sorgente stesso. Dunque possiamo concludere che la *preliminary injuction* che impedisce a Bunner di pubblicare il Decss possa essere ritenuta giustamente una proibizione della libertà d'espressione"

396 *US Second Circuit Court of Appeals Decision N.Y. affirming District Court ruling against defendants, in Universal v. Reimerdes (Nov. 28, 2001)*

La vicenda DECSS ha dunque evidenziato come "Technology is actually granting copyright holders more control over content than copyright law itself would require"[397]. Ma se ciò accade è perchè la stessa legge lo permette.

[397] Cfr. Lawrence Lessing, "*Preserving the Innovation Commons: What's at Stake*" keynote to the O'Reilly Conference on Peer to Peer and Web Services - url http://www.openp2p.com [traduzione: "La tecnologia sta addirittura assegnando ai titolari di copyright più controllo sopra il contenuto di quanto la legge stessa in se richiederebbe].

PARTE QUARTA

CRITTOGRAFIA, DIRITTI DI LIBERTA' E SORVEGLIANZA GLOBALE DELL'INDIVIDUO

Capitolo Diciassettesimo

CRITTOGRAFIA E SORVEGLIANZA GLOBALE

SOMMARIO: 1. Il progetto *Platform*. – 2. Le reazioni internazionali al caso *Echelon*: i rapporti del Parlamento Europeo. – 3. Il progetto 'P415'. – 4. Il sistema di intercettazione *Echelon*. – 5. *Echelon* ed Internet: lo spionaggio della posta elettronica. – 6. Dentro ad *Echelon*: il sistema dei 'dizionari'. – 7. - Il sistema dei 'dizionari' ed il controllo delle informazioni. – 8. Il progetto *Enfopol*.

1. Il progetto *Platform*.

Il giornalista e ricercatore neozelandese Nicky Hager afferma che l'integrazione di tutta la rete delle stazioni Uk-Usa che portò alla creazione di *Echelon* si è realizzata con l'introduzione del sistema *Platform*, all'inizio degli anni Ottanta[398].
Le prime notizie, con riferimento a *Platform*, si trovano nel Volume *The Puzzle Palace* del 1982[399] dello scrittore e giornalista americano James Bamford, il quale scrisse di un progetto a proposito di una rete mondiale di computer segreta, dal nome in codice 'Platform', gestita dalla *National Security Agency* ed operativa dal 1983, rete che avrebbe collegato insieme 52 sistemi di computer sparsi nelle stazioni d'ascolto disseminate in ogni parte del mondo.
Il quartier generale di questo *network* sarebbe stato la *National Security Agency*, la quale, dalla sua sede a Fort Meade, Maryland, Stati Uniti d'America, avrebbe gestito e diretto questo sistema[400].
Tutte le altre quattro agenzie facenti parte dell'Accordo Uk-Usa, il *Government Communications Head Quarters* (GCQH) britannico, il *Communications Security Establishment* (CSE) canadese, il *Defense Security Directorate* (DSD) australiano ed il *General Communications Security Bureau* (GCSB) neozelandese aderirono, anche se in tempi differenti, a questo sistema.

---

398 Cfr. N. HAGER, *Echelon: sottoposti al sistema di sorveglianza globale*, in *Covert Action Quartely*, n. 59, 1998, p. 8 (disponibile la versione originale sul sito Web http://jya.com/echelon.htm e la versione tradotta in italiano sul sito http://www.tmcrew.org/privacy/caq/sorvegli.htm, siti consultati il 20 luglio 2002).
399 Cfr. J. BAMFORD, *The Puzzle Palace - Inside the National Security Agency, America's most secret intelligence organization*, Penguin Books, New York, 1983, p. 138.
400 *Ibidem*.

Durante gli anni, questo sistema si sarebbe sviluppato in un'entità sovranazionale altamente segreta con un proprio linguaggio e proprie leggi e regole[401].
Sia Nicky Hager in *Secret Power* che James Bamford nel più aggiornato *Body of Secrets* concordano nell'affermare che l'Operazione *Platform* portò poi ad *Echelon*[402].
Effettivamente, tutte le stazioni di intercettazione delle comunicazioni appartenenti al sistema *Platform* omologarono tutto il *software* dei loro computer passando ad un programma che la *National Security Agency* aveva creato ed applicato sui propri sistemi informatici.
Platform, pertanto, collegò per la prima volta tutti i computer dei cinque Paesi facenti parte dell'Accordo Uk-Usa, omologandoli e creando così un sistema globale in materia di attività SIGINT.
Le agenzie sarebbero state, pertanto, in grado di sottoporre i propri obiettivi alle stazioni d'intercettazione gestite dalle altre agenzie, effettuando, in questo modo, una ricerca su scala mondiale ed assicurandosi uno spionaggio globale delle comunicazioni.
Con questo sistema, ciascuna agenzia avrebbe condiviso il proprio materiale con le altre in maniera pressoché automatica, in quanto tutto il lavoro sarebbe stato svolto autonomamente dai computer dei loro quartier generali.
Secondo Hager, il GCSB neozelandese ed il DSD australiano avrebbero dotato le proprie strutture di questo programma più tardi rispetto alla NSA, al GCHQ ed al CSE, integrandosi nel sistema solo nei primi anni Novanta[403], quando anche le loro basi SIGINT passarono al programma di condivisione automatica via computer del materiale intercettato. Programma che sarebbe stato denominato 'Progetto P415', o *Echelon*[404].

2. Le reazioni internazionali al caso *Echelon*: i rapporti del Parlamento Europeo.

Simon Davies, sul quotidiano *The Los Angeles Times*, ha di recente scritto: "La NSA [...] si è data come compito il monitoraggio continuo della rete di comunicazioni di tutti i paesi del mondo. Ha creato un sistema che raggiunge e connette tutti i sistemi telefonici e informatici di ogni paese. Si tratta di una attività segreta che avviene al di fuori di ogni verifica democratica e senza alcuna base legale. Il sistema così creato dalla NSA, che opera con il sostegno di agenzie governative inglesi, può intercettare ogni e-mail, ogni fax, ogni telefonata all'interno dell'Unione Europea. Il rapporto intitolato "Una valutazione delle tecnologie e di controllo politico" conferma che la NSA ha la capacità di sorveglianza che copre l'intera Europa e tutto il suo sistema di

401 Cfr. J. BAMFORD, *Body of Secrets - Anatomy of the ultra-secret National Security Agency: from the Cold War through the dawn of a new century*, Doubleday, New York, 2001, p. 403.
402 *Ibidem*, p. 404, e N. HAGER, *Secret Power - New Zealand's role in the international spy network*, Craig Potton Publishing, Nelson, New Zealand, 1996, p. 40.
403 Cfr. N. HAGER, *ibidem*.
404 Cfr. N. HAGER, *ibidem* e D. CAMPBELL, articolo *op. cit.*

comunicazioni. L'operazione è condotta attraverso una catena di supercomputer detti "Echelon" capaci di seguire simultaneamente uno spettro vastissimo di comunicazioni in corso, comprese quelle il cui accesso è bloccato da parole-codice. Qualunque dubbio sul fondamento di quanto affermato nel primo rapporto è stato confutato dal secondo rapporto, "Interception Capabilities 2000", che rileva tutti gli aspetti tecnici dell'operazione. Il rapporto rivela anche che esiste un piano segreto per dare vita a una rete di sorveglianza continua di tutte le forme di comunicazione, di portata planetaria e capace di violare ogni barriera, codice o confine, e destinata a non lasciare alcuna traccia. Dopo il secondo rapporto, il Congresso americano ha ordinato alla NSA [...] di consegnare tutta la documentazione sul progetto "Echelon". La NSA ha rifiutato. L'opinione che si ricava da queste notizie è che i confini nazionali e le barriere di difesa della discrezione individuale si sono disintegrati. Al loro posto è dislocata la presenza continua delle agenzie di monitoraggio. In Italia il Garante della Privacy, Stefano Rodotà, ha espresso la sua preoccupazione"[405].

Già dal 1997 il Parlamento Europeo iniziò ad interessarsi ad *Echelon* ed alla sua presunta attività di spionaggio elettronico delle comunicazioni allo scopo di favorire le aziende e le imprese dei Paesi aderenti al progetto.

Allo scopo di accertare le reali potenzialità del sistema *Echelon*, nel dicembre del 1997 il *Scientific and Technological Options Assessment* (STOA), il comitato tecnico-scientifico del Parlamento Europeo, a nome della Commissione sulle Libertà Civili e gli Affari interni, commissiona uno studio alla *Omega Foundation*, organizzazione anti-militarista di Manchester, specializzata in ricerche su armi, conflitti e tecnologie di controllo politico[406].

Il rapporto *An appraisal of technologies of political control*, firmato da Steve Wright, è una lunga relazione sui sistemi elettronici nelle prigioni, sulle nuove tecniche di tortura negli interrogatori, sulle potenzialità delle nuove armi elettroniche.

Al caso *Echelon* sono dedicate due pagine, nelle quali si menziona per la prima volta che Echelon esiste e, tramite il suo utilizzo, "in Europa tutte le e-mail e le comunicazioni via fax e telefoniche sono intercettate dalla NSA degli Stati Uniti..."[407].

Nel settembre 1998 il caso *Echelon* diventa oggetto dell'attenzione della stampa internazionale, scatenando un acceso dibattito.

Le reazioni dell'opinione pubblica e dei vertici politici europei sono talmente accese che lo STOA commissiona a Steve Wright un *Executive Summary*[408] da presentare all'assemblea europea.

In questo documento Wright precisa che "le tecnologie di sorveglianza sono usate per controllare i dissidenti politici, gli attivisti, i giornalisti, i leader studenteschi, le minoranze...".

---

405 Cfr. S. DAVIES, articolo apparso sul quotidiano *The Los Angeles Times* il 10 agosto 1999, in F. COLOMBO, *Privacy*, *op. cit.*, pp. 88-90.

406 Cfr. A. USAI, *Di cosa si parla quando si parla di spie?*, sito Web del quotidiano *La Repubblica* (in Internet all'indirizzo http://www.repubblica.it), 7 aprile 2000 (sito consultato il 15 luglio 2002).

407 Cfr. *An Appraisal of the Technologies of Political Control*, *STOA Working Document*, redatto da STEVE WRIGHT - Omega Foundation - Manchester, PE 166.499, 6 gennaio 1998.

408 Cfr. *Updated Executive Summary prepared as a background document for the September 1998 part-session* (*An Appraisal of the Technologies of Political Control*), STOA Interim Study, PE 166.499/Int.St./Exec.Sum., settembre 1998.

Il 16 settembre 1998 il Parlamento Europeo esamina il rapporto di Steve Wright, e molti europarlamentari sollevano dubbi sulla reale esistenza del sistema *Echelon*.
L'unica presa di posizione da parte del Parlamento Europeo è una risoluzione, *Sulle relazioni transatlantiche e il sistema Echelon*, riguardante una serie di problemi commerciali tra Unione Europea e Stati Uniti d'America, nella quale, al punto 14, si chiedono agli Stati Uniti "misure precauzionali per quanto concerne le informazioni economiche e un efficace sistema di cifratura"[409].
Nell'aprile 1999 esce il nuovo rapporto sul caso Echelon, *Interception Capabilities 2000*, commissionato dal *Scientific and Technological Options Assessment* al giornalista scozzese Duncan Campbell.
In questo rapporto, Campbell descrive dettagliatamente il funzionamento e le capacità di *Echelon* affermando che questo sistema è utilizzato, soprattutto, come spia commerciale a danno di aziende europee a favore di aziende degli Stati Uniti d'America[410].
Le affermazioni di Campbell portano ad uno scandalo politico-diplomatico che coinvolge tutti i Paesi dell'Unione Europea, in particolare la Gran Bretagna, accusata di tradire gli alleati europei durante la sua collaborazione con gli Stati Uniti d'America[411].
Il garante italiano per la *privacy*, Stefano Rodotà, afferma durante un dibattito che "Echelon è una minaccia per la democrazia, ed ora sulla questione devono intervenire anche i governi nazionali europei"[412].
Nel maggio 1999 esce il nuovo rapporto del Parlamento Europeo sul caso *Echelon*, diviso in quattro parti, il quale copre tutti gli aspetti tecnici del progetto *Echelon* e degli aspetti correlati, come lo spionaggio elettronico, la crittografia, le capacità di un suo utilizzo per attività di spionaggio economico fino ad includere gli aspetti legali di questa vicenda, come le presunte violazioni della *privacy* e della riservatezza delle telecomunicazioni dei cittadini europei[413].

---

409 Cfr. A. USAI, *op. cit.*
410 Cfr. D. CAMPBELL, *Interception Capabilities 2000*, rapporto al Parlamento Europeo, Maggio 1999, capitolo 5; *Risoluzione del Parlamento Europeo sull'esistenza di un sistema di intercettazione globale per le comunicazioni private ed economiche* (sistema d'intercettazione *Echelon*), 2001/2098 (INI), settembre 2001; *Is the US stealing trade secrets from the EU*, pagina Web CNN, 27 marzo 2000 (disponibile alla pagina Web http://www.cnn.com/2000/TEC...puting/03/27/industrial.theft/index.htm, sito consultato il 15 luglio 2002); *Echelon, l'Europa accusa: favorisce le imprese USA*, quotidiano *La Repubblica*, 13 febbraio 2000 (disponibile alla pagina Web http://www.repubblica.it, sito consultato il 15 luglio 2002).
411 Cfr. A. GINORI, *Allarme UE, Echelon spia le e-mail*, quotidiano La Repubblica, 30 maggio 2001, p. 17, A. BONANNI, *Il grande orecchio americano vi spia, inviate e-mail criptate*, *Il Corriere della Sera*, 30 maggio 2001, p. 1 e 16 e *Draft document on the existence of a global system for intercepting private and commercial communications (Temporary Committee on the Echelon interception system)*, relazione della commissione temporanea al Parlamento Europeo sul sistema di intercettamento *Echelon* (*European Parliament Investigation of Echelon*), GERARD SCHMID, PE 305.391, 18 maggio 2001, cap. 7 *Compatibility of an "Echelon" type interception system with Union law* (disponibile sul sito web: www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf, sito consultato il 15 luglio 2002).
412 Cfr. A. USAI, *op. cit.*
413 *Ibidem*

Il rapporto di Campbell, *Interception Capabilities 2000*, fa parte di questo rapporto, il quale comprende: *The perception of economic risks arising from the potential vulnerability of electronic commercial media to interception*, rapporto redatto dallo studioso Nikos Bogonikolos; *The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, european and national law*, scritto da Chris Elliott, specialista in telecomunicazioni; infine, *Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues*, scritto da Franck Leprévost della Technische Universitat di Berlino[414].

Echelon esce dalla scena internazionale fino al Novembre del 1999, quando la rete televisiva inglese BBC mette in onda un dettagliato servizio dal titolo *Echelon esiste*: durante il programma, si ribadisce come questo sistema possa essere usato per attività di spionaggio economico; contemporaneamente, l'Unione Europea si muove per aprire una procedura per violazione della *privacy* contro gli Stati Uniti d'America, prendendo in considerazione il fatto che alcuni programmi *software* destinati al mercato europeo, tra cui il *chip* "spia" Intel contenuto nel microprocessore Pentium III, siano dotati di un livello di protezione inferiore ai loro corrispondenti prodotti americani[415].

Inoltre, nel gennaio del 2000, Jeffrey Richelson, ricercatore della *George Washington University* afferma di essere entrato in possesso di prove, ottenute da documenti declassificati, che confermerebbero l'esistenza di *Echelon* e del suo uso per attività di spionaggio economico-industriale[416].

Nel marzo 2000 il gruppo Verde dell'Europarlamento raccolse 160 firme da presentare all'assemblea di Bruxelles per chiedere la costituzione di una speciale Commissione d'inchiesta sul caso *Echelon*. Questa Commissione, istituita il 5 luglio 2000 e presieduta dal socialdemocratico tedesco Gerhard Schmid, dopo un'indagine durata dieci mesi ha messo a punto il rapporto *On the existence of a global system for intercepting private and commercial communications (Echelon interception system)*[417]: questo rapporto di 120 pagine, attualmente il più aggiornato e recente in materia, oltre a colmare alcune lacune tecniche dei precedenti rapporti aggiungendo una grande quantità di informazioni tecniche, ha ulteriormente avvalorato la tesi che *Echelon* sia usato per intercettare comunicazioni personali e commerciali[418].

Inoltre, nel rapporto viene esaminata la controversa posizione della Gran Bretagna, in quanto Paese membro dell'Unione Europea e, contemporaneamente, membro dell'Accordo Uk-Usa: in effetti, il rapporto critica il ruolo del Paese membro a proposito di *Echelon*; la Commissione

---

414 Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control), part 3/4: *"Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues"*, Scientific and Technological Options Assessment (STOA), Dr. Franck Leprévost - Technische Universitat Berlin - Parlamento Europeo, PE 168.184, aprile 1999 (rapporto disponibile sul sito web: cryptome.org/stoa-r3-5.htm, sito consultato il 20 luglio 2002).

415 Cfr. D. CAMPBELL, *Interception Capabilities 2000*, *op. cit.*, paragrafo 63.

416 Cfr. A. USAI, *op. cit.* ed articolo di Chris Oakes, *Echelon Proof Discovered*, 26 gennaio 2000, in http://www.lycos.com/wirednews (sito consultato il 20 luglio 2002).

417 Cfr. *European Parliament Investigation of Echelon op. cit.*

418 Cfr. A. GINORI, *op. cit.*

speciale ha esplicitamente chiesto alla Commissione europea di aprire una procedura nei confronti della Gran Bretagna per aver violato la Convenzione europea per i diritti umani che garantisce la *privacy* dei cittadini[419].

3. Il progetto 'P415'.

Nel 1988, il giornalista investigativo scozzese Duncan Campbell nel suo articolo *They've got it taped*[420] parlò per primo di un progetto segreto operato dalla GCHQ congiuntamente alla NSA ed alle agenzie COMINT di Australia, Canada e Nuova Zelanda. Secondo Campbell, le cinque agenzie COMINT erano in procinto di investire ingenti risorse, in termini sia di denaro che di strutture e personale, in una operazione, dal nome in codice di "Progetto P415", che avrebbe portato ad un'espansione senza precedenti dei loro sistemi di sorveglianza elettronica, i quali sarebbero stati gestiti dalle rispettive agenzie di *intelligence* delle comunicazioni[421]: già nel 1980, in una rara dichiarazione pubblica a proposito della capacità della *National Security Agency* e delle altre quattro agenzie di avere la capacità di intercettare il traffico delle comunicazioni globali, un funzionario dell'agenzia dichiarò "ci sono tre satelliti sopra l'Atlantico, ognuno capace di trasmettere su circa 20.000 circuiti. Ci sono otto cavi transatlantici con circa 5000 circuiti. Noi li ascoltiamo tutti"[422].
Questo progetto prevedeva la realizzazione di nuove stazioni in ogni parte del globo adibite al monitoraggio, all'intercettazione ed all'analisi delle comunicazioni, collegate tra loro tramite un *network* di computer che avrebbero utilizzato il medesimo sistema: il nome in codice di questo sistema sarebbe stato *Echelon*.
Leader di questo progetto sarebbe stata la NSA, mentre la maggior stazione per l'intercettazione delle comunicazioni sarebbe stata la base militare americana di *Menwith Hill* in Inghilterra.

4. Il sistema di intercettazione *Echelon*.

La parola *Echelon* deriva dal francese antico *eschelon*, a sua volta dal tardo latino *scala*, da cui scalino, gradino, scaglione ed anche "gruppo di unità singole non allineate"[423], termine che risalirebbe all'accordo Uk-Usa: secondo la ricercatrice e giornalista investigativa Susan Bryce "UKUSA è un accordo a gradini, la NSA è chiamata primo partito... rispetto agli altri paesi dell'accordo, si assume l'impegno di numerose operazioni clandestine. [...] Può essere descritta solo

---

419 Cfr. A. BONANNI, *op. cit.*
420 Cfr. D. CAMPBELL, *op. cit.*.
421 I*bidem,* p. 2.
422 Citazione tratta da L. MELVERN, *Exit Smiley, Enter IBM, Sunday Times*, 31 ottobre 1982.
423 Cfr. *Basi segrete e satelliti: ecco la rete Echelon*, sul sito Web del quotidiano "La Repubblica" (http://www.repubblica.it), 20 marzo 1999 (sito consultato il 20 luglio 2002).

come il più grande di tutti i fratelli"[424].
Il rapporto del 1998 *An Appraisal of Technologies of Political Control* del Parlamento Europeo[425] afferma che il sistema di intercettazione globale delle comunicazioni *Echelon* avviene attraverso tre componenti principali: 1) il monitoraggio dei satelliti Intelsat, preposti alla trasmissione delle telecomunicazioni internazionali (telefonate, fax, e-mail) utilizzati dalle maggiori compagnie telefoniche; 2) il monitoraggio di satelliti adibiti alla trasmissione di telecomunicazioni regionali e/o locali; 3) Il monitoraggio di telecomunicazioni che avvengono tramite stazioni di terra o tramite cavi sottomarini, le quali sono trasmesse attraverso sistemi via cavo od attraverso *network* di stazioni di superficie.
Le intercettazioni di comunicazioni internazionali (oltre a telefonate, anche fax ed e-mail) che avvengono via satellite vengono svolte principalmente da cinque basi che orientano le loro enormi parabole sui satelliti di comunicazione Intelsat, utilizzati dalle maggiori compagnie telefoniche del mondo per le comunicazioni internazionali per intercettare le comunicazioni in transito[426].
Il sistema satellitare Intelsat si basa su 17 satelliti in orbita geo-stazionaria intorno alla terra, i quali provvedono la trasmissione di telefonate, fax, e-mail, ed altre comunicazioni internazionali di oltre 200 nazioni sparse in tutto il mondo.
Questo sistema è gestito dall'*International Telecommunications Satellite Organization* di Washington, D.C.: ironicamente, il motto della compagnia è "We link the world's telecommunications network together"[427].
Le cinque agenzie preposte sono l'agenzia COMINT britannica GCHQ, la quale gestisce le base di Morwenstow, in Cornovaglia, controllando le comunicazioni trasmesse dai satelliti in orbita sopra l'Atlantico, l'Europa e l'Oceano Indiano; la base americana di Sugar Grove, in Virginia, intercetta quelli del Nord e Sud America; la base gestita dalla NSA di Yakima, nello stato di Washington, sulla costa ovest degli Stati Uniti gestisce il traffico dei satelliti in orbita sopra l'Oceano Pacifico, zona est; la base in Nuova Zelanda a Waihopai, diretta dal GCSB, intercetta le comunicazioni satellitari dell'Oceano Pacifico, zona ovest; infine, la base australiana di Geraldton, controllata dal DSD si preoccupa dei satelliti sopra l'Oceano Indiano[428].
Una seconda rete di intercettazioni è costituita dalle basi che sorvegliano i satelliti russi per le comunicazioni, oltre ad altri sistemi regionali, come

---

424 Cfr. A. FAZIO, L. GUIDI, *Il caso Echelon. Fino a che punto è socialmente accettabile l'intercettazione delle comunicazioni?*, (articolo disponibile alla pagina web: www.unipi.it/guidi/echelon.htm, sito consultato il 15 luglio 2002)

425 Cfr. Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control), part 4/4: *"The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition"*, Scientific and Technological Options Assessment (STOA), PE 168.184, Aprile 1999, p. 19. (Rapporto disponibile sul sito web: www.europarl.eu.int/dg4/stoa/en/, sito consultato il 15 luglio 2002).

426 Cfr. A. FAZIO, L. GUIDI, *op. cit.*, p. 2-3.

427 Cfr. J. BAMFORD, *Body of Secrets*, p. 404.

428 Cfr. A. FAZIO, L. GUIDI, *op. cit.*, e D. CAMPBELL, *Interception Capabilities 2000*, *op. cit.*, paragrafo 73-79.

Eutelsat, il sistema satellitare europeo[429].
Esse sono: la stazione di Menwith Hill in Inghilterra, la stazione più importante, per dimensione e capacità, del sistema Echelon, la quale, tra le sue molteplici funzioni, comprende l'intercettazione delle comunicazioni dei satelliti russi; Shoal Bay, Australia, la base di Leitrim, Canada, la stazione di Bad Aibling in Germania, la base di Misawa in Giappone ed infine la stazione di Pine Gap in Australia[430]. La base di Shoal Bay, in Australia, concentra prevalentemente la propria attività sui satelliti indonesiani, mentre la base canadese di Leitrim intercetta le comunicazioni dei satelliti latino-americani, incluso il satellite utilizzato dalla compagnia telefonica messicana "Morelos"[431].
Se si pensa che tutte queste stazioni sono collegate tra loro ed utilizzano gli stessi sistemi e gli stesso programma di intercettamento, analisi e gestione del materiale, è possibile rendersi conto delle capacità di questo *network*.
Solo la base di Menwith Hill riesce a gestire oltre 100.000 telefonate al secondo, le quali entrano nella base tramite cavi a fibra ottica della British Telecom e vengono poi analizzate dai potenti computer: in solo un'ora, due milioni di messaggi sono intercettati attraverso il programma *Echelon*, 13.000 vengono trattati sulla base dei dizionari ed analizzati per trovare parole chiave di particolare interesse, 2.000 sono elaborati dai computer e schedati.
Di questi, 20 vengono selezionati dagli analisti, i quali produrranno poi, sulla base del materiale ottenuto, 2 rapporti con nomi, cifre e tipo di conversazione che verranno immediatamente inviati al quartier generale della NSA[432].
Qui il materiale recepito dalle stazioni sparse per il globo viene ulteriormente processato attraverso i computer dell'agenzia, che tratta i dati con un dizionario di parole chiave: i dati ottenuti vengono poi selezionati e da essi gli analisti ne traggono informazioni da passare a chiunque possa esserne interessato, come il Governo, il Dipartimento di Stato o della Difesa, persino aziende commerciali[433]. L'attività COMINT di comunicazioni domestiche, cioè a livello nazionale, viene effettuata da stazioni a terra tramite apposite antenne, mentre messaggi inviati utilizzando cavi sottomarini vengono intercettati nel momento in cui questi cavi risalgono in superficie per trasmettere via etere i messaggi per raggiungere i destinatari, anche se non è raro che l'intercettazione avvenga direttamente sui cavi sottomarini.
Echelon è in grado di intercettare non solo le comunicazioni internazionali che avvengono via satellite, ma anche le comunicazioni nazionali trasmesse tramite stazioni di terra e quelle che viaggiano attraverso cavi sottomarini.
Per quanto riguarda le comunicazioni domestiche, si ritiene che *Echelon* utilizzi basi di terra ed appositi satelliti spia per intercettare comunicazioni "di superficie", cioè comunicazioni che viaggiano o via cavo o attraverso stazioni di terra[434].
Le basi di intercettazione di questo tipo di comunicazioni si trovano negli Stati

---

429 Cfr. G. SCHMID, *European Parliament Investigation of Echelon*, *op. cit.*, paragrafo 4.
430 Cfr. A. FAZIO e L. GUIDI, *op. cit.*, p. 2-3.
431 Cfr. P. S. POOLE, sito web *op. cit.*, p. 6.
432 Cfr. *Inchiesta Echelon*, in *La Repubblica*, 17 giugno 2001, p. 11.
433 *Ibidem*, p. 10.
434 Cfr. *An Appraisal of Technologies of Political Control*, *op. cit.*, cap. 1, paragrafo 5.

Uniti d'America (vicino a Denver), in Italia (base di San Vito dei Normanni, Puglia), Inghilterra (Menwith Hill), Germania, Turchia, Nuova Zelanda, Canada ed Australia[435].

Le comunicazioni trasmesse attraverso cavi sottomarini stanno assumendo un ruolo dominante nel campo delle telecomunicazioni internazionali, in quanto, al contrario delle trasmissioni via satellite, le quali dispongono di una limitata banda di frequenza, i sistemi di trasmissione via fibre ottiche hanno in pratica una capacità illimitata di gestione del traffico[436].

Effettivamente, se i primi sistemi erano in grado di gestire simultaneamente solo poche centinaia di telefonate, ora i moderni sistemi a fibre ottiche riescono a trasmettere fino a 5 Gbps (*Gigabits* per secondo) di dati, equivalenti a circa 60.000 telefonate simultanee[437].

L'intercettazione delle comunicazioni trasmesse attraverso cavi sottomarini è stata un'attività largamente praticata dai servizi COMINT americani: sin durante gli anni della guerra fredda, la NSA era riuscita ad intercettare le comunicazioni sovietiche che viaggiavano attraverso cavi sottomarini[438].

Dal 1985, operazioni di intercettamento di cavi sottomarini furono attuate anche nel Mediterraneo, per intercettare le comunicazioni tra l'Europa ed l'Africa Ovest[439].

Grazie ai continui progressi tecnologici, oggigiorno gli Stati Uniti d'America sono in grado di controllare cavi sottomarini che gestiscono le comunicazioni di aree ben più vaste, come il Medio Oriente, l'intero bacino del Mediterraneo, l'Asia Orientale ed il Sud America[440].

5. *Echelon* ed Internet: lo spionaggio della posta elettronica.

L'impressionante sviluppo che ha avuto la rete Internet negli ultimi anni, in termini sia di dimensioni che di importanza, ha rappresentato un'ulteriore sfida ai servizi d'intelligence[441].

Il vice Direttore della NSA, Barbara McNamara, sottolineò nel 1999 che la crescita esponenziale che stava compiendo Internet, e le forme di comunicazione digitale ad esso collegate, rappresentava uno dei problemi più attuali dell'agenzia: nella società si era avviato un processo di eccessiva comunicazione. *"Quarant'anni fa c'erano 5.000 computer, non connessi tra loro, non c'erano macchine fax e neanche telefoni cellulari... Nel 1999 esistono oltre 420 milioni di computer, la maggior parte dei quali interconnessi tra loro. Esistono 14 milioni di macchine fax e 468 milioni di telefoni cellulari, e queste cifre continuano a crescere. L'Industria delle telecomunicazioni sta investendo miliardi di dollari per coprire il mondo di miglia di cavi a*

---

435 *Ibidem*.

436 Cfr. D. CAMPBELL, *Interception Capabilities 2000*, pp. 9 e 13.

437 *Ibidem*, p. 9.

438 *Ibidem*, pp. 10-11.

439 Cfr. S. SONTAG, C. DREW , *Blind man's Bluff: the untold story of American submarine Espionage*, Public Affairs, New York, 1998, in D. CAMPBELL, *Interception Capabilities*, 2000, *op.cit.*, p. 14.

440 Cfr. D. CAMPBELL, *ibidem*.

441 Cfr. D. CAMPBELL, *Interception Capabilities 2000, op. cit.*, paragrafo 53.

fibre ottiche a banda larga".

McNamara aggiunse anche che 304 milioni di persone si sarebbero connessi ad Internet nell'anno 2000, l'80 per cento in più rispetto all'anno precedente. E per la prima volta, meno della metà di queste persone vivevano in Nord America[442].

La NSA non si è fatta però cogliere impreparata da questa nuova sfida, anzi: l'agenzia americana, in collaborazione con i suoi quattro partner UKUSA già negli anni '80 utilizzava per le proprie comunicazioni un network internazionale basata sulla stessa tecnologia dell'odierno sistema Internet[443]. L'agenzia inglese GCHQ, per esempio, ha collegato tutti i propri sistemi fra loro attraverso un sistema denominato LAN (Local Area Network), collegato alla altre stazioni sparse per il mondo tramite un ulteriore network, il WAN (Wide Area Network).

Questo network collega tra loro tutte le stazioni di terra ed i quartier generali appartenenti ai cinque paesi dell'Accordo: il nome di tale progetto è EMBROIDERY, il quale include PATHWAY, il maggiore e più importante network di computer per la condivisione delle comunicazioni intercettate, che provvede alle comunicazioni del sistema Echelon, garantendo rapidità e sicurezza[444].

A partire da metà degli anni '90, le cinque agenzie COMINT hanno sviluppato sistemi in grado di intercettare, selezionare ed analizzare il traffico delle comunicazioni via Internet.

Gli Stati Uniti sono stati particolarmente avvantaggiati in quanto è proprio lì che il sistema Internet si è sviluppato e radicato, e la maggior parte delle comunicazioni tramite Internet, anche se partono da paesi terzi e sono diretti sempre verso paesi terzi, molto spesso passano attraverso i centri di smistamento Internet americani[445].

Molto recentemente, la NSA avrebbe perfezionato particolari sistemi per effettuare attività COMINT su queste nuove tecnologie.

Queste congetture vennero discusse in una riunione altamente segreta alla NSA il 30 settembre 1999[446(43)], tra il vice-direttore per i servizi Terry Thompson e membri del settore tecnico dell'agenzia: in quell'incontro, tutti i partecipanti concordarono sul fatto di aumentare, in termini sia qualitativi che quantitativi, le attività di intelligence a riguardo di Internet.

Si decide di proseguire la strada sin lì percorsa dall'agenzia in materia di spionaggio della posta elettronica, cioè di continuare ad assumere personale specializzato nella produzione dei componenti fondamentali che costituiscono il sistema Internet, magari assumendo proprio ex-dipendenti di aziende americane che producessero materiale riguardante la rete mondiale e i nuovi sistemi di comunicazione in genere. Con il loro aiuto, la *National Security Agency* sarebbe stata al passo dei tempi.

---

442 Cfr. J. BAMFORD, *Body of Secrets*, *op. cit.*, p. 458.

443 Cfr. D. CAMPBELL, *Interception Capabilities 2000*, *op. cit.*, paragrafo 53.

444 *Ibidem.*

445 *Ibidem*, paragrafo 54 e 55.

446 Cfr. J. BAMFORD, *Body of Secrets*, *op. cit.*, p. 464.

Un esempio delle straordinarie capacità COMINT raggiunte dall'agenzia anche in questi nuovi settori è il caso dell'azienda *"Cisco"*.
La Cisco Systems è un'azienda californiana specializzata nella produzione di componenti per computer: un loro particolare prodotto che ha destato l'interesse dei servizi d'*intelligence* americani era un microscopico componente il quale ha la funzione di incanalare il flusso delle informazioni che viaggiano sulla rete Internet verso altri *network*.
Questo prodotto opera come una specie di ufficio postale virtuale, con la funzione di ricevere, analizzare e successivamente inoltrare i dati ricevuti: la NSA, scoprendo il funzionamento preciso di questo componente, sarebbe stata in grado di intercettare una quantità notevole di traffico elettronico trasmesso via Internet[447].
Thompson e i suoi collaboratori decisero, pertanto, che il reclutamento di personale civile estraneo ad ogni attività di *intelligence* era un passo da compiere assolutamente: in effetti, recentemente la NSA ha assunto un ingegnere della Cisco affinché diventasse il supervisore tecnico di questo nuovo progetto dell'agenzia. Secondo un *ex* dipendente dell'agenzia, la NSA dal 1995 ha installato un programma *software* denominato *"Sniffer"*, letteralmente "fiutatore" che ha la funzione di intercettare e collezionare il traffico delle comunicazioni (che consistono in *e-mail*, file contenenti immagini, progetti ecc.) trasmesse utilizzando la rete Internet nel momento in cui queste comunicazioni raggiungono i centri IXP di smistamento (Internet Exchange Points): attualmente, la NSA terrebbe sotto controllo i nove maggiori centri IXP negli Stati Uniti d'America[448].
I centri FIX East e FIX West sono gestiti da agenzie del Governo degli Stati Uniti d'America, i centri MAE East e MAE West dalla MCI, una delle maggiori compagnie telefoniche private americane, mentre i centri di San Francisco e di Chicago rispettivamente dalla Pacific Bell e dalla Ameritech[449].
Duncan Campbell in *Interception Capabilities 2000*, il secondo rapporto al Parlamento Europeo sul caso *Echelon*, afferma[450] inoltre che un'azienda americana[451], *leader* nel settore di Internet e delle telecomunicazioni, ha collaborato con la NSA per sviluppare un sistema per intercettare precisi dati sulla rete Internet, e che sempre la NSA si è accordata con le principali aziende produttrici di programmi per computer (Microsoft, Lotus e Netscape) affinché alterassero con tale sistema i loro prodotti, ma non tutti: solo quelli destinati al mercato estero[452].
Di fatto, nel 1997, durante un processo tenutosi in Inghilterra riguardante presunte violazioni della *privacy* da parte della NSA attraverso attività COMINT, testimoni appartenenti alla US Air Force, l'aeronautica statunitense, dichiararono che la *National Security Agency* svolge un'effettiva attività di

---

447 *Ibidem*, p. 465.
448 Cfr. W. MADSEN, P*uzzle palace conducting internet surveillance*, tratto da *Computer Fraud and Security Bulletin*, giugno 1995, in D. CAMPBELL*, Interception Capabilities* 2000, *op. cit.*, paragrafo 60.
449 *Ibidem*.
450 Cfr. D. CAMPBELL, *ibidem*, paragrafo 61.
451 *Ibidem*: il rapporto omette il nome dell'azienda.
452 *Ibidem*.

sorveglianza della rete Internet. La NSA non ha né ammesso né smentito tali dichiarazioni[453].

Quando si utilizza il servizio di posta elettronica tramite la rete Internet, si attivano automaticamente nei *software* dei livelli di protezione, più o meno elevati, a seconda della riservatezza del materiale inviato: per esempio, se si effettuano operazioni finanziarie e si inviano o ricevono informazioni strettamente personali, come il numero di una carta di credito, i *software* di cui sono dotati tutti i moderni computer trasformano i nostri dati in cifre completamete differenti, a prima vista casuali, utilizzando per fare ciò elaborati sistemi di crittografia.

Solo un computer che utilizzi lo stesso programma può ritrasformare i dati ricevuti 'in chiaro', cioè ricomporli utilizzando lo stesso codice crittografico per renderli comprensibili: questa operazione è necessaria per evitare che qualcuno, tramite un terzo sistema, possa intercettare la comunicazione ed impossessarsi dei dati e delle informazioni contenute.

Anche qualora l'intercettamento avvenisse, ci si potrebbe impossessare solo di incomprensibili ed inutili sequenze alfanumeriche[454].

Questo sistema di sicurezza tramite l'utilizzo di codici crittografici attirò l'interesse della *National Security Agency* già nel 1995: in effetti, le maggiori aziende produttrici di programmi per Internet (Microsoft, Netscape, Lotus) stavano già inserendo elevati sistemi di sicurezza nei loro programmi, e nel giro di un paio d'anni tutti i computer del mondo avrebbero utilizzato i loro sofisticati sistemi di protezione delle informazioni inviate; questo per l'agenzia e per gli altri quattro *partner* avrebbe limitato notevolmente la capacità di analisi delle comunicazioni intercettate via Internet, ed avrebbe richiesto un loro maggior impegno, sia in termini di tempo sia di risorse. Per ovviare a ciò, la *National Security Agency* si accordò con queste aziende affinché acconsentissero di applicare sui loro programmi livelli di protezione minori e, in particolare che riducessero quelli destinati al mercato estero[455].

Un caso esemplare è il programma *Notes*, prodotto dall'azienda statunitense Lotus, facente parte del gruppo IBM: tale programma è in grado di rendere sicure le *e-mail* in quanto, utilizzando un sofisticato programma di crittografia, garantisce un livello di protezione elevato.

Ma questo espediente non era unanime per tutti: in effetti, nei programmi destinati al mercato estero, il livello di protezione era decisamente minore di quello installato nei prodotti destinati al mercato americano.

Questo stratagemma era frutto di un accordo tra la Lotus, la casa produttrice, e la *National Security Agency*, che si garantiva così un più facile accesso alle comunicazioni straniere via Internet.

---

453 Cfr. D. CAMPBELL, *More Naked Gun than Top Gun*, in *The Guardian*, 26 novembre 1997.

454 Cfr. M. BERGAMI, *"Due barriere per difendere il vostro PC"*, in *Sicurezza*, supplemento alla rivista *PC_Professionale*, n. 122, Maggio 2001, pp. 15-31 e *Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control)*, part 3/4: *"Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues"*, Scientific and Technological Options Assessment (STOA), DR. FRANCK LEPRÉVOST - Technische Universitat Berlin - Parlamento Europeo, PE 168.184, Aprile 1999. (Rapporto disponibile sul sito web: cryptome.org/stoa-r3-5.htm, sito consultato il 15 luglio 2002).

455 Cfr. D. CAMPBELL, *Interception Capabilities 2000*, *op. cit.*, paragrafo 42.

Questo particolare venne scoperto nel 1997, quando il governo svedese scoprì che il programma di protezione crittografica *Notes* della Lotus, versione 'europea', era estremamente vulnerabile, e la *National Security Agency* era in grado di decifrare un messaggio inviato con tale programma in pochi secondi.
Questo grazie ad un particolare programma, il *workfactor reduction field*, che diminuiva sensibilmente il livello di protezione delle *e-mail* spedite da utenti non americani: tecnicamente, il sistema utilizzato negli Stati Uniti d'America funzionava con chiavi di cifratura a 64 *bit*, mentre i programmi destinati al mercato extra-americano funzionavano a 24 *bit*[456]. La Lotus ammise questa differenza: "La differenza tra la versione americana del programma Notes e la versione esportata risiede nel livello crittografico applicato. Noi consegniamo prodotti con chiavi di cifratura a 64 *bit* a tutti i consumatori, ma a 24 *bit* per quei prodotti destinati al di fuori degli Stati Uniti, come d'accordo con il governo americano"[457].
L'esempio preso in considerazione non è da considerarsi un caso isolato: espedienti simili sono applicati su tutte le versioni dei *browser* prodotti da Microsoft e Netscape destinati al mercato estero: se per i prodotti destinati all'utenza americana si applica un sistema di protezione a 128 *bit*, alla versione "export" non viene diminuita la potenza della chiave di cifratura: le due aziende mantengono sempre un sistema a 128 *bit*, ma il programma ne utilizza solo 88.
I restanti 40 *bit* servono alla NSA per decifrare immediatamente il messaggio.
Ne consegue pertanto che la maggior parte dei computer attualmente in uso in Europa contengono al loro interno un sistema di riduzione dei livelli di sicurezza che garantirebbe alla NSA l'accesso e la lettura dei messaggi inviati e ricevuti[458]. L'editoriale *"The End of Privacy"* apparso sul quotidiano "The Economist" il 18 maggio 1999[459] evidenzia inoltre che "quest'anno sia Intel che Microsoft hanno provocato una tempesta di reazioni e di critiche quando si è saputo che tutti i chip ed i software da essi prodotti [...] trasmettono numeri di identificazione che sono come le impronte digitali di ciascuno di noi: unici ed immediatamente identificabili. Intel e Microsoft si sono offerti di fare marcia indietro, ma è inutile: un numero sempre più grande di espedienti e software della comunicazione elettronica mandano l'uno all'altro numeri indelebili di identificazione".
Le informazioni ottenute da ogni singola stazione appartenente al sistema *Echelon* viene trasmessa non solo al quartier generale dell'agenzia di *intelligence* competente, ma anche alla NSA a Fort Meade, la quale analizza, interpreta ed archivia, giorno per giorno, il materiale proveniente da tutte la stazioni di intercettamento e da tutte e basi militari facenti parte questo *network* globale. Il prossimo paragrafo illustrerà, appunto, il modo in cui si intercettino le

---

456 I*bidem*, paragrafo 43.
457 Cfr. F. LAURIN, C. FROSTE, S. DAGBLADET, *Secret Swedish E-Mail Can Be Read by the USA*, 18 Novembre 1997, in D. CAMPBELL, *Interception Capabilities 2000*, *op. cit.*, paragrafo 43.
458 Cfr. D. CAMPBELL, *Interception Capabilities 2000, op. cit.*, paragrafo 44.
459 Cfr. *The End of Privacy*, in *The Economist*, 18 maggio 1999, citato in F.COLOMBO, *Privacy,* Rai - Eri Rizzoli, Milano, 2001, pp. 117-118.

comunicazioni, come i potenti computer le analizzino e le archivino nelle loro memorie[460].

6. Dentro ad *Echelon*: il sistema dei 'dizionari'.

Tutti i computer utilizzati nel sistema *Echelon* sono chiamati 'dizionari', i quali sono tutti collegati tra loro attraverso linee di comunicazione crittate, altamente sicure, che collegano assieme i *database* dei quartier generali delle cinque agenzie.
In questi *database* finiscono tutti i messaggi quotidianamente selezionati dai 'dizionari'.
I computer utilizzati dalle cinque agenzie COMINT facenti parte l'Accordo Uk-Usa erano in grado di effettuare ricerche di precise parole chiave sin dai primi anni Settanta, ma è con la creazione del sistema *Echelon* negli anni Ottanta che tutti i computer utilizzati furono interconnessi tra loro, permettendo alle stazioni di tutto il mondo di funzionare come un sistema unico[461].
Prima di *Echelon*, in effetti, i cinque partner effettuavano operazioni di "intelligence gathering"[462], cioè di condivisione del materiale intercettato, ma ciascuna agenzia usualmente processava ed analizzava le intercettazioni direttamente nelle proprie stazioni[463].
I computer 'dizionari' facenti parte del sistema *Echelon* non contengono pertanto solo la lista di parole chiave inserita dalla rispettiva agenzia, ma anche liste trasmesse dalle altre quattro agenzie[464].
Per esempio, i computer della base di Geraldton, in Australia, non contengono unicamente la lista di parole chiave da intercettare che interessa il DSD, l'agenzia COMINT australiana, ma anche specifiche liste di parole che interessano la NSA americana, il CSE canadese, il GCHQ inglese e il GCSB neozelandese: in questo modo, ciascuna stazione dirige le proprie ricerche verso telefonate, fax, telex ed e-mail che contengano una o più parole chiave che siano state precedentemente inserite nei programmi di ricerca dei computer e, in caso di riscontro positivo, automaticamente spedisce all'agenzia interessata il materiale ottenuto[465].
Questo sistema è stato dettagliatamente descritto per la prima volta dal giornalista Nicky Hager nel suo *Secret Power*: egli scrive che ogni mattina gli

---

460 Cfr. N. Hager, *Secret Power*, *op. cit.*, cap. 3 *"The Power of the Dictionary. Inside* Echelon", p. 42.
461 Cfr. J. BAMFORD, *Body of Secrets, op. cit.*, p. 404 e Hager, *ibidem,* p. 29.
462 Cfr. D. CAMPBELL, *Interception Capabilities 2000*, *op. cit.*, paragrafo 22.
463 Cfr. N. HAGER, Secret Power, *op. cit.*, p. 29 e 43.
464 Nell'articolo *"Basi segrete e satelliti: ecco la rete Echelon"* del 25 giugno 1999, apparso sul sito web del quotidiano *La Repubblica* (http://www.repubblica.it) sono elencate una serie di parole chiave utilizzate dai "dizionari" di *Echelon*. Esse sono: Verisign, Secure, ASIO, Lebed, ICE, Lexis-Nexis, Bugs Bunny, FliR, JIC, bce, Lacrosse, Flashbangs, IRA, DIA, BOP, BMDO, site, SASSTIXS, O, bemd, SABENA, SHAPE, bird dog, HALO, SAS, Lander, GSM, T Branch, HAHO, benelux, Forte, AT, Exon Shell.
465 Cfr. N. HAGER, *Secret Power*, *op. cit.*, p. 29 e 43.

analisti che lavorano per le cinque agenzie COMINT a Washington, Ottawa, Canberra, Wellington e Cheltenham, accendono i loro computer ed entrano nel sistema dei "dizionari".
Il loro compito consiste nell'inserire un codice di quattro cifre, assegnato dalla NSA americana che li trasmette a tutte le stazioni e le basi aderenti ad Echelon, codice che corrisponde ad una parola chiave[466(63)] che può interessare vari soggetti, dall'MI 6 britannico all'americana CIA.
Per esempio, 1911 sta per comunicato diplomatico giapponese, proveniente dall'America Latina, raccolto dal CSE canadese, 3848 sta per comunicazioni politiche da e sulla Nigeria, e 8182 riguarda qualsiasi messaggio riguardante tecnologie di crittografia[467].
Per esempio, il Dipartimento di Stato americano può avere interesse nel conoscere la proliferazione delle armi nucleari da parte di paesi ostili, e, più precisamente, del fatto che la Cina possa vendere componenti di tali armi a paesi come Pakistan o Iran: in questo caso, i Dipartimenti di Stato e della Difesa americani, per esempio, possono passare alla *National Security Agency* specifiche parole chiavi, che possono essere anche una semplice sequenza numerica, come in numero telefonico, e passarle alle agenzie *partner*, le quali passeranno la lista alle proprie basi.
Quindi gli analisti, dopo aver selezionato che tipo di ricerca intendono effettuare quel giorno, mettono in moto un'operazione di ricerca che, tramite questo *network*, cerca senza sosta messaggi che contengano quella precisa parola chiave: se la ricerca ha esito positivo, l'agenzia ottiene il risultato che si era prefissato, cioè tutti i messaggi contenenti quel determinato soggetto che la rete *Echelon* ha 'catturato'.
In seguito, gli operatori scorrono tutte le informazioni ricevute contenenti i risultati della loro ricerca, e, quando un messaggio appare particolarmente interessante, lo selezionano dal resto della lista e, nel caso non sia in lingua inglese, viene tradotto da una apposita sezione e successivamente inviato alla agenzia COMINT di competenza ed alla *National Security Agency*, che è l'unica ad avere il controllo su tutto il materiale intercettato dalle altre quattro agenzie[468].
Per facilitare il compito di risalire alla stazione che ha intercettato la comunicazione, i centri di intercettamento assegnano ad ogni singolo messaggio il proprio codice identificativo: ALPHA-ALPHA (GCHQ), ECHO-ECHO (DSD), INDIA-INDIA (GCSB), UNIFORM (CSE) e OSCAR-OSCAR (NSA)[469]. Inoltre, al materiale intercettato viene assegnato un codice che ne specifica il livello di segretezza: MORAY (segreto), SPOKE (livello ancora maggiore di segretezza), UMBRA (livello massimo di segretezza), oltre ai codici GAMMA (materiale di provenienza sovietica), DRUID (materiale inoltrato a Paesi non facenti parte dell'Accordo UKUSA)[470].

---

466 Cfr. J. BAMFORD, *Body of Secrets*, *op. cit.*, p. 409.
467 Cfr. N. HAGER, *Echelon: sottoposti al sistema di sorveglianza globale*, *op. cit.*, p. 8.
468 Cfr.J. BAMFORD, *Body of Secrets*, *op. cit.*, p. 409 e N. HAGER, *Secret Power*, *op. cit.*, p. 44.
469 Cfr. P. S. POOLE, sito web *ECHELON: America's Secret Global Surveillance Network*, p. 7, pp. 9-10.
470 *Ibidem*.

7. Il sistema dei 'dizionari' ed il controllo delle informazioni.

Al fine di controllare con precisione il tipo di materiale che si sta cercando (e chi può avere accesso a queste informazioni) è stato organizzato un sofisticato sistema sul quale tutto il sistema *Echelon* è basato. I 'dizionari' non contengono solo la lista delle parole chiave per effettuare la ricerca, e inoltre tutte le informazioni finiscono in un unico *database* che le agenzie possono consultare a proprio piacimento.
Tutto il procedimento è molto più complesso. Innanzitutto, gli indici di ricerca sono divisi nelle stesse categorie del codice a quattro cifre. Ogni agenzia decide le proprie categorie compatibilmente alle responsabilità della stessa all'interno del *network* (per esempio, il *Government Communications Security Bureau* (GCSB) in Nuova Zelanda controlla le comunicazioni dei governi dell'area di sua competenza, cioè il Sud Pacifico, delle ambasciate giapponesi e delle attività russe nell'Antartide)[471].
Le agenzie poi elaborano dalle 10 alle 50 parole chiave che hanno immesso in ogni categoria. Queste parole chiave comprendono nomi di persone, di operazioni, di organizzazioni di ogni genere, di progetti non solo militari, ma anche economici e politici, numeri di telefono, indirizzi di posta elettronica, cioè tutti quegli elementi che possano rendere più precisa la ricerca che si vuole effettuare. A volte, infatti, le agenzie utilizzano combinazioni di "keywords" prestabilite per velocizzare la ricerca[472].
Questo sistema, cuore del progetto *Echelon*, è stato progettato dalla *National Security Agency* e successivamente adottato da tutte le altre agenzie, creando così il *network* globale del sistema *Echelon*: i computer "dizionari" cercano tra tutti i messaggi in entrata basando la loro ricerca sulle parole chiave immesse dalle agenzie, contemporaneamente annotando dati tecnici come orario, data e luogo dell'intercettazione sul messaggio di modo che un operatore successivo, di qualsiasi agenzia, potrà sapere dove e quando il messaggio è stato intercettato.
Il computer aggiunge poi in modo automatico quattro cifre al codice identificativo del messaggio, cifre che rappresentano le parole chiave contenute all'interno del messaggio: una sorta di codice di riconoscimento del messaggio. Questo permetterà di catalogare tutti questi messaggi nel *database* dell'agenzia, permettendo così di poterli reperire più agevolmente in un secondo tempo[473].
Il sistema dei "dizionari" efficacemente mostra come il sistema *Echelon* non sia uguale per tutti, ma come piuttosto operi differentemente a seconda che lo utilizzi la *National Security Agency* o, piuttosto, una qualsiasi delle altre quattro agenzie COMINT. Difatti ogni agenzia non ha accesso a tutto il *database*, ma solo ai quattro codici a quattro cifre, a differenza dell'agenzia di Fort Meade che ha accesso all'intero *network* di *Echelon*. Un ufficiale dei servizi di *intelligence*

---

471 Cfr. N. HAGER, *Secret Power*, *op. cit.*, p. 46.
472 *Ibidem*, p. 47.
473 *Ibidem*, p. 48.

neozelandesi ha specificato che "le agenzie possono cercare attraverso i propri codici anche negli altri dizionari, ma l'accesso è strettamente controllato. I più difficili da trattare sono quelli americani. [...] ci sono molti livelli attraverso cui passare, a meno che non sia anche di loro interesse, in quel caso lo faranno per te"[474].
Solo la *National Security Agency*, pertanto, grazie al suo ruolo di *leader* del progetto *Echelon* e della sua importanza all'interno dell'alleanza ha accesso a tutte le potenzialità del sistema[475].
Il sistema dei "dizionari" rende palese la pericolosità di *Echelon*: il progetto *Echelon* sin qua descritto rende evidente come le comunicazioni di qualunque tipo siano vulnerabili alle intercettazioni dei servizi di *intelligence* e come questo sistema ampiamente oltrepassi gli scopi di sicurezza nazionale per il quale era stato creato in principio, essendo in grado, difatti, di controllare le comunicazioni private di cittadini, di aziende e di organizzazioni, diventando così un potenziale strumento per effettuare operazioni che oltrepassano la sicurezza nazionale per sconfinare nel campo dello spionaggio economico-commerciale, violando inoltre diritti fondamentali quali la *privacy* e la riservatezza delle comunicazioni.

8. Il progetto *Enfopol*.

Enfopol sarebbe la risposta europea ad *Echelon*: una rete di intercettazione europea delle comunicazioni, creato allo scopo di collegare fra loro la fitta rete delle Polizie ed agenzie di *intelligence* europee, per esigenze di sicurezza nazionale e prevenzione e lotta alla criminalità. *Enfopol* è talmente simile ad *Echelon*, seppur di minori potenzialità, che non poteva che fare capo ad un'agenzia americana, precisamente l'FBI[476].
Il documento di *State Watch* riassume il rapporto USA-UE di Enfopol: "L'Unione Europea in collaborazione con l'FBI americano sta per attivare un sistema di sorveglianza globale delle comunicazioni per combattere gravi crimini e per proteggere la sicurezza nazionale, ma per fare questo ha creato un sistema in grado di controllare e chiunque e qualsiasi cosa. L'Unione Europea – insieme ai suoi partner – sarà in grado di analizzare l'etere di tutto il mondo alla ricerca di pensieri sovversivi e punti di vista dissidenti[477]".
Ma non vi è il pericolo che *Infopol* sia un altro orecchio americano, oltre ad *Echelon*? Il 29 e 30 novembre 1993, durante l'incontro a Bruxelles tra i Ministri della giustizia e dell'interno dei Paesi dell'Unione Europea, si adottò una risoluzione riguardante *Enfopol*, nel quale il Consiglio sull'intercettazione delle

474 Cfr. N. HAGER, *Echelon: sottoposti al sistema di sorveglianza globale*, op. cit., p.10.
475 Cfr. N. HAGER, *Secret Power*, *op. cit.*, p. 51.
476 Cfr. R. CHIESA, *Le reti di Controllo Globale*, 26 gennaio 2000, in Internet sul sito Web http://www.apogeonline.com, p. 15 (sito consultato il 15 luglio 2002).
477 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *Segreti spie codici cifrati – Crittografia: la storia, le tecniche, gli aspetti giuridici*, Milano, Apogeo, 1999, p. 200.

comunicazioni specificò che[478]: si estendeva il progetto Enfopol ad Australia, Nuova Zelanda e Hong Kong per ragioni di praticità[479]; i fornitori di telecomunicazioni europei devono dotarsi degli stessi standard per semplificare l'attività di intercettazione dei servizi di *intelligence* e di sicurezza[480]; i gestori di telefonia mobile dovevano consentire la localizzazione fisica dell'utente di un telefono cellulare[481].

I motivi di interesse da parte dell'FBI nella gestione di un sistema di intercettazione europeo sono evidenti se consideriamo che a partire dai primi anni Novanta in Europa il settore delle telecomunicazioni fu interessato dalla privatizzazione.

Questo fattore comportava un problema per le agenzie di *intelligence* degli Stati Uniti d'America, in quanto le compagnie telefoniche avrebbero presto sviluppato nuove tecnologie, abbandonando gli *standard* sui quali si erano basate le intercettazioni fino ad allora.

Una collaborazione USA-UE avrebbe giovato ad entrambi: gli Stati Uniti d'America potevano aumentare la loro capacità di spionaggio COMINT in Europa, unendola al sistema *Echelon* del quale erano il Paese *leader*, mentre l'Europa avrebbe tratto un vantaggio di tipo tecnico, appoggiandosi ad un paese dotato della più avanzata tecnologia in materia di spionaggio delle comunicazioni.

Era pertanto necessaria, per rimanere al passo con i tempi e con un settore che si evolveva rapidamente come quello delle telecomunicazioni, formare una stretta collaborazione a livello internazionale tra Polizie ed *intelligence*. In effetti, l'intesa UE-FBI, era una "cooperazione globale tra le forze di polizia europee, inclusa una nuova coscrizione dei fornitori dei nuovi sistemi di comunicazione, al fine di portare avanti le intercettazioni nel caso in cui ve ne fosse la necessità, seguendo specifiche istruzioni"[482].

Oltre ad *Echelon*, l'Europa è sottoposta ad un altro tipo di controllo, *Enfopol*: ma se *Echelon* è pressochè estraneo all'Europa (escluso il duplice, ambiguo ruolo dell'Inghilterra, membro dell'Unione Europea ed al contempo *partner* del progetto *Echelon*), così non si può dire di *Enfopol*. Tale progetto, anzi, ha una sua precisa valenza politica, come è stato evidenziato il 3 dicembre 1995 a Madrid, nel corso del summit "EU-US", quando è stato firmato il trattato *Transatlantic Agenda*. Tale documento conteneva il *Joint EU-US Action Plan*, nel quale si sono gettati le basi per "ridefinire l'Alleanza Atlantica nell'era post Guerra Fredda"[483].

Come per *Echelon*, il Parlamento Europeo, i Governi dei singoli Paesi membri, nemmeno il Comitato per le libertà civili del Parlamento Europeo, hanno attuato alcuna forma di controllo su tale sistema, il quale, secondo *StateWatch*, sarebbe stato deciso in segreto tra i governi dei paesi interessati. Se il grande

---

478 Rapporto al COREPER "Interception of communications", ENFOPOL 40, 10090/93, Bruxelles, 16-11-93.

479 La similitudine con *Echelon* è rafforzata proprio dal fatto che Australia e Nuova Zelanda sono partner stessi del progetto.

480 Cfr. C. GIUSTOZZI, A. MONTI, E. ZIMUEL, *op. cit.*, p. 201.

481 I*bidem*.

482 Cfr. R. CHIESA, *op. cit.*, pp. 16-17.

483 I*bidem*.

orecchio di *Echelon* ha trovato un valido alleato, la *privacy* ha trovato un altro avversario.

Capitolo Diciottesimo

CRITTOGRAFIA, SORVEGLIANZA GLOBALE E *PRIVACY*

SOMMARIO: 1. Le accuse ad *Echelon*. – 2. *Echelon* e *privacy* negli Stati Uniti d'America. – 3. *Echelon* e l'Unione Europea. – 4. La compatibilità tra *Echelon* e la legislazione dell'Unione Europea. – 5. La Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali. – 6. L'Articolo 8 della Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali e le attività dei servizi di *intelligence*. – 7. Alcune considerazioni. - 8. Conclusioni.

1. Le accuse ad *Echelon*.

Il caso *Echelon* non ha scosso l'opinione pubblica mondiale solo a proposito di tematiche di natura economica. Al contrario, anche il fatto che *Echelon* rappresenti una minaccia alla *privacy* dei cittadini ha provocato la reazione del Parlamento Europeo e di vari Governi nazionali[484], compresi quelli dei Paesi facenti parte dell'Accordo UK - USA.
In tutto il mondo il caso *Echelon* ha scatenato un coro unanime di proteste: singoli parlamentari ed europarlamentari, garanti della *privacy* come Stefano Rodotà, il garante italiano, organizzazioni per la tutela dei diritti civili, i *mass media*, tutti sono d'accordo nel condannare l'attività di *Echelon* considerando tale sistema una palese violazione del diritto alla *privacy* ed alla riservatezza delle comunicazioni[485].

---

[484] Cfr. *European Parliament Investigation of Echelon*, *op. cit.,* paragrafo 5.9. "Parliamentary reports" e *Development of Surveillance Technology and Risk of Abuse of Economic Information* (*An Appraisal of Technologies of Political Control*), part 2/4:"The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and natinal law", PROF. CHRIS ELLIOTT, Scientific and Technological Options Assessment (STOA), Parlamento Europeo, PE 168.184/Part 2/4, Aprile 1999 (rapporto disponibile sul sito web: cryptome.org/dst-2.htm, sito consultato il 12 luglio 2002).
[485] Cfr. S. RODOTÀ, *L'occhio di Echelon e la società trasparente*, su La Repubblica, 6 aprile 2000 (disponibile sul sito Web http://www.repubblica.it, sito consultato il 15 luglio 2002) ed intervista *L'alleanza per lo spionaggio globale va contro le leggi dell'Unione Europea*, dossier *Echelon*, in *La Repubblica*, 19 giugno 2001, p. 13.

Accertata l'esistenza di *Echelon*, il problema che si pone ora la comunità internazionale è di definirne le sue finalità: è solo un sistema utilizzato per fini di sicurezza nazionale? O comprende altri scopi?
In precedenza si è evidenziato come la portata di *Echelon* sia ben più ampia: tale sistema, infatti, sarebbe utilizzato dai cinque Paesi che lo gestiscono, Stati Uniti d'America *in primis*, per acquisire dati di natura economica per avvantaggiare le proprie aziende, diventando così uno strumento per compiere attività di spionaggio economico-commerciale, distorcendo la competizione e la concorrenza internazionale tra imprese, alterandola a favore di quelle appartenenti ai cinque Paesi che aderiscono al progetto *Echelon*.
Ma le accuse ad *Echelon* non riguardano unicamente il settore dell'economia internazionale: tale sistema è attualmente accusato di violazione del diritto alla *privacy* ed alla riservatezza delle comunicazioni.
Le accuse maggiori provengono non solo dal Parlamento Europeo, ma anche dallo stesso Governo americano che vede in *Echelon* un pericolo per la *privacy* dei propri cittadini.

2. *Echelon* e *privacy* negli Stati Uniti d'America.

Le accuse ad *Echelon* non sono una prerogativa unicamente europea: negli Stati Uniti d'America si sono avute diverse reazioni a proposito di *Echelon*.
In effetti, tale sistema di sorveglianza globale delle comunicazioni preoccupa lo stesso Governo americano, il quale teme che questo sistema possa ritorcersi contro l'America stessa ed i suoi cittadini[486].
Come già si è visto, *Echelon* è in grado di intercettare qualsiasi tipo di comunicazione elettronica in qualunque punto della terra, e, soprattutto, di immagazzinare, oltre a comunicazioni, anche dati ed informazioni riguardanti qualunque persona, compresi i cittadini americani: la *National Security Agency* è in grado di memorizzare negli archivi dei suoi potenti computer più di 5.000 miliardi di pagine.
Ma i dati riguardanti persone di cittadinanza americana non possono essere conservati per sempre, ma solo per un limitato periodo di tempo, cioè un anno; al contrario, informazioni concernenti persone di cittadinanza straniera possono essere conservate per sempre.
Il fatto che la *National Security Agency* spii i propri cittadini è una problematica tuttora aperta, ma affatto nuova.
Anche in passato l'agenzia di Fort Meade aveva dovuto rispondere ad accuse di violazione dei diritti alla *privacy* dei cittadini americani, violazioni commesse durante lo svolgimento di operazioni come l'"Operazione Shamrock" ed il "Progetto Minaret", operazioni che resero evidenti le reali capacità della NSA e del pericolo che tale agenzia poteva rappresentare in assenza di una precisa regolamentazione e di un adeguato organo di controllo da parte del Governo statunitense.

---

486 Cfr. J. BAMFORD, *Body of Secret*, *op. cit.*, p. 427.

In effetti, a seguito dello scandalo e della commissione d'inchiesta (il *Church Committee*) che indagò su tali attività da parte della *National Security Agency*, il Governo degli Stati Uniti d'America decise di creare il "Foreign Intelligence Surveillance Act" (FISA), dove per la prima volta si creava una sorta di regolamentazione delle attività della *National Security Agency* e si elencava quello che l'agenzia poteva e, soprattutto, non poteva fare[487].
Uno dei punti fondamentali di quell'atto era il divieto assoluto, da parte della NSA, della creazione delle "watch lists", le liste di cittadini americani che l'agenzia di Fort Meade (ma non solo, visto che alla compilazione di tali liste avevano partecipato anche altre agenzie governative come la CIA) doveva tenere sotto controllo perché sospettati di attività illegali o sovversive nei confronti del governo americano.
Il "Foreign Intelligence Surveillance Act" istituì anche una apposita corte federale, la "Foreign Intelligence Surveillance Court" (FISC), la quale ha tuttora il preciso compito di evitare che la *National Security Agency* compia azioni di spionaggio indiscriminate nei confronti dei cittadini americani.
Si vuole evitare in questo modo che essa metta in moto massicce operazioni di spionaggio su vasta scala, non mirate su specifici cittadini, ma, al contrario, basate su intercettazioni di migliaia di cittadini americani.
Se la *National Security Agency* vuole compiere operazioni verso un preciso cittadino americano, essa è obbligata ad ottenere un permesso speciale dal *Foreign Intelligence Surveillance Court*, che valuterà l'effettiva necessità e la reale esistenza di prove che ammetterebbero il ricorso alle intercettazioni.
Al fine di concedere il permesso, la corte deve accertare che il cittadino da tenere sotto controllo sia implicato in attività di spionaggio, terrorismo o collabori per un Paese straniero, e che tali attività rappresentino una effettiva minaccia alla sicurezza nazionale.
Ulteriore regolamentazione delle attività consentite alla NSA è la Direttiva 18, "Limitations and Procedures in Signals Intelligence Operations of the United States Sigint System" del *United States Signals Intelligence* (USSID 18), in vigore dal maggio 1976, cioè appena dopo la conclusione dell'investigazione del *Church Committee*.
Appare evidente che questa regolamentazione delle attività della NSA valgono solo sul territorio americano.
In effetti, l'agenzia può effettuare intercettamenti di cittadini americani non appena essi oltrepassino il confine, e per fare ciò non è necessaria l'autorizzazione del *Foreign Intelligence Surveillance Court*, ma è sufficiente quella del procuratore generale degli Stati Uniti d'America.
L'autorizzazione del FISC non è necessaria neppure per monitorare le comunicazioni da e verso le ambasciate straniere ed il personale diplomatico che si trovano sul territorio americano.
È importante considerare come le regolamentazioni applicate alle attività della *National Security Agency* funzionano su un duplice livello: da una parte, esiste una forte regolamentazione a proposito di operazioni riguardanti cittadini americani

---

[487] Cfr. J. BAMFORD, *Body of Secret*, *op. cit.*, p. 440 e *Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control*), part 2/4, *op. cit.*, sottoparagrafo 4.2 "Third countries".

residenti negli Stati Uniti, mentre per quanto riguarda persone di cittadinanza non americana, sia che si trovino o meno sul territorio americano, ad esse si applica una regolamentazione decisamente meno rigida e ciò rende più facile per la NSA svolgere operazioni di monitoraggio delle loro comunicazioni.
Tale distinzione è possibile ritrovarla anche a proposito di cittadini appartenenti ai Paesi membri dell'accordo UK-USA: in effetti, ai cittadini di Canada, Regno Unito, Australia e Nuova Zelanda le regolamentazioni statunitensi specificano che si debbano trattare i loro dati come se si trattassero di cittadini americani, in virtù proprio dell'accordo di collaborazione reciproca e di condivisione di materiale COMINT.
Questo punto è alla base delle accuse di violazione del diritto alla *privacy* formulate dal Parlamento Europeo a proposito di *Echelon*: questa disparità di trattamento ha suscitato notevoli reazioni che hanno portato all'istituzione di apposite commissioni d'inchiesta le quali hanno portato ad altrettanti rapporti al riguardo.
L'ultimo rapporto in ordine cronologico, l'*European Parliament Investigation of Echelon* del maggio 2001, ha evidenziato in effetti come un sistema di intercettamento globale delle comunicazioni come *Echelon* sia di fatto incompatibile con le leggi e le direttive comunitarie[488] per la difesa della *privacy* dei cittadini europei.
Tali accuse sono state formulate non solo nei confronti degli Stati Uniti d'America, ma anche nei confronti del Regno Unito: questo Paese si trova di fatto in una posizione particolare, in quanto è membro sia dell'accordo UK-USA, ed è un partecipante attivo al progetto *Echelon*, ma è anche un membro dell'Unione Europea e di conseguenza è sottoposto alle specifiche leggi comunitarie in materia di *privacy*[489].

3. *Echelon* e l'Unione Europea.

Il quotidiano inglese *The Economist*[490] ha scritto nell'editoriale *The End of Privacy* che:"[...] tutti i tentativi di limitare la sorveglianza elettronica e l'intrusione di tale sorveglianza nella vita privata falliranno. Forse si adotterà qualche leggina [...] ma la *privacy* scomparirà comunque. È meglio comunque che i cittadini si abituino a vivere senza *privacy*. Sarà il vero grande cambiamento del mondo

---

488 Le specifiche leggi comunitarie in materia di *privacy*, di riservatezza delle comunicazioni e di trattamento dei dati personali sono: Articolo 286 del Trattato CE; Direttiva 95/46/EC; Direttiva 97/66/EC; Articolo 6(2) del Trattato sull'Unione Europea che sancisce l'obbligo per l'Unione Europea a rispettare i diritti fondamentali; Articolo 7 (tutela della vita privata e della vita familiare e del rispetto delle comunicazioni) ed Articolo 8 (diritto alla protezione dei dati di carattere personale) della Carta dei Diritti Fondamentali dell'Unione Europea. Articolo 8(2) (tutela della vita privata e della riservatezza della corrispondenza) della Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali.
489 Cfr. *European Parliament Investigation of Echelon*, *op. cit.,* "Compatibility of an "Echelon" type interception system with Union Law".
490 Cfr. l'editoriale *The End of Privacy*, quotidiano The Economist, 18 maggio 1999, in F. COLOMBO, *op. cit.,* pp. 116-117.

moderno che comincia ora. [...] si capisce al volo che per il prossimo futuro la *privacy* è condannata a sparire".
Lo scenario che questo articolo prospetta sembra essere tratto dal romanzo di George Orwell, *1984*, nel quale si ipotizzava uno società totalmente controllata in ogni sua forma, dove la libertà e la *privacy* erano state spazzate via da un'entità superiore che controllava le azioni ed i pensieri di ogni singolo cittadino.
Oggigiorno risulta difficile credere che le profezie che Orwell prevedeva oltre cinquant'anni or sono possano avverarsi nell'immediato futuro: la realtà è ben diversa, ma è possibile, in ogni modo, porsi alcune considerazioni in materia di *privacy* e di come tale diritto sia rispettato o meno.
Il paragrafo precedente ha illustrato i problemi che il caso *Echelon* ha creato negli Stati Uniti d'America, il Paese *leader* di questo progetto, e di come il Governo americano abbia creato precise regolamentazioni ed organi per impedire un uso indiscriminato ed incontrollato di tale sistema: da una parte una efficace struttura di *intelligence* per scopi di sicurezza nazionale, dall'altra un organo troppo potente da risultare incontrollabile, il quale potrebbe ritorcersi proprio contro gli Stati Uniti d'America.
Problemi ancor maggiori sono emersi difatti nei Paesi che rappresentano l'oggetto delle attività di spionaggio di *Echelon*, come i Paesi membri dell'Unione Europea, in quanto le comunicazioni di questi Paesi sono sottoposti ad *Echelon*, il sistema di sorveglianza delle comunicazioni.
La questione relativa alla legalità di un sistema come *Echelon* e della compatibilità o meno con le leggi dell'Unione Europea è stata ampiamente affrontata prima dal rapporto *Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control)*:"The legality of the interception of electronic communications: a concise survey of the principal legal issues and instruments under international, European and national law" dell'aprile 1999 e poi dal più recente rapporto *European Parliament Investigation of Echelon*[491] del maggio 2001, il quale ha specificato ed integrato alcuni importanti punti relativi questa delicata questione.

4. La compatibilità tra *Echelon* e la legislazione dell'Unione Europea.

Nell'Unione Europea la tutela dei diritti e delle libertà fondamentali dell'uomo in materia di *privacy* è assicurata dagli Articoli 6 e 7, in particolare dall'articolo 6, punto secondo del TUE, il trattato dell'Unione Europea.

---

[491] Cfr. *European Parliament Investigation of Echelon*, *op. cit.,* paragrafo 7.2., "Compatibility of an intelligence system with Union law", in particolare sottoparagrafo 7.2.1. "Compatibility with EC law" e 7.2.2. "Compatibility with other EU law", capitolo 8, "The compatibility of communications surveillance by intelligence services with the right to privacy" e *Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control)*, part 2/4, *op. cit*., paragrafo 2 "International Agreements", paragrafo 3 "EU legislation and agreements" e paragrafo 4 "National Legislation".

Questi articoli contemplano il rispetto di questi diritti come garantito dall'*European Convention for the Protection of Human Rights and Fundamental Freedoms* (ECHR), la Convenzione Europea per la Salvaguardia dei Diritti e delle Libertà Fondamentali dell'Uomo[492].

Questi articoli affermano che se uno Stato membro promuovesse l'uso di un sistema di intercettazione, consentendo ai propri servizi di *intelligence* di operare un sistema tale o consentendo ai servizi di *intelligence* di un Paese straniero di utilizzare il suo territorio per questo scopo, tutto ciò rappresenterebbe indubbiamente una violazione del diritto comunitario[493].

Tutti gli Stati dell'Unione Europa devono garantire, pertanto, l'assoluta riservatezza delle comunicazioni, "in particolare essi devono proibire l'ascolto, l'intercettazione, la registrazione ed altri tipi di intercettazione o sorveglianza delle comunicazioni"[494].

Da ciò risulta evidente come un sistema di intercettazione globale delle comunicazioni come *Echelon* sia in contrasto con le leggi sulla difesa della *privacy* dell'Unione Europea, in quanto esse proibiscono ai propri membri di compiere tali operazioni.

Di conseguenza la Gran Bretagna, Paese che aderisce al progetto *Echelon*, si troverebbe in una situazione di palese violazione del diritto comunitario in quanto rea di compiere attività di spionaggio ai danni degli altri Paesi membri. Ma prima di trarre conclusioni affrettate, è necessario interpretare pienamente gli atti comunitari in materia.

In effetti, il punto 14 dell'articolo 6(2) del Trattato dell'Unione Europea specifica che sussiste la possibilità di compiere eccezioni, ma solo in caso esse fossero ritenute assolutamente necessarie per salvaguardare la sicurezza nazionale e la difesa della nazione[495].

Echelon, pertanto, non rientra in queste eccezioni, in quanto, anche se i cinque Paesi aderenti al progetto lo hanno creato principalmente per motivi di sicurezza nazionale, esso è un sistema di controllo globale delle comunicazioni il quale si basa su un sistema di intercettamento su vasta scala sulla base di liste di parole chiave, non mirato su un preciso obiettivo.

Inoltre, le attività di spionaggio industriale compiute utilizzando *Echelon*, contemplate nel precedente capitolo, rafforzerebbero le accuse di illegalità nei confronti di tale sistema, in quanto tali azioni non rientrerebbero nel campo della sicurezza nazionale, ma piuttosto in quello dello spionaggio economico, violando di conseguenza l'articolo 6(2) del TUE[496].

In materia di *privacy*, la Unione Europea ha fortemente difeso questo diritto: ogni atto che implica l'intercettazione di comunicazioni, ed anche la registrazione di dati da parte dei servizi di *intelligence* per questo scopo, rappresenta una violazione della *privacy* individuale.

---

492 Cfr. rapporto *European Parliament Investigation of Echelon*, *op. cit.,* sottoparagrafo 7.2.2., *op. cit.* e *Development of Surveillance Technology and Risk of Abuse of Economic Information (An Appraisal of Technologies of Political Control)*, part 2/4, *op. cit*., paragrafo 2 e paragrafo 3.

493 Cfr. rapporto *European Parliament Investigation of Echelon*, op. cit., paragrafo 7.3 "The question of compatibility in the event of misuse of the system for industrial espionage".

494 *Ibidem.*

495 *Ibidem.*

496 *Ibidem.*

Nei Paesi dell'Unione Europea la *privacy* gode di una protezione speciale, e violazioni di tale diritto sono autorizzate solo dopo accurate analisi degli aspetti legali, e sempre nel rispetto del principio di proporzionalità[497].
La tutela della *privacy* e la sua difesa come diritto fondamentale è contemplata non solo dal diritto comunitario, ma esistono numerosi accordi anche nel diritto internazionale[498].
Particolare importanza rivestono la Convenzione Internazionale sui Diritti Civili e Politici, per la precisione l'Articolo 17, che fu adottata dall'Assemblea Generale delle Nazioni Unite il 16 dicembre 1966[499].
L'articolo 7 della Carta dei Diritti Fondamentali dell'Unione Europea, "Rispetto per la vita privata e familiare", contiene le basi per la tutela della *privacy* di ogni singolo cittadino dell'Unione Europea: "Ciascuno ha il diritto al rispetto della propria vita familiare, del proprio domicilio e delle proprie comunicazioni".
In aggiunta, l'articolo 8 della medesima Carta sancisce il diritto fondamentale alla tutela dei dati personali[500].
La Carta è stata firmata dai Presidenti di Parlamento, Consiglio e Commissione il 7 dicembre 2000, ma ad essa è possibile attribuire solo una rilevanza dal punto di vista politico: essa, infatti, non offre ai cittadini europei una adeguata protezione dal punto di vista legale, in quanto non è stata inserita nel Trattato dell'Unione Europea.
In ogni modo, l'Unione Europea è dotata di un valido strumento per la tutela della *privacy*: l'"European Convention for the Protection of Human Rights and Individual Freedom (ECHR)"[501].

5. La Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali.

---

497 *Ibidem*, paragrafo 8.1 "Communications surveillance as a violation of the fundamental right to privacy".
498 Il rapporto *European Parliament Investigation of Echelon* riporta gli articoli in materia di *privacy* contenuti in trattati internazionali e comunitari: Articolo 12 della Dichiarazione Universale dei Diritti dell'Uomo; Articolo 17 della Convenzione delle Nazioni Unite sui Diritti Civili e Politici; Articolo 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea; Articolo 8 dell'"European Convention for the Protection of Human Rights and Individual Freedom" (ECHR); Recommendation of the OECD Council on guidelines for the security of information systems, adottato il 26/27 Novembre 1993, C(1992) 188/final.
499 Il Protocollo Opzionale di tale convenzione estende i poteri del Comitato per i Diritti dell'Uomo, al quale i singoli individui possono rivolgersi: tale protocollo non è stato però firmato dagli Stati Uniti d'America. Pertanto, un cittadino non può fare ricorso a tale comitato nel caso in cui i suoi diritti, contenuti nella Convenzione Internazionale sui Diritti Civili e Politici, vengano violati dagli Stati Uniti d'America.
500 Cfr. rapporto *European Parliament Investigation of Echelon*, *op. cit.,* paragrafo 8.2."The Protection of Privacy under international agreements".
501 Cfr. rapporto European Parliament Investigation of Echelon, *op. cit.,* sottoparagrafo 8.3.1. "The importance of the ECHR in the EU".

A differenza della Carta dei Diritti Fondamentali dell'Unione Europea, la Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali riveste un'importanza superiore in quanto è stata ratificata da tutti i Paesi membri della Unione Europea: in questo modo, i Paesi dell'Unione Europea hanno costituito un livello di protezione uniforme in Europa per quanto concerne questo settore.
I Paesi firmatari, recependo i principi contenuti nella convenzione, hanno accettato la Corte Europea per i Diritti dell'Uomo di Strasburgo come l'organo competente a pronunciarsi in materia di *privacy*[502].
Tale convenzione ha rappresentato un'importante innovazione in questo campo, in quanto ha riconosciuto la *privacy* come un diritto dell'uomo non legato alla sua nazionalità[503].
Tale diritto deve essere garantito in tutto il territorio dell'Unione Europea, e non sono ammissibili eccezioni di carattere locale, le quali costituirebbero una violazione della convenzione.
Un altro importante punto introdotto dalla convenzione è la validità che viene riconosciuta alla *privacy* anche al di fuori del territorio delle parti contraenti: la Convenzione garantisce a qualunque persona la quale si trovi sul territorio di un Paese aderente al trattato (e non solo ai cittadini di tale Paese) il diritto alla *privacy*, e tale diritto è valido anche all'esterno del territorio dei Paesi UE.
Sussiste pertanto una violazione nel caso in cui una persona subisca una violazione del diritto alla *privacy*, anche se l'azione di interferenza avviene all'esterno dei Paesi dell'Unione Europea[504].
La Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali non ha pertanto circoscritto il diritto alla *privacy* all'interno di confini di natura geografica, ma ne ha invero esteso la sua validità anche all'esterno: ciò assume una rilevanza particolare nel caso della sorveglianza elettronica delle comunicazioni che svolge per l'appunto *Echelon*.
In effetti, le attività Comint sono spesso svolte da Stati (come gli Stati Uniti d'America nei confronti dell'Europa) i quali si trovano geograficamente distanti dal luogo dove si trova la persona sottoposta a sorveglianza e dal luogo dove avviene l'intercettazione della sua comunicazione.
Per esempio, una persona telefona da Parigi a New York: la sua comunicazione è intercettata dalla *National Security Agency*, di stanza nel Maryland, attraverso apparecchi all'interno della base di Menwith Hill, la quale si trova invece in Inghilterra. Secondo quanto sancito dalla Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali, questo costituirebbe una violazione del diritto alla *privacy*, anche se l'intercettazione della comunicazione è svolto a distanza[505].
Questo punto si riferisce in particolare alle comunicazioni internazionali, ma può essere applicato anche alle comunicazioni nazionali, se sono trasmesse utilizzando connessioni esterne, come un satellite.

---

502 *Ibidem*.
503 *Ibidem*, sottoparagrafo 8.3.2. "The geographical and personal scope of the protection provided under the ECHR".
504 Cfr. sentenza Loizidou/Turkey, 23 marzo 1995, Corte Europea per i Diritti dell'Uomo.
505 Cfr. rapporto *European Parliament Investigation of Echelon, op. cit.,* sottoparagrafo 8.3.2., *op. cit.*

6. L'Articolo 8 della Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali e le attività dei servizi di *intelligence*.

La clausola I dell'Articolo 8 della Convenzione evidenzia che "ciascuno ha il diritto al rispetto per la sua vita privata e familiare, il suo domicilio e la sua corrispondenza"[506].
Il rispetto per la *privacy* include non solo il contenuto della comunicazione, ma anche l'atto dell'intercettazione: in effetti, è considerato una violazione della *privacy* anche la raccolta di dati 'esterni' alla comunicazione, come il destinatario, l'ora ed il giorno in cui tale comunicazione è avvenuta e la durata della stessa[507].
Il secondo paragrafo dell'Articolo 8 specifica quali attività sono consentite o meno ai servizi di *intelligence* dei Paesi membri, riportando le eccezioni che acconsentono operazioni di sorveglianza e di intercettamento delle comunicazioni.
Tali attività sono consentite solo nell'interesse della sicurezza nazionale, della sicurezza pubblica e del benessere economico del Paese.
Il rapporto "European Parliament Investigation of Echelon" sottolinea il fatto che motivi di benessere economico non giustificano il ricorso ad attività di spionaggio economico-industriale come quelle descritte nel precedente capitolo, compiute utilizzando il sistema *Echelon*.
In effetti, queste eccezioni sono ammesse solo se "necessarie"[508], e, in ogni modo, nello svolgimento di tali operazioni devono essere sempre utilizzati i metodi meno invasivi possibili ed appropriate forme di garanzia devono essere sempre stabilite per evitare abusi di potere da parte dei servizi Comint.
L'attività dei servizi di *intelligence*, qualora intendano effettuare operazioni Comint, è regolata dall'articolo 8: il contenuto di tale articolo della convenzione rende evidente l'illegalità di *Echelon*, in quanto tale sistema non può essere considerato un'operazione necessaria ai fini della sicurezza nazionale per più motivi.
Innanzitutto, *Echelon* è gestito da Paesi non appartenenti all'Unione Europea: Stati Uniti d'America, Canada, Australia e Nuova Zelanda aderiscono al progetto e fanno parte del *network* di spionaggio globale che fa dell'Europa, e delle sue comunicazioni, un obiettivo principale, se non addirittura il più importante.

---

506 Anche se non vi è un esplicito riferimento alla tutela delle telecomunicazioni, esiste un "case law" della Corte Europea per i Diritti Umani (Klass, European Court of Human Rights, 6.1978) che ha specificato che i termini "vita privata" e "corrispondenza" includono qualunque tipo di comunicazione, la quale in qualunque forma.
507 Cfr. rapporto *European Parliament Investigation of Echelon, op. cit.,* sottoparagrafo 8.3.3. "The admissibility of telecommunications surveillance pursuant to Article 8 of the ECHR".
508 *Ibidem*.

Tali Paesi svolgono pertanto attività di spionaggio ai danni dei Paesi membri dell'Unione Europea, in violazione di quanto sancito nella Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali.
Inoltre, l'attività che questi Paesi compiono attraverso *Echelon* non possono essere considerate necessarie alla sicurezza nazionale ed alla pubblica difesa, in quanto è un sistema che tiene sotto controllo, ripetutamente e quotidianamente, una mole molto vasta di comunicazioni, basando le proprie ricerche su liste di parole chiave generiche: un termine che interessa gli Stati Uniti d'America, può essere una parola chiave di una ricerca effettuata dalla Gran Bretagna, per esempio.
Di conseguenza *Echelon* effettua attività di sorveglianza delle comunicazioni non su precisi soggetti, i quali potrebbero effettivamente rappresentare un pericolo per la sicurezza nazionale, ad esempio terroristi, ma al contrario svolge una capillare azione di controllo su uno spettro di comunicazioni talmente vasto da risultare difficilmente conciliabile con concetti di sicurezza e di difesa nazionale.
L'Articolo 8 specifica che se i servizi di *intelligence* ritengono necessario effettuare attività di controllo delle comunicazioni di un determinato soggetto per motivi di effettiva sicurezza nazionale, tale potere di invasione della *privacy* deve però essere sempre basato sul principio della proporzionalità[509], come definito dall'Articolo 8, comma secondo: la Corte Europea dei Diritti dell'Uomo ha infatti chiaramente espresso che l'interesse dello Stato nel proteggere la propria sicurezza nazionale deve sempre avvenire nel rispetto, per quanto possibile, della *privacy* individuale.
L'ampia intercettazione delle comunicazioni che effettua *Echelon* è, perciò, in netto contrasto con quanto contenuto in tale Convenzione, e costituisce una violazione di tale articolo[510]: un sistema di sorveglianza segreto come *Echelon*, la cui esistenza ed operatività sono giustificate per esigenze di sicurezza nazionale e per la difesa della libertà e della democrazia dei Paesi che ne fanno parte, può al contrario rappresentare proprio una minaccia a quel sistema democratico ed a quella libertà che *Echelon* si prefigge di difendere.
L'Unione Europea deve, pertanto, assicurare ai propri cittadini, ed alla loro *privacy*, un'adeguata tutela, e dotarsi di sistemi di controllo che garantiscano il pieno rispetto di tale diritto da parte di manifeste violazioni, sia da parte di paesi terzi, sia da parte degli stessi membri dell'Unione[511].

7. Alcune considerazioni.

Sulla base dei documenti e dei rapporti esaminati, è possibile fare alcune considerazioni.

---

509 *Ibidem*, sottoparagrafo 8.3.4. "The significance of Article 8 of the ECHR for the activities of intelligence services".
510 *Ibidem.*
511 *Ibidem.*

È necessario innanzitutto che l'Unione Europea si doti in tempi brevi di una precisa regolamentazione in materia non solo dei servizi Comint, ma, più in generale, di una regolamentazione che comprenda tutti i settori dei servizi di *intelligence*: lo scambio di materiale tra servizi di *intelligence* di Paesi differenti può essere permesso, purché questo avvenga nel rispetto della legalità e solo su basi ristrette[512].
La collaborazione tra questi servizi non deve essere impedita, anzi, spesso i migliori risultati in campo internazionale sono ottenuti proprio dal lavoro congiunto di due o più servizi.
La cooperazione che avviene tra le *intelligence* di vari Paesi è perciò comprensibile, ma differente è lo scambio incontrollato di elevate quantità di materiale Comint tra servizi di *intelligence* appartenenti a Paesi differenti.
Lo scambio e la condivisione di materiale Comint può essere ammessa, ma solo su basi ristrette: un'agenzia di *intelligence* può, ad esempio, ottenere informazioni da un'altra agenzia di un Paese straniero, ma tale materiale deve essere stato ottenuto nel rispetto delle leggi di quel Paese. L'agenzia che trasmette materiale, ottenuto violando la legge, commette un reato in quanto non sono stati rispettati i diritti fondamentali di rispetto della *privacy* e della riservatezza delle comunicazioni.
Infatti, anche se il materiale ottenuto è stato commissionato da un'agenzia di *intelligence* di un altro Paese (come avviene durante le operazioni tramite *Echelon*), questo non giustifica in ogni modo la violazione del diritto alla *privacy* da parte dell'agenzia che svolge l'operazione.
Ulteriore considerazione è il fatto che i Paesi dell'Unione Europea, i quali hanno recepito la Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali, non possono consentire a servizi ed agenzie di *intelligence*, appartenenti a Paesi terzi, di effettuare operazioni Comint sul loro territorio nei confronti degli altri Paesi membri dell'Unione Europea[513].
Quanto considerato sin d'ora rende alquanto controversa la posizione del Regno Unito, in quanto tale Paese è membro sia dell'Unione Europea sia del progetto *Echelon*.
In questo paese dell'Unione Europea i servizi di *intelligence* collaborano con quelli di Paesi terzi (sulla base dell'Accordo Uk-Usa), condividendo con essi materiale Comint.
Non è ammissibile, pertanto, che un Paese terzo utilizzi il territorio di un Paese dell'Unione Europea per installare basi e strumenti allo scopo di utilizzarli per finalità di spionaggio[514].
Ciascuno Stato è responsabile delle attività che avvengono sul proprio territorio nei confronti degli altri Paesi dell'Unione, in particolare in un settore così delicato come quello dei servizi di *intelligence*.

---

512 *Ibidem*, paragrafo 8.4. *"The requirement to monitor closely the activities of other countries' intelligence services"*, sottoparagrafo 8.4.1. "Inadmissibilitty of moves to circumvent Article 8 of the ECHR through the use of other countries' intelligence services".
513 *Ibidem*, sottoparagrafo 8.4.1.
514 Ibidem, paragrafo 8.4.2. "Implications of allowing non-European intelligence services to carry out operations on the territory of Member States which are ECHR contracting parties", sottoparagrafo 8.4.2.1. "The relevant case law of the European Court of Human Rights".

La Corte Europea dei Diritti dell'Uomo ha evidenziato come gli Stati contraenti la Convenzione sul rispetto dei diritti dell'uomo abbiano il dovere di adottare misure positive allo scopo di garantire la tutela della *privacy* ai propri cittadini[515].

Se un Paese dell'Unione Europea acconsente all'installazione di basi e strutture nel proprio territorio a servizi di *intelligence* ed agenzie di altri Paesi, le loro attività dovranno, però, essere compiute nel pieno rispetto della legge: il Governo di tale Paese deve, pertanto, assumersi la responsabilità di garantire, non solo ai propri cittadini, ma a tutti quelli dell'Unione Europea, che tali attività non costituiscano una violazione del diritto alla *privacy*, diritto che deve essere assicurato e difeso in base a quanto contenuto nella Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali.

Le precedenti considerazioni hanno implicazioni per le stazioni appartenenti a Paesi terzi che si trovano sul territorio di Paesi dell'Unione Europea.

Per esempio, le basi di *Menwith Hill* in Inghilterra e la base di *Bad Aibling* in Germania sono state dichiarate territorio americano[516]: in queste stazioni, i servizi di *intelligence* americani, per la precisione la *National Security Agency*, svolge, attraverso il sistema *Echelon*, attività di intercettazione di comunicazioni non-militari di privati, i quali si trovano sul territorio di Paesi i quali hanno aderito alla convenzione.

Inoltre, secondo quanto riportato dall'investigazione "European Parliament Investigation of Echelon", nella base di Morwenstow, in Inghilterra, il GCHQ, i servizi Comint inglesi, collaborano con la *National Security Agency* nelle operazioni di intercettazione di comunicazioni civili[517].

In casi come questi, Gran Bretagna e Germania sono responsabili della violazione dell'Articolo 8 della Convenzione: anche se le attività all'interno delle basi sono compiute da un Paese terzo, ed anche se il materiale ottenuto viene utilizzato da un Paese terzo per finalità alle quali Gran Bretagna e Germania sono estranee, la violazione di diritti fondamentali avviene comunque sul loro territorio, e spetta a loro garantire che le attività che vengono svolte all'interno non costituiscano una violazione del diritto alla *privacy*[518].

Se, in futuro, si vorranno evitare violazioni di tali diritti, l'Unione Europea necessita di un'efficace organismo di controllo sui servizi di *intelligence* dei Paesi membri dell'Unione, al fine di assicurarsi che l'operato di tali servizi sia sempre effettuato nel pieno rispetto delle leggi comunitarie.

Tale struttura deve anche assicurare la tutela della *privacy* dei cittadini dell'Unione Europea ed evitare ingerenze da parte di Paesi terzi, come sta avvenendo attualmente con *Echelon*.

---

515 *Ibidem*, sottoparagrafo 8.4.2.1., *op. cit.*

516 Cfr. rapporto *European Parliament Investigation of Echelon*, *op. cit.,* sottoparagrafo 8.4.2.2. "Implications for stations".

517 *Ibidem*, sottoparagrafo 8.4.2.3. "Implications for interception carried out on behalf of third parties".

518 *Ibidem.*

Come descritto precedentemente[519], l'operato della *National Security Agency*, la maggiore agenzia Comint al mondo, è sottoposto ad una forma di controllo da parte di una corte federale, la "Foreign Intelligence Surveillance Court"; inoltre la comunità di *intelligence* degli Stati Uniti d'America è costantemente controllata da commissioni della *House of Representatives* e del Senato.
Questi organi hanno il compito di tenere sotto osservazione le attività dei servizi di *intelligence* americani, supervisionando il loro operato affinché sia sempre svolto nel rispetto della legge e dei diritti dei cittadini americani[520].
Ma questa forma di controllo non viene svolta su tutte le attività alla stessa maniera: in effetti, le operazioni che la *National Security Agency* svolge all'estero non godono dello stesso livello di controllo come quelle che l'agenzia svolge negli Stati Uniti d'America.
Inoltre, la maggior parte della documentazione a proposito delle operazione consentite o meno alla *National Security Agency* qualora svolga operazioni all'estero è inaccessibile in quanto classificata[521].
Se i Paesi membri dell'Unione Europea sono intenzionati alla creazione di un organismo di controllo delle attività dei servizi di *intelligence*, al fine di garantire ai cittadini dei loro Paesi una effettiva tutela della *privacy*, devono conoscere innanzitutto quali attività il Governo degli Stati Uniti d'America acconsente alla *National Security Agency* durante il suo operato all'estero.
Se tali attività non fossero compatibili con quanto sancito nella Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali, l'Unione Europea e gli Stati Uniti d'America dovranno trovare un accordo per garantire ai cittadini dell'Unione Europea un livello di protezione adeguato.
Tale livello di protezione dovrà assicurare che eventuali attività di intercettazioni delle comunicazioni siano esercitate nel rispetto del diritto alla *privacy* che la Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali e la Carta dei Diritti Fondamentali garantiscono e dovranno essere sempre basate sul principio di proporzionalità.
Nel caso delle accuse di spionaggio economico-industriale formulate dall'Unione Europea agli Stati Uniti d'America, le autorità americane hanno ripetutamente giustificato tali operazioni di intercettamento delle comunicazione adducendo che in Europa è frequente l'uso della corruzione e delle tangenti per aggiudicarsi affari[522].
Se questo fosse vero, e le competenti autorità americane ritenessero che le proprie aziende verrebbero svantaggiate da tali pratiche, dovrebbero lasciare il compito di procedere per vie legali al sistema giudiziario europeo, od a quello del Paese nel quale tale reato avviene.
Il Tribunale competente giudicherà l'esistenza o meno di tale reato: nel caso esso realmente sussista, i diritti lesi delle aziende americane saranno garantiti e

---

519 Cfr. paragrafo 7.2 "Echelon e privacy negli Stati Uniti d'America".
520 Cfr. rapporto *European Parliament Investigation of Echelon*, *op. cit.,* sottoparagrafo 8.4.2.4. "Particolar duty of care in connection with third states".
521 *Ibidem.*
522 Cfr. WOOLSEY, *ex* direttore della CIA, nell'articolo *Why America spies on its Allies*, quotidiano *The Wall Street Journal Europe*, 22 marzo 2000, p. 31.

difesi, ma, in caso contrario, si sarà evitato una violazione della *privacy* dei cittadini europei da parte dei servizi COMINT americani.
In effetti, quando la *National Security Agency* effettua operazioni di controllo delle telecomunicazioni di un'azienda europea, sospettando che essa pratichi attività di corruzione e violando, così, le norme del diritto commerciale internazionale, essa stessa compie una violazione, in quanto tali attività sono basate solo su sospetti, non su prove certe[523].
Utilizzando *Echelon*, la National Security Agency attua un sistema di sorveglianza non proporzionale, violando un diritto umano e compiendo, pertanto, un'azione inammissibile.
Se si vuole, pertanto, che la Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Individuali garantisca concretamente i diritti in essa contenuti, l'Unione Europea deve accordarsi con gli Stati Uniti d'America affinché conducano le loro operazioni per motivi di effettiva sicurezza nazionale e sempre nel rispetto dei diritti dei cittadini europei.
Oltre a ciò, le operazioni di sorveglianza delle telecomunicazioni che la National Security Agency effettua sul territorio europeo devono essere regolamentate e controllate dal Governo americano stesso, il quale si impegnerà a tenere sotto controllo le attività compiute dai servizi di *intelligence* per evitare un loro abuso di potere ai danni di cittadini di altre Nazioni[524].

8. Prime conclusioni.

La necessità di dotare l'Unione Europea di una struttura che svolga un'operazione di controllo sulle attività dei servizi di *intelligence* è particolarmente importante per due ragioni: la prima è che le loro operazioni sono coperte da alti livelli di segretezza, e spesso lo stesso Governo per il quale lavorano è all'oscuro del loro operato. In secondo luogo, perché un sistema come *Echelon* effettua operazioni di sorveglianza su vasta scala, entrando in possesso, di conseguenza, di un elevato numero di informazioni personali che spesso non hanno niente a che fare con il vero scopo dell'operazione[525].
Appare evidente che i servizi di *intelligence* delle comunicazioni svolgano attività particolarmente delicate e, spesso, sono preposti ad operazioni al limite della legalità: ciò renderebbe sicuramente ardua l'attività di supervisione da parte di un organo di controllo esterno, e proprio l'attività di quest'ultimo potrebbe risultare inadeguata.
Tale struttura di controllo deve, pertanto, essere in grado di adempiere alle proprie responsabilità nel migliore dei modi, libera da qualsiasi vincolo di natura politica, e questo obiettivo può essere raggiunto - e l'attività dell'organo di controllo può considerarsi soddisfacente - solo se si rispettano i seguenti quattro parametri:

---

523 Cfr. rapporto *European Parliament Investigation of Echelon*, *op. cit.,* sottoparagrafo 8.4.2.4., *op. cit.*
524 *Ibidem.*
525 *Ibidem*, paragrafo 9.3. cfr. "Monitoring of intelligence services".

1) il potere di ordinare operazioni di sorveglianza di telecomunicazioni deve essere riservato solo ad alte Autorità;
2) tale sorveglianza può essere effettuata solo sulla base di un'autorizzazione emanata da un giudice;
3) un organo indipendente deve svolgere un'indagine accurata delle operazioni di sorveglianza che saranno attivate;
4) l'intero operato dei servizi di *intelligence* deve essere soggetto alle attività di controllo da parte di un organo parlamentare[526].
Questi quattro punti sono da ritenersi le condizioni indispensabili al fine di ottenere un organo di controllo in grado di monitorare efficacemente le attività dei servizi di *intelligence*.
Attualmente, la situazione in Europa è da considerarsi insoddisfacente[527]: ciascun Paese dell'Unione Europea possiede legislazioni differenti in materia di servizi di *intelligence* e la stessa differenza sussiste a riguardo degli organi preposti al loro controllo.
In effetti, non tutti gli Stati membri, nei quali operano servizi Comint, si sono dotati di indipendenti organi parlamentari di controllo, dotati di precisi poteri di supervisione. È pertanto necessario che i Paesi membri dell'Unione Europea uniformino le loro legislazioni in materia di servizi Comint, servizi che saranno sottoposti al controllo da appositi organi, i quali garantiranno la legittimità del loro operato.
L'Unione Europea deve garantire un livello di tutela adeguato ai propri cittadini, basato su principi democratici uniformemente condivisi[528]. Queste garanzie di protezione dei cittadini europei stanno assumendo un aspetto nuovo e particolarmente rilevante dal momento in cui l'Unione Europea ha intrapreso la direzione di una politica di sicurezza comune: tale sicurezza comune non può assolutamente disinteressarsi di questi servizi, i quali hanno come compito principale proprio la sicurezza nazionale del loro Paese.
Se si vorrà creare un'unione dei Paesi europei veramente completa, uniforme sotto tutti i punti di vista, politici, economici e sociali, le attività dei servizi di *intelligence* dei Paesi europei necessitano, pertanto, una riforma verso una integrazione dei loro compiti e finalità, non più chiuse all'interno dei loro confini nazionali, ma in un ottica più ampia, più europea.
Quando questi impegni saranno assunti e queste condizioni rispettate, si potrà raggiungere un duplice obiettivo: anzitutto, una effettiva cooperazione a livello europeo tra i servizi di *intelligence*, condizione indispensabile per la creazione di una politica europea di sicurezza comune. Inoltre, si fornirà ai cittadini dell'Unione Europea un livello adeguato di protezione da parte dei servizi di *intelligence* sia del loro Paese, sia appartenenti a Paesi stranieri, e da imponenti sistemi di intercettazione delle comunicazioni come *Echelon*, garantendo così la tutela di diritti fondamentali quali la *privacy* e la riservatezza delle comunicazioni.

---

526 *Ibidem*.
527 *Ibidem*, cfr. paragrafo 9.4 "Assessment of the situation for European citizens".
528 *Ibidem*.

PARTE QUINTA

CRITTOGRAFIA, DIRITTO D'AUTORE E COMMERCIO ELETTRONICO

Capitolo Diciannovesimo

CRITTOGRAFIA E SISTEMI DI PROTEZIONE DEL DIRITTO D'AUTORE

SOMMARIO: 1. Lo scenario e la rilevanza giuridica delle misure tecnologiche di protezione. – 2. Il marchio digitale (*digital watermarking*). – 3. Alcune considerazioni tecniche. – 4. I servizi di *watermarking*. – 5. Altri sistemi di protezione. – 6. I sistemi di protezione del Dvd.

1. Lo scenario e la rilevanza giuridica delle misure tecnologiche di protezione.

La digitalizzazione dei contenuti connessa all'utilizzo sempre più esteso di sistemi *peer to peer* e all'introduzione della banda larga rappresentano, per l'industria dell'*entertainment*, una sfida di importanza cruciale.
La cosiddetta 'napsterizzazione' del mondo dello spettacolo, espressa dal binomio 'digitalizzazione-condivisione', è suscettibile, infatti, di determinare il crollo dell'industria dell'*entertainment*, azzerando i profitti connessi alle tradizionali forme di distribuzione dei contenuti.
Le *major* del mondo della musica che, com'è noto, per prime si sono trovate ad affrontare il fenomeno della distribuzione illecita in Rete di contenuti protetti, hanno denunciato, negli ultimi due anni, un calo del fatturato pari al dieci per cento.
Le dimensioni assunte dal fenomeno della pirateria in Rete potrebbero, certamente, condurre a molteplici riflessioni di ordine giuridico sulla rispondenza e aderenza dell'attuale stato della legislazione in materia rispetto al contesto in cui si muovono, oggigiorno, autori e fruitori di contenuti di carattere creativo.
In questa sede, senza addentrarci in analisi di ampio respiro sulle dottrine del *copyleft*, della filosofia *open source* e della cosiddetta 'gift economy' propria della Rete, basti dire dell'ormai raggiunta consapevolezza circa l'insufficienza di qualsiasi soluzione puramente regolamentare e normativa del fenomeno.
Sono in molti, oggi, a sostenere che l'unica strada realmente percorribile per un'effettiva tutela del *copyright* in ambito digitale sia quella della protezione tecnologica delle opere poste in Rete.
I più recenti provvedimenti normativi adottati in materia di *Intellectual Property Rights* (IPRs) contengono, infatti, specifiche disposizioni volte a sanzionare l'attività di elusione delle misure tecnologiche di protezione del *copyright*, così

come l'attività di progettazione, commercializzazione e distribuzione di strumentazioni a ciò finalizzate.
Ci si riferisce, *in primis*, alle disposizioni contenute nei Trattati Wipo[529] le quali dispongono che ciascuno Stato debba introdurre adeguate forme di tutela giuridica e precostituire mezzi di ricorso efficaci contro l'elusione delle misure tecnologiche utilizzate dagli autori nell'esercizio dei loro diritti, "allo scopo di impedire che vengano commessi nei confronti delle loro opere atti non autorizzati dagli autori stessi o vietati per legge". In secondo luogo, alla normativa statunitense di cui al *Digital Millenium Copyright Act*[530] e comunitaria, di cui alla Direttiva 2001/29 CE, sul diritto d'autore e i diritti connessi nella società dell'informazione.
In ambito nazionale, si è concluso il 24 gennaio 2002 l'esame, da parte del Senato, del Disegno di Legge comunitaria 2001, contenente disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia alla Comunità Europea.
L'art. 29 del Disegno impone l'attuazione della Direttiva 2001/29/CE in materia di diritto d'autore e diritti connessi nella società dell'informazione.
In base a tale articolo, il Governo dovrà emanare, entro un anno dall'entrata in vigore della Legge comunitaria 2001, i Decreti Legislativi recanti le norme necessarie per dare attuazione alla Direttiva 2001/29/CE: nello specifico, il Governo dovrà "prevedere un'adeguata protezione giuridica a tutela delle informazioni sul regime dei diritti, stabilendo idonei obblighi e divieti" e "rideterminare il regime della protezione giuridica contro l'elusione dei meccanismi tecnologici per la protezione del diritto d'autore e dei diritti connessi".
Nell'ambito delle opzioni previste dall'art. 5 della Direttiva 2001/29 CE, dovranno essere ridisciplinate anche le eccezioni ai diritti esclusivi di riproduzione e comunicazione al pubblico (nell'ipotesi, ad esempio, di copia privata per uso esclusivamente non commerciale): si tratta, cioè, di ridefinire i confini del *fair use* al fine di garantire un equo contemperamento tra gli interessi in gioco (quelli alla remunerazione dell'attività creativa e scientifica e quelli al libero accesso al mondo della cultura e dell'informazione).
Attualmente, sembra, infatti, prevalere la tutela del primo tipo di interesse (da cui il dibattito sulla funzione del *copyright* e sulla legittimità di una logica proprietaria in ordine all'accesso e alla fruizione di un comune patrimonio culturale).
La necessità di un approccio combinato di tutela giuridica e tecnologica appare più che evidente ove si consideri che gli strumenti di repressione degli illeciti

---

529 Il *Wipo Copyright Treaty* e il *Wipo Performances and Phonograms Treaty*, sottoscritti in seno all'Organizzazione Mondiale per la Proprietà Intellettuale nel 1996, ed entrati definitivamente in vigore il 5 marzo 2001 con la ratifica del Gabon, ad integrazione del numero minimo di ratifiche per l'entrata in vigore degli stessi (Trenta Stati).
530 Legge federale emanata dall'amministrazione Clinton nell'ottobre del 1998, le cui sezioni 1201 e 1202 sanzionano, rispettivamente, le attività di aggiramento delle misure antiaccesso nonché la loro produzione, commercializzazione e in genere ogni attività che sia primariamente finalizzata alla suddetta elusione, e l'attività di rimozione e alterazione delle *Copyright Management Informations* (cosiddette Cmi).

sono applicabili solo successivamente al raggiungimento della prova della commissione dell'atto o del comportamento illecito.
Ora, nel passaggio dalla comunicazione tramite reti proprietarie a reti pubbliche aperte quali Internet, accade che l'assenza di obblighi di identificazione e, quindi, l'anonimato del navigatore, unito all'enorme quantità di dati che transitano in Rete, renda estremamente difficile non solo l'identificazione dell'autore dell'illecito ma, altresì, l'identificazione e la prova della perpetrazione stessa dell'attività illecita.
Ecco, quindi, che si impone in modo sempre più urgente la necessità di garantire la confidenzialità, l'integrità e la paternità dei dati che transitano *on-line*, non più assicurata dal tipo di rete (proprietaria) utilizzata e dai relativi accordi-quadro, come nell'*Electronic Data Interchange* (Edi).
In questa sede si prenderanno, peraltro, in considerazione esclusivamente le tecnologie atte a garantire una corretta distribuzione *on-line* di contenuti protetti da *copyright*.
Ma quali sono le esigenze sottese ad una corretta distribuzione *on-line* di opere digitali tutelate?
A ben vedere esse si riducono alla necessità di impedire la circolazione non autorizzata dell'opera e, quindi, *in primis*, la riproduzione abusiva del dato digitale.
Va da sé che impedire la riproduzione abusiva significa possibilità, per il titolare dei diritti, di poter identificare in modo univoco la propria opera e l'utilizzatore legittimo della stessa.
È necessario, in altre parole, individuare sistemi tecnologici in grado di seguire l'opera nel suo cammino attraverso la Rete, mantenendone una traccia indelebile in modo che, quand'anche l'opera dovesse essere sottoposta a modifiche e alterazioni, rimanga comunque possibile individuarla con precisione.
A tal fine, il ricorso a sistemi di crittografia si rivela quasi sempre insufficiente, in quanto non si riesce ad impedire che l'informazione, una volta decifrata, possa essere diffusa liberamente in Rete e liberamente duplicata o modificata senza che di queste operazioni rimanga alcuna traccia.
Per soddisfare l'esigenza sopra esposta, si deve necessariamente far ricorso a sistemi di marchiatura delle opere che permettano l'identificazione delle stesse a prescindere da eventuali modifiche o alterazioni.

2. Il marchio digitale (*digital watermarking*).

Il marchio digitale si basa su equazioni matematiche che vengono immesse nel codice binario dell'informazione digitalizzata.
Avviene, sostanzialmente, che si ha un'aggiunta di informazioni sotto forma di codice binario alla quale corrisponde, all'atto della fruizione dell'opera, un'alterazione impercettibile - o tendenzialmente tale – dell'opera stessa.
La trama numerica inserita all'interno del *file* associa ad esso informazioni che lo caratterizzano quali, ad esempio, quelle relative all'autore, al distributore e

all'acquirente autorizzato: generalmente la filigranatura sarà invisibile e permetterà di identificare la fonte, l'autore, il proprietario, il distributore o, più semplicemente, l'utente autorizzato, senza che quest'ultimo possa, in alcun modo, percepire l'esistenza di tali informazioni.
Esistono, tuttavia, anche filigrane visibili: in quest'ipotesi, la funzione della filigranatura digitale è comparabile a quella della tradizionale tecnica di filigranatura della carta in cui il disegno o l'emblema ottenuti nello spessore del foglio risultano visibili in trasparenza.
In sostanza, entrambi i tipi di filigrana hanno lo scopo di inibire l'utilizzazione non autorizzata di un'opera tutelata differendo, tuttavia, nella loro concreta operatività: le filigrane visibili hanno una chiara funzione deterrente, mentre quelle invisibili si collocano evidentemente sul piano dell'agevolazione dell'azione persecutoria.
In questa seconda ipotesi, ammesso che la filigrana sia effettivamente permanente e inalterabile, è possibile, in caso di uso illecito del *file*, rivendicare la titolarità dei diritti esclusivi violati, in quanto non concessi in licenza e tracciare l'illecita redistribuzione del *file* protetto in Rete.
Le tecniche per contrassegnare le opere si distinguono, quanto ai mezzi tecnici utilizzati, a seconda del tipo di opera sul quale il marchio digitale deve essere apposto: in seguito, si fornirà, a riguardo, una sintetica *overview* sulle soluzioni più diffuse.
Prioritariamente, risulta tuttavia opportuno soffermarsi brevemente sulle caratteristiche fondamentali cui il marchio digitale deve rispondere per dirsi efficace.
Tali caratteristiche possono essere ricondotte alle seguenti: 1) non invasività (il marchio deve essere sia statisticamente che percettivamente non rilevabile); 2) rapida estraibilità (al proprietario dei dati o ad un'autorità di controllo *ad hoc* deve essere garantita la possibilità di estrarre e controllare i dati contenuti nel codice in modo rapido); 3) robustezza: (il marchio non deve essere rimovibile e deve resistere agli attacchi sino al punto che eventuali manipolazioni per rimuoverlo debbano rendere l'opera inservibile prima che sia possibile ottenerne la rimozione o la modifica); 4) univocità (il marchio deve garantire che non vi sia ambiguità nell'identificazione dell'opera); 5) non numerabilità (deve essere possibile generare un gran numero di marchi fra loro distinti).
La filigranatura di un *file*, pur implicando una rielaborazione del contenuto originale dello stesso, differisce profondamente dalle tecniche di cifratura che, pur comportando anch'esse la modifica del *file* originale, non ne consentono la fruizione senza l'opportuna chiave di decifrazione.
Le tecniche crittografiche mirano, infatti, ad assicurare la confidenzialità delle informazioni trasmesse per cui, tramite il loro utilizzo, si garantisce che nessuno che non sia in possesso della chiave privata corrispondente alla chiave pubblica utilizzata per la codificazione delle informazioni possa rendere intelligibile il messaggio trasmesso.
Al contrario, un *file* sottoposto a filigranatura digitale rimane invariato e, quindi, riconoscibile immediatamente nei suoi contenuti.
Un documento cifrato, inoltre, una volta decifrato non mantiene o, almeno, non dovrebbe mantenere alcun effetto residuo del processo cui è stato

sottoposto: esso potrà, quindi, essere agevolmente riprodotto e, eventualmente, redistribuito in violazione delle privative d'autore.
Al contrario, lo scopo della filigranatura è quello di associare una determinata trama al *file* al fine di condizionarne ogni successiva utilizzazione.
A tal fine, la filigrana dovrà chiaramente essere difficile, se non impossibile, da eliminare senza causare un evidente degrado del *file* da cui sia stata eventualmente rimossa (cosiddetta 'robustezza del marchio').
In particolare, una delle caratteristiche fondamentali che deve possedere il *watermark* è quella di rendere possibili quelle modifiche che sono maggiormente comuni alla normale gestione del *file* marcato.
Ad esempio nel caso di immagini debbono essere consentite, oltre alle scontate operazioni di manipolazione geometrica quali il ridimensionamento, la rifilatura, la traslazione, la rotazione e il ribaltamento, anche operazioni quali il *dithering*, ossia la ricalibrazione dei colori o l'applicazione di filtri.
Una caratteristica praticamente irrinunciabile consiste, inoltre, nella capacità del *watermark* di sopravvivere ad una delle operazioni più frequenti cui viene sottoposta un'immagine: la compressione, per esempio in formato JPEG, mediante eliminazione delle informazioni percettivamente non rilevanti e conseguente significativa riduzione delle dimensioni del *file*.
Altra caratteristica fondamentale che deve possedere il *watermark* è costituita, come sopra accennato, dalla possibilità di stratificare in momenti differenti, all'interno dello stesso *file*, filigrane diverse e fra loro non correlate, senza che le prime vengano a deteriorarsi per l'aggiunta delle successive garantendosi, in tal modo, l'aggiornamento del *right management*.

3. Alcune considerazioni tecniche.

Le tecniche di marchiatura sviluppate si basano su complesse equazioni matematiche: in sostanza, all'interno del bene oggetto di tutela viene inserito un segnale che provoca un'impercettibile modifica del contenuto dell'opera al momento della sua fruizione.
Qualsiasi tipo di contrassegno digitale deve rispondere alle seguenti caratteristiche di efficacia: a) il marchio non deve essere invasivo (in nessun caso dovrà, quindi, comportare un'alterazione qualitativa del prodotto multimediale); b) deve presentare requisiti di robustezza tali da potere resistere ad eventuali manipolazioni finalizzate alla sua rimozione; c) deve permettere l'individuazione dell'opera a prescindere da eventuali modifiche conseguenti alla fruizione; d) deve essere prontamente individuabile dall'autore dell'opera o da altro autorizzato; e) non deve essere in nessun modo individuabile su base statistica, ovvero previa comparazione di più copie appartenenti allo stesso autore; f) deve garantire univocamente la corrispondenza tra l'opera e il codice identificativo apposto.
La tecnica della filigranatura digitale (*digital watermarking*) è stata pensata con l'intento di rendere possibile la tutela dei diritti di proprietà connessi ad un

qualunque tipo di bene soggetto al diritto d'autore e trasmissibile in forma elettronica.
Una 'filigrana digitale' è data da un segnale o da una trama numerica inserita all'interno di un *file*, in modo da associare ad esso informazioni che lo caratterizzino (a seconda del contesto applicativo ipotizzato, si potrà identificare l'autore, il distributore, l'acquirente autorizzato, fornire semplici avvertenze legali ed altro ancora).
Dal momento che tale segnale è presente in ogni copia (non modificata) dell'originale, la filigranatura digitale potrebbe anche esser vista come una 'firma digitale': può essere comune a più copie (e quindi individuare univocamente la provenienza del documento), o può anche essere unica per ogni copia (così da identificarne al contempo lo specifico destinatario).
In ogni caso, la filigranatura di un documento ne implica una rielaborazione del contenuto originale.
È proprio sotto questo aspetto che la filigranatura digitale si distingue da tutti quei molteplici procedimenti esistenti già da tempo (che si potrebbero far genericamente rientrare sotto il nome di tecniche di autenticazione numerica delle informazioni) che prevedono, in effetti, la sola creazione di un *file* separato (se non fisicamente, almeno concettualmente) con cui sintetizzare i contenuti originali del *file* preso in esame.
Le tecniche di cifratura comportano, viceversa, anch'esse la modifica del *file* originale, ma senza l'opportuna chiave di decifratura le informazioni in esso contenute risulteranno non riconoscibili; un *file* sottoposto a filigranatura digitale rimane, invece, sostanzialmente invariato e, quindi, completamente riconoscibile nei suoi contenuti.
Un documento cifrato, infine, una volta decifrato, non mantiene (o, almeno, non dovrebbe mantenere) alcun effetto residuo del processo cui è stato sottoposto.
Lo scopo della filigranatura digitale, di contro, è proprio quello di legare una determinata trama al generico documento in cui è stata inserita, così da condizionarne ogni successiva visualizzazione, stampa o ritrasmissione.
A tal fine, la filigrana dovrà esser difficile (se non addirittura 'impossibile') da eliminare almeno sino al punto da causare un evidente degrado del documento da cui sia stata eventualmente rimossa.
Di pari passo, si dovrà rendere possibile che il *watermark* applicato sopravviva a quelle modifiche che sono comuni alla normale gestione del bene in questione, di modo che l'utente autorizzato non debba soffrire limitazioni eccessive nel suo utilizzo, né possa correre il rischio di danneggiarne inconsapevolmente la filigrana.
Nel caso si abbia a che fare con delle immagini appaiono, ad esempio, quasi scontate e sicuramente innocue manipolazioni geometriche (come il ridimensionamento, la rifilatura, la traslazione, la rotazione ed il ribaltamento di un'immagine) che invece, operate anche solo in misura minima, possano rendere del tutto illeggibile una qualsiasi filigrana che non

sia stata adeguatamente progettata pur mantenendo, al contempo, praticamente inalterata la qualità complessiva dell'immagine stessa[531].
Le manipolazioni geometriche non sono le sole elaborazioni cui può facilmente venir sottoposta un'immagine: si pensi, ad esempio, al *dithering*, alla ricalibrazione dei colori, ed alla semplicità con cui possono venire modificati contrasto e luminosità.
Una variazione di questi ultimi, a dire il vero, non comporta particolari rischi (un loro incremento può, viceversa, addirittura favorire il processo di riconoscimento); né deve poi destare particolare preoccupazione la possibile applicazione della maggior parte dei filtri (lineari e non): possono sì portare ad un'alterazione significativa del *watermark*, ma solo se utilizzati in modo massiccio, così che anche la qualità dell'immagine non può che risultarne gravemente compromessa.
Esistono, però, alcuni filtri particolarmente potenti che, operando in modo adattivo, sono in grado di rielaborare pesantemente il contenuto informativo di un'immagine senza per questo causarne alcun percettibile deterioramento qualitativo.
Altrettanto a rischio è, poi, una delle operazioni più frequenti a cui possa venir sottoposta un'immagine: la compressione.
Il Jpeg (uno dei formati più usati per le immagini disponibili sul Web e, forse, il più usato in assoluto) permette, ad esempio, una spesso significativa riduzione delle dimensioni di un'immagine eliminando da essa qualsiasi informazione non risulti percettivamente rilevante, analogamente a quanto avviene, ad esempio, per l'Mp3.
La capacità di sopravvivere indenne a tale tipo di archiviazione costituisce quindi, per qualsiasi tecnica di filigranatura, un ottimo *test* di robustezza, oltre che una caratteristica praticamente irrinunciabile.
La generica tecnica di *watermarking* non dovrà solo dimostrarsi resistente all'applicazione, anche simultanea, delle diverse possibili manipolazioni fin qui elencate (nonché di qualsiasi altra possa risultare pericolosa in relazione ad altre tipologie di dati); dovrà anche consentire che in uno stesso documento possano venire stratificate, in momenti differenti, filigrane diverse e fra loro scorrelate, senza che le prime vengano a deteriorarsi all'aggiunta delle successive.
L'eventualità di una contraffazione (che modifichi le informazioni contenute nella filigrana, pur mantenendone l'apparente validità) è chiaramente ben più grave dei rischi connessi ad una semplice cancellazione (parziale o totale) delle informazioni legalmente inserite: la contraffazione va assolutamente evitata, in quanto tutti i meccanismi basati sul *watermarking* perderebbero immediatamente ogni ragion d'essere; con la cancellazione o il deterioramento di una filigrana, invece, venendone danneggiati i soli meccanismi persecutori, si può convivere tranquillamente.

---

[531] La resistenza verso simili manipolazioni geometriche è molto importante anche perché è assai facile che di esse si finisca per fare un uso 'implicito' qualora si voglia poter rilevare una filigrana anche a partire dall'immagine stampata (è assai improbabile che una scansione risulti perfettamente allineata con l'originale, nel caso questo non sia noto).

Di contemplare una tale eventualità non se ne può, anzi, fare a meno, visto che, allo stato attuale, non si vede come si possa impedire la collusione fra più acquirenti di una stessa opera e la conseguente realizzazione di una nuova copia sicuramente priva di qualsiasi informazione relativa al *copyright*.
Si possono distinguere, in prima istanza, due tipi di filigranatura digitale, a seconda che la trama introdotta risulti facilmente visibile o meno all'utente occasionale.
Quando visibile, la filigranatura digitale ricorda molto la normale tecnica di filigranatura della carta (concepita dagli antichi cartai come un modo per caratterizzare univocamente la propria produzione), in cui il disegno, l'emblema o la scritta ottenuti nello spessore del foglio risultano comunque visibili in trasparenza. Documenti sottoposti a filigranatura digitale visibile potrebbero essere quindi considerati come documenti impressi in modo elettronico.
La filigranatura invisibile, viceversa, permette di identificare la fonte, l'autore, il proprietario, il distributore o, più semplicemente, l'utente autorizzato, senza che ad esso o ad altri utenti di un documento o di un'immagine possa apparire evidente l'esistenza di tali informazioni.
Ammesso che la marcatura introdotta in un *file* con la filigranatura digitale risulti effettivamente permanente ed inalterabile (così da renderne il riconoscimento certo e indiscutibile), sarebbe allora facile, in caso di un uso illecito, risalire all'utente cui ne fosse stato concesso l'uso, e rivendicare senza tema di smentite la proprietà del documento o dell'immagine.
L filigranatura digitale può essere vista come uno strumento che potrebbe rendere possibile il mantenimento di una traccia di come *file* sottoposti a *copyright* vengano illecitamente ridistribuiti.
In sostanza, tanto le filigrane visibili quanto quelle invisibili hanno lo scopo di inibire il 'furto' di un'opera sottoposta a *copyright*, ma il modo in cui tale obiettivo viene raggiunto è significativamente diverso nei due casi.
Le filigrane visibili, permettendo un'immediata ed evidente identificazione del 'proprietario', azzerano praticamente il valore commerciale di un documento agli occhi di un potenziale 'ladro' senza, peraltro, danneggiare o limitare in alcun modo l'uso legale dello stesso[532]. Scopo primario delle filigrane visibili è, allora, una chiara identificazione della fonte come deterrente per una duplicazione non autorizzata.
Lo stesso deterrente può esser dato dalle filigrane invisibili, ma solo se il 'malintenzionato' è a conoscenza della loro possibile presenza.
Le filigrane invisibili, d'altra parte, meglio si prestano all'autenticazione digitale di un'opera e al riconoscimento del destinatario per essa previsto, così da renderne un'eventuale trasmissione non ripudiabile a posteriori; il loro scopo primario potrebbe quindi, più correttamente, essere individuato nell'agevolazione dell'azione persecutoria, una volta che il 'crimine' sia stato commesso, più che nella sua prevenzione pura e semplice.

---

[532] Un'applicazione pratica di questo concetto è già attualmente implementata, ad esempio, da diverse emittenti televisive, con la sovrapposizione di un *logo* parzialmente trasparente ad una qualche porzione dell'immagine trasmessa.

In linea di principio, però, visto che nessun tipo di filigrana può ritenersi assolutamente inattaccabile, sarebbe auspicabile che il generico acquirente venisse messo in grado, se non addirittura di 'leggere' tutte le informazioni codificate nel *watermark*, di riconoscerne almeno la presenza e la validità.
Ma anche qualora non fosse identificabile dal normale utilizzatore, la filigrana applicata ad un documento digitale dovrà, comunque, essere facilmente individuabile da quegli enti che siano preposti al controllo della diffusione delle opere sottoposte a *copyright*.
In certi contesti potrebbe anche risultare preferibile che la riconoscibilità della filigrana sovrimposta ad un documento possa prescindere dal confronto con la versione originale (non filigranata) dello stesso, di modo che la proprietà intellettuale di un'opera multimediale rappresentata in forma elettronica possa essere verificata con maggiore tempestività ed efficacia.
Un'altra importante distinzione può esser fatta tra quei metodi di filigranatura in cui le informazioni inserite potranno essere effettivamente lette, e quelli che invece inseriscono solo un 'marchio' che potrà essere solamente identificato (controllando la corrispondenza o meno di un dato codice, che dovrà necessariamente esser noto per altra via).
Una filigrana del tipo 'leggibile' può essere molto poco sicura, se è anche non 'confidenziale', in quanto chiunque potrà avere accesso alle informazioni in essa contenute.
Una filigrana si dice confidenziale (*private*) quando prevede un qualche meccanismo per rendere impossibile l'estrazione delle informazioni a chiunque non sia autorizzato
Le tecniche di *watermarking* si distinguono, e vanno quindi analizzate, in relazione al tipo di documento elettronico che si voglia sottoporre a filigranatura: testi, immagini, *file* audio o video.
Comune a tutte si può considerare solo la fase preliminare di definizione del reale contenuto informativo associato al *watermark* che, volendo, potrà comunque venir anch'esso condizionato in base al tipo e agli effettivi contenuti del documento da 'filigranare' (così da favorirne la non percettibilità).
In effetti, ben raramente le informazioni da inserire saranno prese tali e quali sono: anche solo una loro semplice rielaborazione sulla base di una qualche chiave privata potrà, ad esempio, risultare particolarmente efficace nell'aumentare l'affidabilità di qualsiasi meccanismo venga poi adottato
Negli ultimi anni sono stati messi a punto vari tipi di *watermark*, classificabili in base ad alcune categorie esemplificative.
a) *Watermark* visibile: il marchio è strutturato in modo da essere facilmente individuato da chi visualizza l'immagine: tuttavia, esso non può essere rimosso dal fruitore. Il principale vantaggio perseguito attraverso tale contrassegno è quello di scoraggiare l'utilizzo illecito dell'immagine: il valore commerciale di quest'ultima è, infatti, ridotto o addirittura annullato dalla presenza di un elemento che individua univocamente il titolare del diritto d'autore.
b) *Watermark* invisibile: il marchio non è percepibile dal fruitore. Ciò implica che tale contrassegno persegue finalità di repressione dell'illecito, permettendo di individuare e perseguire l'eventuale autore della condotta dannosa.

c) *Watermark* fragile, semifragile, robusto: la categoria suddivide i contrassegni sulla base della loro resistenza alle modifiche dell'immagine: a seconda del livello di robustezza, infatti, essi possono permanere più o meno inalterati.
In particolare, il *watermark* fragile è progettato per essere distorto o distrutto in seguito alla più piccola alterazione dell'immagine; il *watermark* semifragile è strutturato in modo da venire distrutto in seguito a qualsiasi cambiamento che superi una determinata soglia scelta dall'utente; il *watermark* robusto resiste a modifiche molto accentuate.
d) *Watermark* spaziale: tale contrassegno è incorporato nei *pixel* dell'immagine, in modo da modificare sensibilmente l'aspetto dell'immagine in caso di stampa abusiva.
e) *Watermark* cieco: rende possibile una verifica della presenza del marchio a prescindere dall'utilizzo dell'immagine originale.
In genere tale tipo di contrassegno è molto robusto: tuttavia, il fruitore dell'immagine non è in grado di verificare, attraverso il marchio, la sussistenza del proprio diritto di utilizzazione.
f) *Watermark* pubblico o privato: la categoria suddivide i marchi in base al fatto che venga o meno utilizzata una chiave che permetta la lettura del contrassegno a chiunque o solo ai soggetti autorizzati.
g) *Watermark* leggibile o individuabile: il primo tipo di marchio può essere letto dopo l'inserimento nell'immagine, mentre del secondo è possibile soltanto individuare la presenza.

4. I servizi di *watermarking*.

La gamma dei possibili utilizzi del *watermarking* è piuttosto ampia:
Il *Watermarking* di immagini consiste nell'apposizione, all'interno di un'immagine, di una serie di informazioni invisibili all'occhio umano riguardanti, ad esempio, il produttore, il titolare del *copyright*, l'acquirente, il tipo di licenza, la data della transazione, ecc. L'inserimento del marchio digitale avviene tramite un *software*, oppure un semplice *plugin* per i maggiori programmi di fotoritocco (ad esempio *Photoshop*), forniti dalla società proprietaria della tecnologia di *watermarking* che, in genere, riconosce i formati più diffusi di compressione delle immagini (gif, jpeg, tiff, bitmap). All'inserimento del *watermark* nell'immagine digitale si accompagna, frequentemente, un servizio di monitoraggio e tracciamento della circolazione abusiva del documento protetto da *copyright* su Internet, con conseguente indicizzazione dei siti che contengono immagini marchiate e reperimento del responsabile dell'illecita diffusione (la cui identità è registrata nel *watermark*).
Tra le applicazioni più diffuse si possono citare quelle di *SafeImage*, di *Alpha-Tec* (*EIKONAmark*) e *Digimark*.
Il *Watermarking* di video consiste, invece, nella apposizione di un marchio digitale in un filmato, ed è un procedimento del tutto simile a quello descritto a proposito delle immagini, essendo basato su un *software* o un *plugin* fornito dalla società produttrice della tecnologia di *watermarking*. In quest'ipotesi, tuttavia, è

bene rammentare che il filmato deve resistere non solo a modifiche di formato o di rapporto di compressione, ma deve anche poter supportare la diffusione mediante tecnologia *streaming*.
Nel *Watermarking* di *file* audio, l'attenzione ai *watermark* apposti su *file* audio è stata, com'è noto, amplificata dalle vicende relative al caso *Napster* e ai suoi cloni. Sono, quindi, numerose le aziende impegnate nello sviluppo di *watermark* che hanno messo a punto servizi *ad hoc* per il formato audio Mp3. In particolare, accanto alle classiche informazioni su autore/produttore/acquirente codificate all'interno del *file*, alcune aziende offrono soluzioni che integrano la tecnologia di marchiatura con l'*e-commerce*.
È possibile citare, a tal proposito, il caso di *Liquid Audio*. La sua soluzione, *Liquid Music Player* Cd, consente a clienti autorizzati di preascoltare, scaricare traccie dal Web, ascoltarle sul *personal computer*, farne un'unica copia per *compact disc* e, nel caso di aggiornamento del loro sistema, anche di trasferire i *file* sul sistema aggiornato. Ogni brano musicale è filigranato con informazioni sul *copyright* e un codice di identificazione del cliente: 'incrociando' continuamente il codice di identificazione di un acquirente con la filigrana digitale incorporata nel brano si impedisce, di fatto, l'uso non autorizzato.
In pratica, per scaricare un brano ogni cliente deve esibire un 'passaporto' digitale con impresso il nome, l'indirizzo e le informazioni sulla carta di credito. La traccia sarà fruibile unicamente con la copia registrata del software *Liquid Music Player* del cliente. Tale sistema combina un'elevata qualità del suono (tecnologia di compressione *Dolby Digital* AC-3, ma supporta anche il più avanzato algoritmo di compressione AAC), con tecnologie di sicurezza quali filigranatura digitale di *Solana Technology* e sistemi di crittografia di Rsa *Data Security*, ed è stato adottato dalle *major* e da circa 150 etichette indipendenti e artisti.
Per quanto concerne specificamente le caratteristiche che il *watermark* apposto su documenti *audio* deve possedere, si evidenzia come lo stesso debba risultare particolarmente robusto e resistente alla diffusione in *streaming technology*.
Significativa, a tal proposito, l'iniziativa del consorzio Sdmi, acronimo per *Secure Digital Music Iniziative*, un consorzio di *music-industries companies* che ha messo a punto un insieme di *data-encoding tecnologies*, tra le quali *Verance Watermark*, attualmente in commercio e utilizzato per i Dvd audio, oltre ad alcuni sistemi di identificazione atti a prevenire l'estrazione di singole tracce da un determinato supporto.
Sotto il profilo dell'affidabilità della tecnologia messa a punto nell'ambito del consorzio, non ci si può esimere dal spendere alcune parole sul 'caso Felten'.
Nel settembre del 2000, Sdmi ha lanciato una 'public challenge' in cui invitava i membri della comunità scientifica a forzare gli algoritmi alla base delle proprie implementazioni.
Il gruppo di lavoro del Prof. Edward Felten, presso il *Department of Computer Science* della *Princeton University* è, quindi, riuscito a reversare la tecnologia Sdmi, e intendeva rendere pubblico il risultato delle proprie ricerche nell'ambito del *4th International Information Hiding Workshop*, che doveva tenersi nell'aprile del 2001.

La divulgazione dei risultati condotti dal gruppo di lavoro del Prof Felten è stata, tuttavia, fortemente avversata dalla RIAA, *Recording Industries Association of America*, la quale ha minacciato azione legale nei confronti del professor Felten e degli organizzatori della conferenza allegando, in proposito, non solo la violazione dell'*Agreement* che vincolava i partecipanti alla *public challenge* alla non divulgazione dei risultati delle ricerche ma, altresì, la violazione del Dmca in quanto attività volta a facilitare l'elusione di misure di sicurezza a protezione del *copyright*.
La vicenda appena tratteggiata non costituisce peraltro un caso isolato: la vicenda DeCss, così come il caso Sklyarov, insieme al caso Felten, impongono certamente di rimeditare il rapporto tra legislazione a tutela del *copyright* e libertà della ricerca scientifica e di espressione.
Esistono poi altri tipi di *watermarking*:. Accanto ai servizi più comuni di *watermarking* alcune aziende offrono particolari servizi: per esempio, l'inserimento di un *watermark*, riconoscibile con uno *scanner* e un *software* proprietario, nel *layout* (sull'etichetta o sul fondo) di un Cd-Rom, oppure l'apposizione di marchi invisibili sul *package* di un prodotto di modo che il contenuto autentico sia riconoscibile anche dalla semplice analisi della scatola.

5. Altri sistemi di protezione.

Il *digital fingerprint*, così come un'impronta digitale identifica inequivocabilmente una determinata persona fisica, è volto ad identificare un determinato *file*.
Il *fingerprint* non è né un tipo di *watermark* né una firma digitale: esso, cioè, non rappresenta un oggetto *embedded* nel *file* ma un'impronta codificata in un messaggio associato al *file*.
Si tratta, quindi, di una tecnologia molto meno invasiva rispetto a quella del *watermark*, ove può accadere che la distorsione percettiva del *file*, seppur minima, sia mal tollerata dall'utente.
Tecnicamente parlando, un *digital fingerprint* costituisce il risultato di una funzione di *hash* unidirezionale e può essere definito come una stringa di dati univocamente riconducibili al codice binario di cui è composto un determinato *file*, sia esso costituito da un testo, da un *file* audio, da un video o da altro.
Il proprietario o il legittimo distributore di un oggetto digitale può, così, conservare un *digital fingerprint* di ogni *file* licenziato e, tramite appostiti *Web Crawler*, monitorare il Web in modo tale che il *file* cui l'impronta si riferisce possa essere localizzato. Ciò permette un efficace controllo sull'utilizzo e sulla circolazione dello stesso.
L'impronta è chiaramente unica per ogni tipo di *file*: ciò significa che essa è associata ad uno specifico oggetto licenziato ad una determinata persona.
In questo modo, il proprietario dell'oggetto è in grado di identificare il responsabile della distribuzione illecita dello stesso nel caso in cui se ne rinvenga una copia nel possesso di una terza parte.
Chiaramente la tecnologia *fingerprint* non supporta alcuna modifica del *file*.

Per frenare l'ormai dilagante fenomeno della duplicazione illecita di materiale musicale protetto dal diritto d'autore, a fronte del crollo dei prezzi dei dispositivi di masterizzazione e dei supporti ottici registrabili, le maggiori etichette discografiche hanno di recente lanciato sul mercato Cd audio che risultano non duplicabili. Le protezioni utilizzate sono costituite dalla *Cactus Data Shield* di *Midbar*, da *Key2Audio* di Sony, da *MediaCloQ* di *SunComm* e da *SafeAudio* di *Macrovision*.
Le quattro protezioni succitate si basano su due tecniche di introduzione di errore: la prima verte sull'alterazione del sommario del Cd, cosiddetto Toc, acronimo per *Table of Content* (l'equivalente della tavola di allocazione dei *file* di un *hard drive*): un normale lettore Cd non utilizzando il sommario è perciò in grado di leggere il supporto mentre la masterizzazione, così come la lettura su Pc/Mac risultano impossibili; la seconda consiste, invece, nell'inserire, mediante apposita calibrazione del laser, traccie anomale, ossia meno marcatamente incise: i lettori Cd di nuova generazione riescono a leggere il supporto nonostante l'inserimento di queste tracce, mentre, i lettori Cd di vecchia generazione e i lettori Cd-Rom, nel tentativo di correggere gli errori, entrano in *loop* e il supporto risulta così non fruibile.
Le protezioni sopradescritte, quindi, oltre ad impedire la duplicazione illecita, impediscono altresì utilizzazioni lecite, quali la fruizione del supporto su *personal computer* o l'estrazione delle tracce *audio* in formato Mp3. Queste le ragioni alla base della vivace polemica che ha preso corpo attorno al fenomeno dei Cd protetti, per cui i consumatori si trovano, di fatto, privati della possibilità di fruire appieno di un prodotto per il cui godimento hanno generalmente corrisposto cifre tutt'affatto risibili.
Contro quella che viene definita una pratica abusiva dell'industria del disco nei confronti dei diritti dei consumatori, ha preso posizione la stessa Philips, co-inventrice del *Compact Disc* nonché la Eff (*Electronic Frontier Foundation*). Philips lamenta la violazione del marchio 'Compact Disc', di cui è titolare, in quanto i Cd protetti, non rispettando le specifiche Philips, non sarebbero da considerarsi dei veri e propri Cd Audio.
La Eff, a riguardo, evidenzia come ciò costituisca una pratica ingannevole nei confronti dei consumatori, i quali sono di fatto impossibilitati a conoscere a priori i limiti di utilizzo del prodotto che acquistano.
In via più generale è possibile comunque dubitare in merito alla liceità dei sistemi anticopia in parola, proprio sotto il profilo della loro conformità alla legislazione a tutela del *copyright*. La possibilità di effettuare una copia di *backup* del Cd originale, così come quella di estrarre singole tracce da fruire negli ormai diffusissimi lettori Mp3 o su *personal computer*, costituiscono, infatti, fattispecie pianamente riconducibili alla cosiddetta dottrina del *fair use*, o delle utilizzazioni libere, a tenore della quale le attività dell'utente legittimo che non si pongano in contrasto con lo sfruttamento commerciale dell'opera, non costituendo pregiudizio agli interessi del titolare dei diritti, sono da considerarsi lecite e libere nella misura in cui si esauriscano nella sfera privata dell'utente legittimo.
Ancora, l'*Audio Home Recording Act* statunitense del 1992, oltre a sancire esplicitamente il diritto degli utenti di effettuare una copia di *backup* del supporto legittimamente acquistato, stabilisce il diritto delle case discografiche

e degli autori ad una percentuale sul prezzo di vendita dei supporti registrabili (Cd-R e musicassette), a parziale risarcimento dei diritti d'autore che potenzialmente il loro utilizzo comporta.
È evidente, in tal senso, che impedire la registrazione domestica toglierebbe la causa d'essere di queste consistenti entrate.
Disposizioni del medesimo tenore sono, peraltro, presenti nelle legislazioni della gran parte delle Nazioni aderenti alla Wipo: la direzione che gli Stati Uniti d'America prenderanno a riguardo potrebbe quindi avere notevoli ripercussioni internazionali e incidere sul futuro dei sistemi anticopia.

6. I sistemi di protezione del Dvd.

Il primo sistema è denominato *Analog* Cps (*Macrovision*). La finalità specifica di questo sistema di protezione consiste nell'impedire la copia analogica del contenuto protetto. Il sistema *macrovision* consiste in un circuito presente in ogni lettore Dvd o scheda video per computer con un'uscita analogica (composita o S-video) che aggiunge un rapido segnale modulato sulla portante del colore (*Colorstripe*) assieme al segnale di sincronizzazione verticale (Agc) alle uscite video composite e s-video. Ciò confonde i circuiti del sincronismo e del livello automatico di registrazione nel 95% dei Vcr in commercio.
Grazie a questo sistema di protezione la copia presenta difetti visivi quali: strisce di colore, distorsione, perdita di sincronia dell'immagine (*rolling*), immagine in bianco e nero e alternanza di chiaro scuri.
Un ulteriore sistema, abbiamo visto, prende il nome di Css (*Content Scrambling System*). Il Css è un sistema di cifratura e autenticazione dei dati sviluppato dalla Toshiba in collaborazione con Matsushita, con la specifica finalità di evitare la copia dei *file* video direttamente dal supporto digitale. Css cripta i *file* video presenti sul Dvd per cui si rende necessario che il lettore decripti il segnale affinché lo stesso possa essere visualizzato.
Per ogni produttore che richieda una licenza Css, viene rilasciata una chiave da un set di 400 chiavi che sono memorizzate su ogni disco cifrato mediante Css (ciò consente di annullare una licenza semplicemente togliendo la rispettiva chiave dai dischi futuri). L'algoritmo di decrittazione Css scambia le chiavi col *drive* in modo tale da generare un canale sicuro e cifrato sul quale viaggerà la chiave di decrittazione che consentirà la visualizzazione dei contenuti.
Affinché un media cifrato mediante Css sia fruibile è, tuttavia, necessario che l'*hardware* di fruizione sia in grado di includere un modulo di decifratura Css.
Allo stato, tutti i *drive* Dvd-Rom hanno un *firmware* aggiuntivo per scambiare le chiavi di autenticazione e decriptazione con il modulo CSS nel computer.
Interessante è anche il sistema Dcps (*Digital Copy Protection System*). La finalità specifica di questa tecnologia consiste nell'impedire la creazione di copie mediante collegamenti digitali tra periferiche. Un'implementazione di questa tecnologia è quella che è alla base del protocollo *FireWire*, sviluppata da Sony, Hitachi, Matsushita e Toshiba e che prende il nome di Dtcp (*Digital Transmission Content Protection*).

Mediante il Dtcp tutti i dispositivi che sono digitalmente connessi tra loro (ad esempio lettori Dvd, TV digitali, videoregistratori digitali, etc.) si scambiano chiavi e certificati di autenticazione in modo da stabilire una connessione sicura.Il lettore Dvd cripta il segnale audio/video e lo invia al dispositivo ricevente che dovrà decriptarlo: ciò garantisce che nessun altro dispositivo collegato, non autorizzato, sia in grado di ricevere un segnale fruibile.

Capitolo Ventesimo

CRITTOGRAFIA, DIRITTO D'AUTORE E COMMERCIO ELETTRONICO: I SISTEMI DI *DIGITAL RIGHT MANAGEMENT*

SOMMARIO: 1. Tratti salienti dei modelli di distribuzione *on-line* di contenuti. – 2. Le soluzioni adottate.

1. Tratti salienti dei modelli di distribuzione *on-line* di contenuti.

Le nuove forme di distribuzione dei contenuti digitali aprono notevoli opportunità per quasi tutti gli attori coinvolti nella relativa catena di produzione-distribuzione, ad esclusione dei tradizionali *retailers*. Esse rappresentano, per il pubblico, nuovi canali di acquisto; espandono le possibilità di fruizione dei contenuti permettendo, ad esempio, di superare i limiti dei negozi tradizionali nell'offrire ai clienti la possibilità di 'conoscere' il prodotto prima dell'acquisto (e ciò costituisce, probabilmente, l'*atout* maggiore della distribuzione *on-line* rispetto a quella tradizionale); aprono nicchie di mercato per distributori indipendenti o alternativi, conseguentemente ampliando le possibilità di scelta da parte degli artisti.
La distribuzione *on-line* è caratterizza dal bypassaggio del ruolo proprio dei tradizionali intermediari, quali editori e produttori videofonografici: ciò consente agli artisti di avere maggiore forza contrattuale in quanto la disintermediazione, rispetto a posizioni di rendita sulle catene fisiche della distribuzione, permette loro di optare per l'autodistribuzione e, quindi, di rinegoziare il valore relativo dei diritti d'autore e connessi.
Accanto ai vantaggi propri della distribuzione *on-line* emergono, tuttavia, le problematiche inerenti l'effettiva tutela del *copyright* in ambiente digitale, con particolare riguardo all'*enforcement* della normativa in materia.
Nel settore della distribuzione musicale, ad esempio, diverse società hanno già iniziato a sviluppare soluzioni di distribuzione *on-line* che impediscono la duplicazione e/o imputano automaticamente le *royalties* per l'uso dei brani musicali.
La natura delle soluzioni adottate rispecchia diversi modelli di *business*: gli approcci possono essere riuniti in tre categorie essenziali di riferimento: l'approccio *pay to record*, l'approccio *pay for play* e infine le soluzioni *try-before-you-buy* che consentono la fruizione *on-line* gratuita di parte dei contenuti offerti (ad esempio, un brano musicale o anche la versione ridotta dell'intero brano o *album*).

Dal punto di vista legale, il modello *pay to record* non pone particolari problematiche, atteso che la gestione dei diritti, in quest'ipotesi, è del tutto analoga a quella propria della distribuzione su supporto fisico: il fornitore, consentendo il *download*, offre, in sostanza, una copia del prodotto e pagherà i diritti corrispondenti ad autori, esecutori, editori e produttori.
Maggiormente problematico, invece, il versante connesso alla sicurezza.
Il modello *pay to listen* ha il vantaggio di eliminare alcune preoccupazioni inerenti la sicurezza, nella misura in cui non consente registrazioni permanenti, ed è un modello decisamente più economico per il fruitore: il cliente paga una modesta tariffa per ascoltare un *album* o brani singoli ed avere così supporto all'eventuale decisione successiva di acquisto di *Compact Disc* o di altri tipi di copie preregistrate. Il pagamento, data la sua modesta entità, avviene generalmente via carta di debito o per abbonamento.
Questo modello implica, chiaramente, il pagamento di tariffe e *royalties* di esecuzione *on-line*, come nella radiofonia, costituendo esercizio del diritto di comunicazione al pubblico.
Rimane l'ipotesi del noleggio *on-line* che permette di ascoltare più volte un brano o un *album* senza essere costretti ad acquistarne una copia.
La versione audio della tecnologia *Digital Video Express* (DIVx) offre la concreta possibilità ad un fruitore di musica di riascoltare un album o un brano quante volte desidera, ma in un arco limitato di tempo: un meccanismo di misurazione si aziona la prima volta che il fruitore ascolta il brano e si blocca al termine definito, a meno che il fruitore non decida di versare un ulteriore corrispettivo per prolungare il diritto di ascolto.
Tale approccio risulta, tuttavia, generalmente insoddisfacente rispetto alle esigenze del pubblico musicale: a differenza di quanto avviene con le opere audiovisive o cinematografiche, l'utente non si accontenterà di fruire *una tantum* dell'opera ma tenderà, al contrario, ad ascoltare indefinitamente un brano musicale di suo particolare gradimento.
Indubbiamente, quindi, il classico modello che offre una copia permanente di un brano o di un album, il cosiddetto *pay to record*, resta tra i più apprezzati, ma è anche il più esposto ai rischi di pirateria.

2. Le soluzioni adottate.

Dal punto di vista strutturale, un modello di distribuzione *on-line* integra diverse componenti: 1) il prodotto da vendere (un *album* musicale, un singolo brano o anche il diritto di ascoltare un *album* o un brano per un certo numero di volte); 2) il metodo di pagamento (acquisto singolo via carta di credito, carta di debito per tanti piccoli acquisti o abbonamento); 3) la tecnologia che abilita il pagamento; 4) il metodo di gestione dei diritti associato a queste transazioni.
Lo sviluppo di un sistema elettronico di gestione dei diritti di proprietà intellettuale si era posto, già a partire dai primi anni Novanta, come uno dei principali obiettivi che la Comunità Europea intendeva perseguire, attesa la

crescente consapevolezza circa la centralità del ruolo degli Ipr nel contesto della cosiddetta *information society*.
È sulla base di questa consapevolezza che affonda le proprie radici il Progetto *Imprimatur*, progetto di ricerca supportato dalla Comunità Europea nell'ambito del programma Esprit, iniziato nel 1995 e conclusosi ufficialmente nel 1998, che ha condotto alla realizzazione di un prototipo (il *Demonstrator*) di piattaforma tecnologica di gestione degli Ipr in ambiente digitale, acquistato infine dalla costituenda *Imprimatur Services Ltd.* col fine di dare una valida continuazione all'opera di ricerca intrapresa.
Non si è trattato, peraltro, di un'esperienza isolata: CITED (*Copyright in Transmitted Electronic Documents*), COPICAT (*Copyright Ownership Protection in Computer Assisted Training*), COPINET (*Billing system for Open Access Networked Information Resources*) e COPEARMS, (*Coordinating Project for Electronic Author'Rights Management System*) costituiscono altrettante iniziative, per citare le più significative, volte all'implementazione di una piattaforma tecnologica efficiente e sicura da adottare per la distribuzione *on-line* di contenuti soggetti a *copyright*.
Un sistema di *Electronic Copyright Management System* (ECMS o DRM, acronimo per *Digital Rights Management*), è costituito da un pacchetto di tecnologie *hardware* e *software* finalizzate alla gestione e al controllo dell'uso autorizzato di contenuti digitali: secondo l'impostazione di base accolta dai progetti succitati, tali sistemi si fondano, essenzialmente, sulla logica della crittazione combinata al controllo degli accessi.
Ciò richiede, chiaramente, un'attenta calibrazione del carico elaborativo introdotto nell'algoritmo crittografico prescelto: una crittografia debole può, infatti, essere agevolmente violata. L'utilizzo di algoritmi progressivamente più elaborati rischia, d'altro canto, di appesantire eccessivamente la transazione.
Il problema diviene ancora più evidente qualora ci si trovi nella necessità di adottare algoritmi che prevedano l'uso di meccanismi di *key escrow* o *key recovery*[533] ove, a parità di robustezza dell'algoritmo, il processo di gestione della transazione rischierebbe di divenire eccessivamente elaborato e dispendioso.
Un Ecms consta, essenzialmente, di due parti: da un lato c'è la componente sottoposta ai meccanismi di protezione, ossia i dati coperti da *copyright* (come pure l'applicazione di interfaccia che ne consente l'utilizzo), dall'altro il sottosistema di 'supervisione' che controlla le richieste concede o meno l'accesso e registra ogni operazione eseguita attraverso diversi moduli *software* specializzati.
A titolo di esempio, secondo l'impostazione adottata in CITED, si avrà: un modulo Mon (*monitor*) che si occupa di bloccare eventuali attacchi provenienti dall'esterno, fornendo l'accesso all'applicazione protetta solamente agli utenti autorizzati; un modulo Ect (*event capture tool*) che gestisce tutti i flussi di informazione che attraversano il sistema; un Csa (*clearing service agents*) che concede o nega le autorizzazioni all'accesso; un Urc (*use right control*) che

533 Per *key escrow* si intende la consegna delle chiavi di decrittazione ad una terza parte fidata e, per *key recovery*, la procedura consistente nel rendere disponibile a determinate agenzie, tipicamente governative, una via di accesso ai dati crittati.

gestisce le chiavi di accesso e le altre informazioni necessarie affinché il Csa agisca correttamente; un modulo Not (*notarisator*) che tiene un giornale di bordo con tutte le informazioni più significative (i dati contabili, i dettagli sui tentativi di accesso non autorizzato rilevati dal Mon, informazioni statistiche di vario genere che potranno risultare utili a chi pubblica o distribuisce i materiali sottoposti a *copyright* ecc.), un modulo Mar (*marker*) che gestisce infine la crittazione-decrittazione dell'intera applicazione o anche solo di alcune sue parti specifiche.
Sostanzialmente, il funzionamento del sistema è il seguente: il contenuto di una determinata opera viene criptato e inserito all'interno di un *file* unitamente alle regole che ne disciplinano l'uso.
Nel momento in cui accede al *file*, l'utente viene indirizzato, attraverso un *link*, al sito del titolare dei diritti sull'opera o ad un *server* mantenuto da un'impresa che offre sistemi di gestione dei diritti digitali e contenente un *database* che registra le licenze relative a ciascun file criptato. A questo punto, l'utente sceglie la licenza che preferisce potendo così, in seguito, accedere al contenuto del *file*, decrittato da un apposito *software* e farne uso secondo le condizioni indicate nella licenza stessa.
Tipicamente le licenze, oltre al corrispettivo, regolano la durata (per quanto tempo è possibile ascoltare un brano o vedere un film, ad esempio), la frequenza dell'accesso (se cioè nell'arco del periodo si può ascoltare un brano solo una volta o un numero indefinito di volte), l'utilizzo (se il contenuto si può copiare salvare archiviare su *Compact Disc*, stampare utilizzare su una periferica portatile) o il trasferimento a terzi (possibile, negato, limitato ad alcuni casi).
I diritti di utilizzazione concessi e la *policy* di utilizzo sono associati ad ogni 'piece of content' in relazione ad ogni singolo utente e comprendono meccanismi di controllo e validazione di ogni singolo accesso, secondo il modello di *business* che si intende adottare: *subscription models*, *pay per view*, promozione, etc.
Generalmente, un sistema di Drm consente anche di effettuare il pagamento del corrispettivo della licenza attraverso la rete Internet e, in alcuni casi, permette la diretta distribuzione delle *royalties* al titolare dei diritti sull'opera.
Ad esempio, Magex.com[534] ha inserito nel proprio portale un sistema di questo tipo: l'utente si registra al sito fornendo alcune informazioni personali ed apre un conto elettronico indicando il numero della propria carta di credito.
A questo punto l'utente può accedere virtualmente a un elenco di fornitori, quali librerie, negozi musicali e negozi di *software,* ed acquistare i prodotti offerti.
Questi vengono poi raccolti nel 'Digibox', "busta digitale", contenente i prodotti acquistati e le regole che ne disciplinano l'utilizzo e il prezzo.
Il prezzo relativo ad ogni acquisto viene automaticamente dedotto dal conto elettronico dell'utente.

[534] In Internet all'indirizzo http://www.magex.com (sito consultato il 15 luglio 2002).

Alcune imprese che producono sistemi di DRM offrono dimostrazioni *on-line*[535] o programmi pilota[536], mentre altre forniscono in Rete dettagliate descrizioni dei loro servizi[537]; molto attiva è, anche, la *InterTrust Technology Corporation*[538].
È anche possibile scaricare, dal sito Web di Microsoft, la versione gratuita del *software Windows Media Rights Manager* e verificarne il funzionamento[539].
È opportuno porre in evidenza che, qualora alla base del sistema adottato vi sia l'uso della sola crittografia, una volta decrittato il contenuto, il *file* in chiaro sarà accessibile a chiunque e, quindi, l'ambiente in cui si renderà possibile decifrare un contenuto digitale dovrà, inevitabilmente, essere un ambiente controllato, privo di una qualsiasi possibilità di trasferire i dati all'esterno.
La fruizione del contenuto deve avvenire quindi in un "tamper resistant" *environment*, un ambiente, cioè, sicuro e protetto.
Si consideri, a riguardo, l'esempio di a2bMusic.com: i brani vengono forniti in forma crittata sulla base di uno degli algoritmi presenti nella libreria di riferimento appositamente sviluppata, la *CryptoLib Security Librar*. Per poterli ascoltare sarà, innanzitutto, necessario procurarsi il relativo *player* e, successivamente, procedere al pagamento dei diritti relativi.
Al momento dell'acquisto viene fornita la speciale 'licenza d'uso' contenente (ancora in forma crittata) la chiave di decrittazione necessaria per la riproduzione di quel dato brano, chiave che solo l'apposito *a2bplayer* sarà in grado di leggere.
Nel momento stesso in cui si richiede a tale programma la riproduzione di un brano, si attiva un particolare *software*, denominato *PolicyMaker*, che controlla che la firma digitale in possesso dell'utente del sistema coincida con quella prevista dalla licenza d'uso: la chiave di decrittazione potrà venire estratta solo se tale controllo risulterà positivo.
Lo stesso *PolicyMaker* si occupa, poi, di interpretare le condizioni d'uso codificate all'interno della licenza e di decidere, in base a queste, se la riproduzione può aver luogo oppure no.

---

535 Si veda, a titolo di esempio, il sito http://www.breakertech.com (sito consultato il 15 luglio 2002).
536 Si veda, a titolo di esempio, il sito http://www.cranberrygrove.com (sito consultato il 15 luglio 2002).
537 Si vedano, a titolo di esempio, i siti http://www.reciprocal.com, http://www.info2clear.com, http://www.magex.com (siti consultati il 15 luglio 2002).
538 *InterTrust Technology Corporation*, società precedentemente nota come EPR, è una società da diversi anni particolarmente impegnata sul fronte di una corretta e adeguata gestione dei diritti di proprietà all'interno dei meccanismi di commercio elettronico, tanto da costituire un apposito centro di ricerca rivolto allo sviluppo di tecnologie di *right management:* lo *Strategic Technology and Architectural Research Laboratory*, noto più semplicemente come STAR *Lab*. *Intertrust* ha creato una piattaforma Drm *general purpose*, consistente in servizi, *tools* e altri *software* generici connessi al Drm, in cui si integrano tecnologie proprietarie appositamente sviluppate e tecnologie *standard* di provata efficacia nella realizzazione di meccanismi effettivamente in grado di gestire *in toto*, e non solo di proteggere, i diritti connessi ai contenuti digitali. Il sito Web è all'indirizzo http://www.intertrust.com (sito consultato il 15 luglio 2002).
539 In Internet all'iindirizzo fttp://www.microsoft.com/windows/windowsmedia/download/ (sito consultato il 15 luglio 2002).

PARTE SESTA

CRITTOGRAFIA E SICUREZZA

Capitolo Ventunesimo

CRITTOGRAFIA E SICUREZZA

SOMMARIO: 1. Introduzione. – 2. Informazione e comunicazione. – 3. Il d.p.r. n. 318 del 1999. – 4. Cifratura dell'informazione ed analisi dei rischi. – 5. Sicurezza in cifratura simmetrica e asimmetrica. – 6. Sicurezza = crittografia? Il progetto *Tempest*. – 7. I *keyboard sniffers*. – 8. Sicurezza e certificazione. – 9. La sicurezza dei sistemi e dei prodotti. – 10. Sicurezza informatica e sicurezza nazionale. – 11. Le funzioni dell'Autorità Nazionale di Sicurezza (ANS) e dell'Ufficio Centrale per la Sicurezza (UCSi).

1. Introduzione.

"La sicurezza assoluta non esiste". Sembra essere, questa, la parola d'ordine degli ultimi anni in materia di applicazioni commerciali connesse ad Internet. Se, da un lato, il sospetto che l'interesse di molti operatori del settore dell'*Information Technology* che offrono servizi di assistenza alle aziende sia proprio quello di alimentare un clima di allarmismo connesso all'uso della Rete, dall'altro, è pur vero che bisogna rivedere il concetto di sicurezza informatica.
Internet nasce e si diffonde come poderoso strumento di diffusione della conoscenza, di condivisione di idee e opinioni; nasce, insomma, come grande mezzo di comunicazione. Non ci si riferisce, con questo, necessariamente, alla comunicazione con la 'c' maiuscola, alla comunicazione di 'alto livello', ma a tutti i tipi di comunicazione, dalle *chat* ai *newsgroup*, ai *software* di condivisione dei *file*. A tutte quelle modalità, in poche parole, che permettono lo scambio e l'incontro tra persone di luoghi e culture diverse. Internet è, fondamentalmente, questo: un *media*, come la televisione o la radio, dove è possibile trovare di tutto e dove tutto, fortunatamente, ha ancora pari dignità. Dove tutto è 'pari ordinato' grazie a quel semplice protocollo di trasmissione, il TCP/IP[540], che tutto e tutti accomuna. La Rete nasce, così, libera, amorfa, tentacolare, disordinata, ma unita dal "linguaggio comune", cioè il suo protocollo di comunicazione.
Su queste basi, come si può parlare di sicurezza? E, soprattutto, perché parlarne?
È evidente che la domanda di sicurezza nasce da un'esigenza ben precisa: la tutela del *business*. È questa la chiave di volta: l'ingresso in Internet del mondo aziendale, realtà nuova e, per certi versi 'estranea' alla concezione originaria

[540] Nel Capitolo seguente verranno trattate più diffusamente le problematiche di sicurezza correlate al protocollo TCP/IP.

della Rete, ha portato al sorgere di una pressante esigenza di sicurezza. L'"obiettivo sicurezza' deve partire da alcune, semplici considerazioni.
La natura di Internet rende enormemente complesso qualunque tentativo di implementazione della sicurezza, sul già accennato presupposto della intrinseca fragilità strutturale della Rete. Ogni strumento utilizzato in tal senso si rivela, strutturalmente, come una sorta di armatura posta a protezione di un corpo estremamente delicato.
La sicurezza è un processo e non un prodotto che richiede risorse *hardware*, *software* e *humanware*. Non è solo attraverso l'utilizzo di strumenti più o meno complessi che si raggiunge.

2. Informazione e comunicazione.

È comprensibile che nell'*Internet business* la sicurezza delle comunicazioni sia d'importanza vitale. I beni 'tradizionali' vengono a perdere progressivamente valore, a favore dell'informazione che assume, sempre più, il ruolo di bene per eccellenza.
Vi sono particolari tipologie di informazioni che nascono per essere diffuse. Il sapere scientifico, per esempio, ha la sua ragion d'essere nella diffusione e nella condivisione. La condivisione di nozioni scientifiche produce cultura, progresso, libertà per i soggetti destinatari e per la società tutta[541]. In età medievale, gli amanuensi ricopiavano con cura certosina i libri dell'antichità classica consapevoli di conservare e trasmettere ai posteri non solo il testo in sé, ma la cultura trasfusa nel testo, sulla quale costruire nuovo sapere.
Vi è, poi, un altro tipo di informazione, il cui valore è, invece, tanto più elevato quanto più esiguo è il numero delle persone che ne sono a conoscenza: è l'informazione industriale o economica. Questo tipo d'informazione assume valore di merce rara e richiesta proprio quando sono in pochi a disporne e quando viene in possesso di soggetti capaci di sfruttarla a pieno.
Risulta, così, evidente come sia *condicio sine qua non* del mantenimento del valore dell'informazione il requisito che solo i destinatari della stessa siano capaci di comprenderla ed interpretarla. In tal senso, si inserisce la necessità di predisporre strumenti idonei alla sicurezza dell'informazione. Strumenti che devono garantire, da un lato, che solo il destinatario riceverà l'informazione e, dall'altro, che, nel caso in cui questo non avvenga, nessuno sarà in grado di comprendere il contenuto del messaggio.
In questo senso, si inserisce il problema della sicurezza, strettamente correlato alle tematiche della crittografia che già sono state affrontate in questo Volume.
Da un lato, 'sicurezza' significherà scelta di strumenti che rendano 'sicuro', per quanto è possibile, il canale di trasmissione dell'informazione: si parlerà, quindi, di *network security*. Dall'altro, 'sicurezza' verrà intesa come protezione dell'informazione inviata sotto forma di messaggio digitale e, in questo caso,

[541] Non sono certo rari i casi in cui l'interesse economico si sia scontrato con la volontà della condivisione. Basti pensare al già visto caso del DeCss.

parleremo di *computer security* riferendoci, in particolare, a quelle operazioni rivolte alla 'messa in sicurezza' del dato.
Alle due tipologie di informazione appena menzionate se ne aggiunge una terza. Si tratta di quelle informazioni che non nascono per essere trasferite o comunicate, ma vengono raccolte per essere gestite. Sono, in particolare, quei dati contenuti nei *database* di aziende telefoniche, bancarie o di strutture pubbliche, quali ospedali o uffici tributari, che riguardano la vita dei dipendenti o dei cittadini fruitori di servizi. Questo tipo di dati risulta sicuramente appetibile per aziende e società di *marketing*, rappresentando uno specchio delle abitudini, dei gusti, dei bisogni di potenziali clienti.
Si distinguono, quindi, due macroscopiche tipologie di dati che devono essere rese invulnerabili da accessi non autorizzati: i dati che devono essere inviati e quelli che devono essere conservati sul posto.
Le *policies* di *computer security* saranno, in ogni caso, finalizzate alla tutela sia dell'informazione di tipo 'statico', cioè conservata e trattata in locale, sia di quella 'dinamica', cioè inviata per via telematica. Questa distinzione risulta, tuttavia, utile per comprendere il perché della scelta di algoritmi di cifratura simmetrici o asimmetrici.
Il rapporto tra tipologie di dati, livello di vulnerabilità degli stessi e strumenti per la sicurezza è stato trasfuso dal Legislatore italiano nel d.p.r. 318/99, recante indicazioni sulle cosiddette "misure minime di sicurezza", che configurano lo *standard* minimo di protezione richiesto nel trattamento di dati personali.
Ai sensi dell'art. 15, 2° comma della Legge 675/96, con Decreto del Presidente della Repubblica sono stati individuati gli *standard* minimi di sicurezza per la protezione dei dati personali.
Il Decreto ha previsto una sorta di tabella in cui sono posti in relazione la tipologia dei dati trattati (comuni o sensibili), il tipo di strumento utilizzato per il trattamento (elettronico o non elettronico) e, nel caso di utilizzo di strumenti elettronici, l'esposizione dell'elaboratore ad accessi esterni.
Il Legislatore ha, quindi, distinto livelli di protezione differenti nel caso in cui l'informazione sia conservata in un "elaboratore isolato" (art. 2, comma 1), un "elaboratore in rete privata" (art. 3, comma 1, lettera *a*) o un "elaboratore in rete pubblica" (art. 3, comma 1, lettera *b*).
Soffermandoci su quest'ultima categoria, che comprende tutti gli elaboratori su cui sono conservati dati personali sensibili o giudiziari e che dispongono di un accesso alla Rete, è evidente come il Legislatore abbia ritenuto indispensabile non solo l'adozione e l'utilizzo di quegli strumenti *hardware* e *software* citati nell'art.4, ma anche la presenza di una consistente componente *humanware*, già accennata.
In questo senso si deve leggere la necessaria presenza del cosiddetto 'Dps', cioè del Documento Programmatico sulla Sicurezza che, ai sensi del primo comma dell'art. 6, "deve essere predisposto e aggiornato con cadenza annuale […] sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi".

Il Legislatore, quindi, ritiene che solo una politica aziendale di formazione, aggiornamento e responsabilizzazione degli operatori possa permettere un maggior grado di "sicurezza" dell'informazione.
Ma allora, cos'è la sicurezza informatica e come viene definita dal Legislatore?
Si noti subito che non esiste una definizione generale di "sicurezza": l'unico riferimento che possiamo trovare è contenuto in una norma UNI 104559 che definisce la sicurezza come "studio, sviluppo ed educazione."

3. Il d.p.r. n. 318 del 1999.

Il Decreto del Presidente della Repubblica 28 luglio 1999, n. 318, pubblicato nella Gazzetta Ufficiale del 14 settembre 1999, serie generale, n. 216, prende il titolo di "Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali a norma dell'articolo 15, comma 2, della legge 31 dicembre 1996, n. 675".
Il punto di partenza di questa impalcatura normativa, come già indicato nel Paragrafo precedente, è l'articolo 15 della Legge 31 dicembre 1996, n. 675, sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.
Ai sensi dell'articolo 15, comma 2, della Legge 31 dicembre 1996, n. 675, occorre infatti individuare, in via preventiva, le misure minime di sicurezza per i dati personali oggetto di trattamento, al fine di assicurare il funzionamento delle misure sanzionatorie penali previste dall'articolo 36 della medesima Legge.
Il Capo I del Decreto è riservato ai principi generali, e l'art. 1 contiene alcune definizioni che si applicano ai fini del Regolamento.
In particolare, si intendono per "misure minime" il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza, previste nel Regolamento, che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti dall'art. 15, comma 1, della legge; per "strumenti": i mezzi elettronici o comunque automatizzati con cui si effettua il trattamento; per "amministratori di sistema" i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione.
Il Capo II del Decreto si occupa, invece, del trattamento dei dati personali effettuato con strumenti elettronici o comunque automatizzati, e nella Sezione I affronta il problema del trattamento dei dati personali effettuato mediante elaboratori non accessibili da altri elaboratori o terminali.
In particolare, l'art. 2, "Individuazione degli incaricati", dispone che, salvo quanto previsto dall'articolo 8, se il trattamento dei dati personali è effettuato per fini diversi da quelli di cui all'articolo 3 della Legge mediante elaboratori non accessibili da altri elaboratori o terminali, devono essere adottate, anteriormente all'inizio del trattamento, le seguenti misure: a) prevedere una parola chiave per l'accesso ai dati, fornirla agli incaricati del trattamento e, ove tecnicamente possibile in relazione alle caratteristiche dell'elaboratore, consentirne l'autonoma sostituzione, previa comunicazione ai soggetti preposti ai sensi della lettera b); b) individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti

alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.
La seconda Sezione del Decreto affronta il problema del trattamento dei dati personali effettuato mediante elaboratori accessibili in rete.
L'art. 3, "Classificazione", prevede che gli elaboratori accessibili in rete impiegati nel trattamento dei dati personali siano distinti in: a) elaboratori accessibili da altri elaboratori solo attraverso reti non disponibili al pubblico; b) elaboratori accessibili mediante una rete di telecomunicazioni disponibili al pubblico.
L' Art. 4, "Codici identificativi e protezione degli elaboratori", avverte che, nel caso di trattamenti effettuati con gli elaboratori di cui all'articolo 3, oltre a quanto previsto dall'articolo 2 devono essere adottate le seguenti misure: a) a ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse; b) i codici identificativi personali devono essere assegnati e gestiti in modo che ne sia prevista la disattivazione in caso di perdita della qualità che consentiva l'accesso all'elaboratore o di mancato utilizzo dei medesimi per un periodo superiore ai sei mesi; c) gli elaboratori devono essere protetti contro il rischio di intrusione ad opera di programmi di cui all'articolo 615-*quinquies* del codice penale, mediante idonei programmi, la cui efficacia ed aggiornamento sono verificati con cadenza almeno semestrale. Le disposizioni di cui al comma 1, lettere a) e b), non si applicano ai trattamenti dei dati personali di cui è consentita la diffusione.
L' Art. 5, "Accesso ai dati particolari", dispone che per il trattamento dei dati di cui agli articoli 22 e 24 della Legge effettuato ai sensi dell'articolo 3, l'accesso per effettuare le operazioni di trattamento è determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati del trattamento o della manutenzione. Se il trattamento è effettuato ai sensi dell'articolo 3, comma 1, lettera b), sono oggetto di autorizzazione anche gli strumenti che possono essere utilizzati per l'interconnessione mediante reti disponibili al pubblico. L'autorizzazione, se riferita agli strumenti, deve individuare i singoli elaboratori attraverso i quali è possibile accedere per effettuare operazioni di trattamento.
Le autorizzazioni all'accesso sono rilasciate e revocate dal titolare e, se designato, dal responsabile. Periodicamente, e comunque almeno una volta l'anno, è verificata la sussistenza delle condizioni per la loro conservazione.
L'autorizzazione all'accesso deve poi essere limitata ai soli dati la cui conoscenza è necessaria e sufficiente per lo svolgimento delle operazioni di trattamento o di manutenzione. La validità delle richieste di accesso ai dati personali è verificata prima di consentire l'accesso stesso. Non è consentita l'utilizzazione di un medesimo codice identificativo personale per accedere contemporaneamente alla stessa applicazione da diverse stazioni di lavoro.
L'art. 6, contenente le disposizioni sul cosiddetto "Documento programmatico sulla sicurezza", dispone che nel caso di trattamento dei dati di cui agli articoli

22 e 24 della legge effettuato mediante gli elaboratori indicati nell'articolo 3, comma 1, lettera b), dev'essere predisposto e aggiornato, con cadenza annuale, un documento programmatico sulla sicurezza dei dati per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi: a) i criteri tecnici e organizzativi per la protezione delle aree e dei locali interessati dalle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi; b) i criteri e le procedure per assicurare l'integrità dei dati; c) i criteri e le procedure per la sicurezza delle trasmissioni dei dati, ivi compresi quelli per le restrizioni di accesso per via telematica; d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire danni.
L'efficacia delle misure di sicurezza adottate ai sensi del comma 1 dev'essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.
L'Art. 7, intitolato "Reimpiego dei supporti di memorizzazione", nota come nel caso di trattamento dei dati di cui agli articoli 22 e 24 della legge effettuato con gli strumenti di cui all'articolo 3, i supporti già utilizzati per il trattamento possano essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.
La Sezione III riguarda, invece, il trattamento dei dati personali effettuato per fini esclusivamente personali.
In questa Sezione l'articolo 8, dal titolo "Parola chiave", stabilisce che ai sensi dell'articolo 3 della legge, il trattamento per fini esclusivamente personali dei dati di cui agli articoli 22 e 24 della legge, effettuato con elaboratori stabilmente accessibili da altri elaboratori, è soggetto solo all'obbligo di proteggere l'accesso ai dati o al sistema mediante l'utilizzo di una parola chiave, qualora i dati siano organizzati in banche di dati.
Il Capo III del Decreto riguarda il Trattamento dei dati personali con strumenti diversi da quelli elettronici o comunque automatizzati.
In questo caso, l'articolo 9, "Trattamento dei dati personali", dispone che nel caso di trattamento di dati personali per fini diversi da quelli dell'articolo 3 della legge, effettuato con strumenti diversi da quelli previsti dal capo II, sono osservate le seguenti modalità: a) nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni ai sensi degli articoli 8, comma 5, e 19 della legge, il titolare o, se designato, il responsabile devono prescrivere che gli incaricati abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati; b) gli atti e i documenti contenenti i dati devono essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, devono essere da questi ultimi conservati e restituiti al termine delle operazioni affidate.
Nel caso invece di trattamento di dati di cui agli articoli 22 e 24 della legge, oltre a quanto previsto nel comma 1, devono essere osservate le seguenti modalità: a) se affidati agli incaricati del trattamento, gli atti e i documenti contenenti i dati sono conservati, fino alla restituzione, in contenitori muniti di serratura; b) l'accesso agli archivi deve essere controllato e devono essere

identificati e registrati i soggetti che vi vengono ammessi dopo l'orario di chiusura degli archivi stessi.
In conclusione, l' articolo 10, "Conservazione della documentazione relativa al trattamento", nota come i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali di cui agli articoli 22 e 24 della legge, debbano essere conservati e custoditi con le modalità di cui all'articolo 9.

4. Cifratura dell'informazione e analisi dei rischi.

Come già visto[542], la cifratura delle informazioni contenute in messaggi non è un fenomeno recente. Criptare è una parola che viene dal greco "cryptos" – nascosto -; e ancor prima, in età Egizia, si usavano strumenti di cifratura dei messaggi. È noto ad esempio che lungo le vie consolari che percorrevano l'impero si snodava un sistema di torri che, attraverso un raffinato apparato di segnalazioni luminose, riverberava il volere del *Princeps* alle legioni dislocate nel limite estremo dei confini imperiali. Dell'esistenza di tale apparato ci riporta notizia anche un bassorilievo sulla colonna traiana[543], che raffigura una torre cinta da una palizzata, con in cima una fiaccola accesa.
Si immagini, ora, come dovesse funzionare tale sistema: le legioni poste a guardia dei confini, al verificarsi di pericolosi movimenti di truppe barbare, inviavano segnali luminosi alle torri più vicine e, con il classico sistema del 'passa parola', si riusciva ad informare il quartier generale più vicino che inviava i rinforzi dove fosse necessario.
Questa comunicazione che impiegava un codice basato su un computo di fiaccole, alcune delle quali accese ed altre spente, non era, ovviamente, esente da rischi. Infatti, le avversità atmosferiche, la pioggia, la neve, il vento potevano sia spegnere una torcia che doveva restare accesa, sia accenderne una che, al contrario, doveva essere spenta.
In entrambi i casi, la torre ricevente avrebbe percepito e registrato una comunicazione errata e gli effetti di ciò sarebbero stati facilmente immaginabili.
Questo tipo di errore, legato a cause accidentali, si può definire *non intenzionale*.
C'era, però, un'altra tipologia di errore che poteva viziare le comunicazioni militari: quella *intenzionale*.
I barbari, intuite le potenzialità del sistema di comunicazione romano, potevano sfruttarlo a loro vantaggio. Potevano intercettare il messaggio, per poi evitare i passi rinforzati e indirizzare il loro attacco verso un accesso lasciato sguarnito. In maniera ancora più subdola, potevano impossessarsi di una torre e, inviando un messaggio alterato in modo che le truppe romane avessero reputato la situazione sotto controllo, sarebbero riusciti a violare i confini imperiali.

---

542 In particolare nei Capitoli I e II del presente Volume.
543 Cfr. O. BRUGIA, *Vademecum per stare lontani da vandali, spioni e manigoldi*, in *Telèma*, in Internet all'indirizzo http://www.telema.it (sito Internet visitato il 20 luglio 2002).

È possibile tracciare un parallelo tra il sistema di comunicazione romano e i nostri? Certamente sì, per lo meno dal punto di vista della cosiddetta "analisi del rischio".
È agevole assimilare il sistema della torcia accesa o spenta alla comunicazione digitale su base binaria. L'acceso/spento si traduce, oggi, in 0 e 1, nel linguaggio degli elaboratori elettronici. L'errore non intenzionale altro non è che il disturbo di segnale, quella serie di impulsi elettromagnetici spurii cui le comunicazioni, soprattutto se intercorrono tra grandi distanze, sono spesso soggette. Tali disturbi possono portare o allo smorzamento del segnale inviato (errore omissivo), trasformando l'1 in 0 o viceversa, o all'innalzamento del segnale (errore immissivo). Le indebite immissioni nella segretezza dell'informazione derivano, come sempre, dall'ambito militare o economico. Solo strumenti di validazione permettono, per esempio, alle banche di evitare che il cliente A si finga B e ordini un trasferimento di somme dal conto di B a quello di A. Così come gli strumenti di validazione impediscono che l'operazione finanziaria ordinata oggi da A venga ripudiata domani perché si è rivelata fallimentare.
Quali contromisure adottare allora?
Una possibile è quella offerta dal sistema di codifica a correzione dell'errore. Si supponga che, per prevenire gli errori di tramissione, ogni messaggio fosse ripetuto tre volte, che 4 era il numero di fiaccole disponibili e 1110 (accese le prime tre fiaccole e spenta la quarta) la combinazione da trasmettere.
Si ipotizzi, poi, che: nella prima esposizione la pioggia spenga la terza fiaccola, con la conseguenza che la torre ricevente vede la combinazione errata 1100; la seconda volta si spenga la prima fiaccola (0110); la terza volta, la seconda fiaccola (1010). Poiché le fiaccole accese sono due contro una sia in prima, sia in seconda, sia in terza posizione, mentre in quarta 'vincono' quelle spente per 3 a 0, la torre ricevente stima, basandosi sulle suddette maggioranze, che la combinazione originaria sia 1110, e indovina, malgrado l'elevata percentuale di errori (1 su 4, per ogni 'fiaccolata').
Come si è arrivati a questa sorprendente correzione dell'errore? Con la triplicazione dei segnali che occorre trasmettere per inoltrare ogni singola combinazione; a prezzo, cioè, dell'introduzione di quella che nell'odierno linguaggio tecnico si chiama *ridondanza*.
Ma esistono metodi più rapidi e meno dispendiosi per porre rimedio all'esistenza dell'errore?
Nel 1948, Claude Elwood Shannon[544], il fondatore della teoria dell'informazione, enunciò un teorema sull'esistenza di codici capaci di correggere una quantità sorprendentemente elevata di errori a prezzo d'una ridondanza sorprendentemente piccola. Il metodo utilizzato fu quello del cosiddetto *codifica a controllo della parità*.
Si torni all'esempio delle fiaccole e si assuma che, a fianco delle quattro che servono all'invio del messaggio, le fiaccole informative, se ne aggiunge una quinta, *di parità*, che sarà accesa o spenta in modo tale che il numero complessivo delle fiaccole accese sia sempre pari.

---

544 Cfr. C.E. SHANNON, *A mathematical theory of communication*, in *Bell System Technical Journal*, vol. 27, Luglio 1948, p. 379-425, Ottobre 1948, p. 623-656.

Quindi, se una qualunque delle fiaccole del messaggio si spenga accidentalmente, la torre ricevente percepirebbe un messaggio anomalo e chiederebbe di ripetere la trasmissione.
Questo sistema lo troviamo trasfuso oggi nella notissima e già vista[545] funzione di Ash. Assieme al messaggio codificato viene infatti elaborato e inviato un codice che permette di effettuare una comparazione con il codice annesso al messaggio ricevuto. Nel caso in cui i due codici fossero discrepanti potremo sicuramente affermare che durante la trasmissione si verificata un'indebita modifica effettuata da parte di terzi.

5. Sicurezza in cifratura simmetrica e asimmetrica.

Veniamo alla già vista fondamentale distinzione alla base della crittografia moderna. Per algoritmo di cifratura simmetrica (o a chiave segreta) si intende quel metodo di cifratura, usato soprattutto in passato, basato sull'esistenza di un'unica chiave segreta utilizzata sia per cifrare che per decifrare i dati.
Questi algoritmi, a loro volta, si dividono in *cifrari a blocco* e *cifrari a flusso*. I primi sono in grado di cifrare un solo *bit* di testo chiaro alla volta, mentre i secondi prendono un certo numero di *bit* (tipicamente 64 *bit* nei moderni cifrari) e li cifrano come una singola unità.
I sistemi a chiave simmetrica vengono oggi utilizzati per proteggere l'informazione da visione non autorizzata; per garantire che l'informazione non venga alterata e che il messaggio arrivi esattamente come è stato spedito; per prevenire la dissimulazione degli utenti consentendo, al vero mittente, di includere nel messaggio informazioni che lo identifichino con certezza.
Tuttavia tali sistemi presentano insormontabili punti deboli: 1) i due corrispondenti devono essere in possesso della stessa chiave che deve essere consegnata per via telematica ad entrambi prima dell'inizio della comunicazione. Spostandosi così il problema della sicurezza dal messaggio alla chiave, è ben possibile che questa, venendo intercettata da terzi, renda le comunicazioni seguenti insicure; 2) poiché gli utenti condividono chiavi segrete, non è possibile, o è altamente problematico, provare a un terzo che un certo messaggio è stato effettivamente generato da uno dei due utenti.
Questi problemi sono risolti dalla crittografia a chiave pubblica.
Le tecniche di cifratura asimmetriche utilizzano coppie di chiavi complementari invece di una sola chiave segreta: ogni singolo utente possiede una coppia univoca di chiavi complementari. Di esse, una è una chiave pubblica, nel senso che può, o meglio, *deve* essere conosciuta da terzi, ed è usata per cifrare il messaggio, mentre l'altra è una chiave privata e, come tale, sarà gelosamente custodita dal proprietario. Le due chiavi sono complementari, cioè un messaggio cifrato da una delle due può essere decifrato solo e soltanto dall'altra.

[545] Cfr. le nozioni di base contenute nel Capitolo II.

In pratica, se si vuole spedire un messaggio a una certa persona, si cifra quel messaggio utilizzando la sua chiave pubblica, e si è sicuri che soltanto quella persona potrà decifrarlo con la propria chiave privata, dato che la chiave pubblica precedentemente utilizzata per cifrare non è assolutamente in grado di decifrare.
Gli algoritmi asimmetrici possono essere utilizzati anche per generare le cosidette 'firme elettroniche'. Esse sfruttano delle elaborazioni algoritmiche particolari (come la cosiddetta funzione di Hash) grazie alle quali è possibile verificare l'autenticità del messaggio.
Con questa tecnica il messaggio originale, la firma e la coppia di chiavi dell'utente risultano strettamente ed inscindibilmente legate; la modifica di una qualsiasi delle componenti comporta il fallimento della validazione della firma.
Il vantaggio principale che la crittografia asimmetrica offre sta, in fin dei conti, nella facilità di gestione delle chiavi; non occorre, infatti, scambiarsi segretamente chiavi di cifratura con il rischio che esse possano essere intercettate, in quanto basta comunicare, o far pubblicare, il proprio numero di chiave pubblica per essere certi che nessun altro sarà in grado di leggere il messaggio inviatoci.
Tuttavia gli algoritmi asimmetrici non sono in grado di risolvere completamente i problemi di sicurezza. Vi sono, in realtà, vari motivi che fanno propendere per un uso ibrido e combinato dei sistemi simmetrici e asimmetrici: se si devono crittare grandi volumi di dati, come per esempio nel caso di dati 'statici', cioè che non devono essere trasferiti, la crittografia asimmetrica impiegherebbe, per tale operazione, un tempo di gran lunga maggiore rispetto a quello impiegato da un algoritmo simmetrico, ragion per cui la scelta dei metodi a chiave unica è quasi obbligatoria; quindi un crittosistema a chiave segreta (simmetrica) è quello più consono, sia perchè è più veloce, sia perchè non esiste alcun problema connesso con lo scambio e la validazione delle chiavi.

6. Sicurezza = crittografia? Il progetto *Tempest*.

Non sempre sicurezza è sinonimo di crittografia Pensiamo al caso in cui, completata la redazione di un documento nella nostra postazione in azienda, salviamo il *file* e per evitare che occhi indiscreti ne prendano visione, lo cifriamo. Ebbene, potrebbe già esser troppo tardi. Infatti, il nostro documento, di importanza strategica per le future scelte dell'azienda, potrebbe essere già stato copiato prima che noi avviamo la procedura di cifratura.
Come? Attraverso la ricezione delle onde elettromagnetiche emesse dal nostro *Personal Computer*.
Ogni apparecchio elettrico ed elettronico, infatti, emette una grande quantità di onde elettromagnetiche la cui portata è direttamente proporzionale alla potenza dell'apparecchio stesso. Un computer, per esempio emette onde per un raggio di circa 700 metri.

Le onde elettromagnetiche, se captate con una semplice antenna, registrate e analizzate con un apparecchio chiamato *scanner*, permettono la ricostruzione dei documenti presenti nel disco fisso del computer.
In tal maniera, per la violazione del contenuto di una macchina non sarà necessario avere un accesso 'fisico' alla stessa, né tantomeno che questa sia collegata in Rete per poter sferrare un attacco per via telematica.
È evidente che queste considerazioni hanno posto in grave pericolo la sicurezza dei dati riservati contenuti negli archivi delle agenzie governative.
Per questo motivo quando, nel 1950, il Governo degli Stati Uniti d'America scoprì che l'emissione di onde elettromagnetiche poteva pregiudicare la sicurezza delle proprie strutture, avviò il cosiddetto progetto *Tempest*.
Non ci sono conferme riguardo al significato del nome *Tempest*, che molti ritengono essere un acronimo (*Transient Electromagnetic Pulse Emanation Standard)*; quello che è certo è che già al suo avvio si intuiva che si sarebbe trattato di un progetto che avrebbe avuto applicazioni industriali dal considerevole valore.
Nel 1970 lo *standard* Tempest fu revisionato nel documento conosciuto con il nome di *National Security Information Memorandum 5100* o *NACSIM 5100*.
L'attuale *standard* è stato riconosciuto il 16 gennaio 1981 nel documento riservato NACSIM 5100A.
L'organo preposto al controllo dello standard *Tempest* è, dal 1984, la *National Security Agency*, che si occupa di informare le varie agenzie di stato sui dispositivi di sicurezza da installare nelle proprie sedi.
La preoccupazione principale nell'utilizzo delle tecniche legate al monitoraggio delle onde elettromagnetiche è incentrata sui monitor dei computer. È proprio il fatto che si riesca a ricostruire ciò che appare sul video di un computer in cui sono memorizzati documenti riservati che desta le maggiori preoccupazioni della *National Security Agency*.
Resta il fatto che, nella maggior parte dei casi, la tecnologia per riuscire a captare segnali elettromagnetici e registrarli è ormai molto diffusa e, tutto sommato, a buon mercato. Anche se gli apparati, già confezionati, per questo tipo di intercettazioni sono abbastanza costosi, nel circuito *hacker* sono circolati gli schemi tecnici per la costruzione di strumenti artigianali che consentono di ottenere risultati sicuramente apprezzabili. Uno *scanner* multi-frequenza, una buona antenna e un sistema televisivo munito di videoregistratore VCR sono sufficienti a comporre un buon impianto per l'intercettazione e la registrazione dei segnali.
La sicurezza offerta dal sistema *Tempest* contro la diffusione di onde elettromagnetiche è basata su protezioni strutturali dei circuiti elettrici tramite le cosiddette 'celle di Faraday'. Si tratta, in pratica, di una schermatura effettuata con materiali isolanti, volta a prevenire qualsiasi diffusione di onde.
Ad un primo progetto di schermatura dei singoli computer, ne subentrò quasi subito un altro, assai meno dispendioso.
Il moltiplicarsi del numero di *Personal Computer* presenti all'interno degli edifici fece ritenere assai più economico schermare questi ultimi, attraverso innesti di materiali isolanti sui muri perimetrali, in modo da realizzare una sorta di ambiente sterile dal quale nessuna informazione via etere è in grado di fuoriuscire.

Nel mondo industriale *Tempest* è stato implementato solo in rarissimi casi: ad esempio, l'IBM ha prodotto un *case* speciale per *Personal Computer* con un costo aggiuntivo di circa 35 dollari, chiamato EMR XT SYSTEM UNIT, modello 4455 1.
Ma quando è davvero utile questo tipo di protezione? Certamente non a casa, dove esistono sicuramente ben altri metodi a disposizione di terze persone per sottrarre documenti da un *Personal Computer*. Basterebbe, per esempio, copiare i *file* mentre si è connessi in Internet, o entrare fisicamente in casa e sottrarli.
Studi indipendenti hanno comunque dimostrato che lo *standard Tempest* può essere implementato mantenendo i costi ad un livello ragionevole e permettendone così la diffusione anche tra le piccole aziende. Un esempio è costituito dal caso della schermatura della CPU nella quale viaggiano tutte le istruzioni contenute nel *Personal Computer*.
Un altro esempio molto interessante di applicazioni alternative al *Tempest* è stato dimostrato dal Prof. Erhart Moller dell'Università di Aachen in Germania, che ha sperimentato un sistema volto semplicemente a confondere i segnali emessi, senza limitarsi a bloccarli.

7. I k*eyboard sniffers.*

Ma quali altri modi esistono per violare la sicurezza dei dati contenuti in un *Personal Computer*? Come è possibile rendere nulle le operazione di cifratura dei *file* più importanti?
Uno degli strumenti più subdoli è senz'altro costituito dai cosiddetti *keybord sniffers*. Si tratta di piccoli *software* che, istallati sulla macchina dell'ignaro utente, permettono la registrazione su *file* di tutte le singole pressioni effettuate sulla tastiera del computer. In tal maniera, l'analisi del *file* in cui sono stati registrati queste informazioni permetterà di conoscere ogni dato presente nel sistema comprese, ovviamente, le *password*. L'intero processo di registrazione dei singoli tasti premuti in ogni *file* viene, ovviamente, eseguito in *background* e con un impiego minimo di risorse.
Il più famoso di questi programmi che gira in ambiente Windows è sicuramente *KeyLogger*, realizzato dalla società americana Amecisco, e distribuito su licenza *shareware*.
È disponibile in due versioni, *KeyLogger97* e *Key- Logger Stealth*, e riesce a registrare la pressione dei tasti utilizzando diverse opzioni per l'intercettazione e registrando tutte le informazioni raccolte su un *file* prestabilito opportunamente cifrato attraverso una tecnica di *scrambling* (ossia di confusione dei caratteri).
Una volta installato, il programma rimane nascosto e non è possibile individuarlo con le classiche tecniche di ricerca dei sistemi Windows.
Per rendersi invisibile, *KeyLogger* utilizza la tecnica dei *virtual device driver*, ponendosi in esecuzione e in continuo ascolto della tastiera tra le applicazioni e la GUI (*Graphical User Interface*) di Windows.

L'attivazione avviene in maniera pressoché automatica: basta riavviare il sistema o eseguire direttamente l'applicazione nella *directory* prescelta per l'installazione (il *file* si chiama "Ik.exe"). Una volta entrato in esecuzione, il programma intercetta tutti i tasti premuti sulla tastiera e registrati in un *file* cifrato chiamato 'Ik.dat'. Per leggere il contenuto, sarà sufficiente eseguire il programma 'dat2txt.exe', presente nella stessa *directory* di *KeyLogger*.
Eseguendo questo programma, il *file* 'Ik.dat' verrà decifrato in un semplice *file* di testo (dal nome 'Ik.txt'), leggibile attraverso un comune *editor* (come il Blocco Note di Windows).
L'utente può, in verità, accorgersi del processo non autorizzato in corso sulla sua macchina. Basta verificare col *Task manager* di Windows l'esistenza della riga 'lk' e terminare l'operazione. Il problema è che al successivo *reboot* della macchina il programma andrà nuovamente in esecuzione.

8. Sicurezza e certificazione.

A fronte di tale, desolante quadro, negli ultimi anni si è parlato sempre più spesso del bisogno di 'certificare' la sicurezza dei sistemi informativi presenti nelle aziende e nelle amministrazioni pubbliche.
La necessità di prevedere rigidi protocolli per la certificazione della sicurezza, analoghi, per certi versi, a quelli per la certificazione della qualità dei processi produttivi, sembra aprire le porte ad un nuovo *business*, quello che farà distinguere le aziende pubbliche o private in 'sicure' o 'non sicure'.
La consapevolezza dell'importanza di proteggere le informazioni possedute ha fatto sì che la certificazione, come il bollino di qualità, sia diventato una sorta di riconoscimento per quelle aziende, che considerano la sicurezza affare assai serio.
Il termine 'certificazione' è utilizzato per indicare la verifica e l'attestazione, condotta da enti terzi soggetti indipendenti e qualificati, della conformità di un prodotto, un processo o un servizio ai requisiti previsti da uno *standard* o da una norma di riferimento.
Per quanto riguarda le certificazioni di sicurezza, esistono oggi *standard* e norme di riferimento sia per l'intero sistema di governo della sicurezza dell'informazione messo in atto da un'azienda (intendendo, con questa espressione, quell'insieme di regole, procedure e misure di protezione di tipo fisico, tecnico e relativo al personale, definite, attuate e mantenute dall'azienda per la salvaguardia dell'informazione nel suo complesso, qualunque forma essa assuma) sia per il settore specifico della sicurezza dei sistemi e dei prodotti informatici.
L'approccio emergente per la certificazione del sistema aziendale di governo della sicurezza è definito dallo *standard* britannico *Bs7799 (Information security management)* recentemente recepito come *standard* internazionale dall'ISO/IEC (*International Organization for Standardization/International Electrotechnical Commission*).

Con riferimento alla certificazione dei sistemi e dei prodotti informatici, invece, è oggi in uso la raccolta di criteri di valutazione europei ITSEC (*Information technology security evaluation criteria*) alla quale, dal giugno del 1999, si è affiancato lo standard ISO/IEC-Is15408 (*Common criteria for information technology security evaluation).*

È ovvio che l'utilità di una certificazione è tanto maggiore quanto maggiore sia l'ambito in cui è riconosciuta.

Nell'ambito dello schema di certificazione sono cinque i ruoli fondamentali:

1) il gestore dello schema. È colui che stabilisce quali sono gli *standard* da rispettare. Il gestore si occupa di avviare operazioni di mutuo riconoscimento con i gestori di schemi analoghi in altri Paesi.

2) L'ente accreditatore. Fornisce l'accreditamento iniziale dei certificatori e dei laboratori di verifica, e controlla circa il mantenimento dei requisiti da parte di tali organismi

3) Il certificatore. Si occupa della verifica di applicazione dello schema e rilascia, sulla base delle relazioni di ispettori e laboratori, il certificato.

4) Gli ispettori e i laboratori. Sono il braccio operativo dei certificatori.

5) Il soggetto committente della certificazione.

È comprensibile che anche l'accreditamento dei certificatori, dei laboratori di valutazione o degli ispettori, deve avvenire in base a criteri di riconosciuta validità.

In Europa, la competenza e l'indipendenza dei suddetti organismi o degli ispettori viene verificata secondo parametri definiti nelle norme della serie En45000.

Con riferimento all'accreditamento dei certificatori dei sistemi aziendali di governo della sicurezza esistono, però delle norme più specifiche.

Nel febbraio del 2000, la *European cooperation for accreditation* (Ea) ha, infatti, pubblicato, il documento Ea7/03, *Guidelines for the accreditation of bodies operating certification/Registration of information security management systems*.

In Italia operano ben tre organismi di accreditamento che godono di riconoscimento a livello europeo: il *Sinal* (per l'accreditamento dei laboratori di prova), il *Sincert* (per l'accreditamento degli organismi di certificazione e di ispezione) e il *Sit* (per l'accreditamento dei laboratori di taratura).

Nessuno dei tre organismi ha, attualmente, un ruolo nel settore delle certificazioni di sicurezza.

Lo *standard* britannico Bs7799 ha, rispetto agli altri modelli analoghi, un profondo vantaggio: considera la sicurezza informatica un processo nel quale la componente organizzativa delle risorse umane ha un enorme rilievo.

Le certificazioni Bs7799 sono, di conseguenza, uno strumento attraverso il quale un'organizzazione può dimostrare di essere capace di tutelare in modo globale il proprio patrimonio informativo (o quello di terzi a lei affidato).

L'avvio dei lavori per la produzione dello *standard* risale agli inizi degli anni '90, quando il DTI (*Department of Trade and Industry*) britannico istituì un gruppo di lavoro finalizzato a fornire alle aziende una guida per il governo della sicurezza del loro patrimonio informativo.

Il gruppo pubblicò, nel 1993, una raccolta di *best practice* (intitolata *Code of practice for information security management*) che costituì la base per lo *standard* vero e

proprio pubblicato dal BsiI (*British standard institution*) nel 1995. Nel 1998 venne aggiunta una seconda parte allo *standard* (intitolata *Specification for information security mangement systems*). Le due parti furono, poi, sottoposte a revisione, che si concluse con la pubblicazione dell'intero lavoro nel 1999.
Il Bs7799, nato come *standard* nazionale, suscitò subito, un grosso interesse anche al di fuori della Gran Bretagna, tanto che paesi come Olanda e Svezia lo usarono come base di propri schemi di certificazione.
Nell'autunno del 1999 la Gran Bretagna propose all'ISO/IEC l'adozione dello standard Bs7799 affinché venisse approvato come *standard* internazionale.
Alla fine del 2000 lo *standard* Bs7799 è divenuta lo *standard* internazionale Iso/Iec Is177991.
Lo *standard* si basa intorno ai due concetti fondamentali di *politica di sicurezza* e di *sistema di governo della sicurezza* (di cui la prima costituisce uno degli aspetti) secondo un approccio simile a quello degli *standard* della serie Iso9000 per la certificazione di qualità di un'azienda.
I concetti di *politica di qualità* e di *sistema di gestione della qualità* sui quali tale serie si basa, sono sostituiti da quelli di *politica di sicurezza dell'informazione* e di *sistema di governo della sicurezza dell'informazione* o Isms (*Information security management system*).
La *politica di sicurezza* è la specificazione ad alto livello degli obiettivi di sicurezza che l'organizzazione si propone di conseguire.
L'Isms, invece, rappresenta quel complesso di regole, protocolli e misure di protezione di tipo fisico, tecnico e relativo al personale definite, attuate dall'organizzazione per assicurare nel tempo il soddisfacimento della politica di sicurezza.
Lo standard prevede un insieme di ben 127 controlli raggruppati nelle 10 categorie: 1) politica della sicurezza; 2) organizzazione della sicurezza; 3) classificazione dei beni; 4) aspetti della sicurezza relativi al personale; 5) sicurezza fisica e ambientale; 6) gestione delle comunicazioni e dell'operatività; 7) controlli di accesso; 8) sviluppo e mantenimento dei sistemi di trattamento dell'informazione; 9) continuità delle attività aziendali (in presenza di guasti o disastri); 10) rispetto delle leggi e delle normative procedurali e tecniche interne.
Non sempre, però, è necessario attuare tutti i controlli. La decisione sul numero e la tipologia di controlli da adottare è valutata attraverso il meccanismo dell'analisi e gestione del rischio. Una volta, però, adottati, questi controlli vengono a comporre un regolamento interno che l'azienda si impone di rispettare e far rispettare ai propri dipendenti.
La certificazione Bs7799 ha riscosso particolare successo tra le aziende che trattano informazioni critiche o per conto di terzi come, ad esempio, quelle operanti nel settore finanziario, sanitario o in quello dei servizi di *data hosting, web hosting, e-commerce hosting*.
Le certificazioni avvengono a seguito di una verifica iniziale sul campo per assicurare che quanto stabilito dall'Isms sia stato efficacemente e correttamente realizzato. La durata del processo dipende dalle dimensioni dell'azienda ma, in genere, si conclude in alcune settimane. Il mantenimento del certificato

richiede visite ispettive periodiche ogni sei mesi e la ripetizione completa delle verifiche una volta ogni tre anni.
La certificazione Bs7799 è maggiormente diffusa in Gran Bretagna dove operano ben quattro certificatori.
In Italia, attualmente non è disponibile uno schema di certificazione basato sullo *standard* ISO/IEC Is17799, ma si può ricorrere ad un certificatore accredidato nell'ambito dello schema inglese.
Vi sono, poi, varie società che offrono una consulenza - che potremmo definire 'informale' - sull'adeguatezza del sistema di governo della sicurezza agli *standard* previsti da ISO/IEC Is17799.

9. La sicurezza dei sistemi e dei prodotti.

A fianco della sicurezza nella gestione dei processi, è necessario che l'azienda si doti di apparecchiature *hardware* e *software* sicure.
Sono stati, così, previsti dei meccanismi di certificazione della sicurezza dei prodotti informatici.
Una prima raccolta di criteri per la certificazione della sicurezza informatica relativa ai prodotti è contenuta nel TCSEC (*Trusted computer security evaluation criteria*), pubblicato nel 1985 negli Stati Uniti d'America. Si trattava dei cosiddetti *Orange book*, dal colore della copertina.
I criteri TCSEC furono sviluppati in ambito militare come strumento per la certificazione dei sistemi operativi da utilizzare in elaboratori elettronici dedicati ad applicazioni critiche dal punto di vista della sicurezza.
La risposta europea fu rappresentata dai criteri ITSEC (*Information technology security evaluation criteria*), sviluppati nel 1991, grazie a uno sforzo congiunto della Gran Bretagna, della Germania, della Francia e dell'Olanda e successivamente riconosciuti da tutti i Paesi dell'Unione Europea.
I criteri Europei sono, rispetto ai TCSEC, maggiormente orientati alle necessità del mondo commerciale, e sono utilizzabili anche in settori diversi da quello puramente informatico, ad esempio in quello delle telecomunicazioni o delle *smart-card*.
I criteri TCSEC e i criteri ITSEC godono di un certo riconoscimento internazionale anche se sono prevalentemente utilizzati negli Stati Uniti d'America, i primi, e in Europa, i secondi.
Dal giugno del 1999 è disponibile, inoltre, lo *standard* internazionale ISO/IEC Is15408 (più noto come *Common criteria*).
La storia di questo *standard* è travagliata. L'ISO/IEC avviò lo sviluppo di una raccolta di criteri di valutazione *standard* nel 1990. Inizialmente l'idea era quella di recepire i criteri ITSEC sottoponendoli soltanto a una revisione formale; Stati Uniti d'America e Canada si opposero a tale scelta che spostava di fatto il baricentro del *security business* dal Nuovo al Vecchio continente.
Si arrivò, allora, ad un compromesso istituendo un gruppo di lavoro esterno all'ISO/IEC, finalizzato alla definizione di una raccolta di criteri, detti *Common criteria* (Cc), capaci di conciliare le esigenze europee e quelle nordamericane.

La definizione dei Cc richiese circa sei anni di lavoro, portato avanti da tale gruppo in collaborazione con gli esperti dell'ISO/IEC, tanto che si arrivò a parametri molto simili a quelli dell'ISO/IEC. Scopo della certificazione dei Cc è quella di verificare la rispondenza del prodotto It a quanto dichiarato dal produttore in un documento detto *Security Target*.

10. Sicurezza informatica e sicurezza nazionale.

Dal 1995 esiste in Italia uno 'Schema Nazionale' che risponde all'esigenza di tutelare il Segreto di Stato.
Tale schema non è operante per i sistemi e i prodotti commerciali, in quanto l'Organismo che lo ha costituito, ovvero la Presidenza del Consiglio dei Ministri - Autorità Nazionale per la sicurezza, non è competente in materia.
La Legge n. 801 del 1977[546], che l'ha costituita, ne confina l'attività ai temi legati alla sicurezza nazionale.
Altre disposizioni, relative alla armonizzazione della produzione e commercializzazione di strumenti ad alta tecnologia con la sicurezza nazionale, 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).
È da ricordare, tuttavia, che nel corso della X legislatura, il Ministero dell'Interno tentò di regolamentare l'uso di sistemi di criptofonia e crittografia attraverso un Disegno di Legge (il n. 3232 dell'11 Febbraio 1992), presentato al Senato, che prevedeva disposizioni in tema di apparecchiature criptofoniche, ovvero destinate alla trasmissione in codice di comunicazioni telefoniche, radiofoniche o di altre forme di telecomunicazioni.
Tale previsione normativa, da un lato, subordinava la produzione, l'introduzione nello Stato, l'esportazione, la messa in vendita di apparecchiature per la ricetrasmissione in codice e per la codificazione di telecomunicazioni alla previa licenza del Questore. Dall'altro, prevedeva che per gli apparecchi di comunicazione in codice il produttore o l'importatore depositasse presso il Ministero delle PP.TT. i dati tecnici e gli apparati necessari per la decodificazione delle comunicazioni: ciò ai fini dell'intercettazione investigativa.
A tutto ciò si aggiungeva il divieto di vendita o di cessione delle apparecchiature a soggetti privi del nulla osta all'acquisto ed all'uso rilasciato dal Questore. Inoltre i detentori delle apparecchiature avrebbero

---

546 Per un commento ai risvolti politico sociali delle novità introdotte dalla Legge n. 801 del 1977, cfr. tra gli altri G. TAMBURINO, *Segreto, il limite delle leggi*, in Internet all'indirizzo http://www.cittadinolex.kataweb.it/CommentView/0,1527,1706%7C160,00.html (pagina visitata il 10 luglio 2002).

immediatamente dovuto denunciare il possesso e le variazioni alle Forze di Polizia. La violazione di qualsiasi disposizione era sanzionata penalmente.
Il Disegno di Legge in questione decadde con lo scioglimento delle Camere. Nel corso della successiva Legislatura, venne preparato un nuovo testo, che però non venne mai trasfuso in un Disegno di Legge.
Solo dopo diversi tentativi il Parlamento ha varato la Legge n. 222 del 27 Febbraio 1992, regolatrice dell'esportazione e del transito dei prodotti ad alta tecnologia.
La Legge precisa, al n. 2 dell'articolo 1, che sono soggetti alle autorizzazioni ed ai controlli dello Stato l'esportazione, in via definitiva o temporanea, ed il transito dei prodotti e delle tecnologie indicati in un apposito "elenco delle merci sottoposte ad autorizzazione per l'esportazione e per il transito", predisposto ed aggiornato ogni sei mesi con decreto del Ministro per il Commercio con l'Estero.
La legge prevede apposite sanzioni penali per l'attività quali l'esportazione o transito senza autorizzazione (articolo 12), per la falsità nella documentazione (articolo 13), per la violazione delle condizioni di consegna (articolo 14). In attuazione di tali disposizioni sono stati emanati poi alcuni decreti ministeriali[547].
Il Ministro della Difesa ha emesso il Decreto del 28 ottobre 1993 con il quale è stato approvato l'elenco dei materiali di armamento da comprendere nella categoria prevista dall'articolo 2, comma 2, della Legge n. 185 del 1990.
Tale decreto è stato poi aggiornato con decreto dell'1 settembre 1995, relativo al nuovo elenco dei sopracitati materiali di armamento.
Nella categoria 11ª, alle lettere d) e f), sono state previste le seguenti categorie: apparecchiature di sicurezza per il trattamento dei dati, apparecchiature di sicurezza per dati e apparecchiature di sicurezza per linee di trasmissione e di segnalazione, utilizzanti procedimenti di cifratura (d), e apparecchiature per l'identificazione, la autenticazione e il caricamento di chiavi crittografiche e apparecchiature per la gestione, produzione e abilitazione di crittografiche.
Il Ministero del Commercio con l'Estero ha aggiornato l'elenco con il d.m. 5 maggio 1994, relativo alla autorizzazione per esportazione definitiva e temporanea e per il transito dei prodotti ad alta tecnologia, facendo seguito a un precedente Decreto (24 giugno 1993) e stabilendo che i prodotti e le tecnologie di cui all'elenco allegato alla Legge del 1992 erano sottoposti ad autorizzazione per l'esportazione.
In esso, dopo aver dato la definizione di crittografia, ha inserito al Paragrafo 4A2, intitolato "Apparecchiature, assiemi e componenti", la voce 5A002, e particolarmente le lettere a) b) c) d) e) g): Sistemi, apparecchiature, "assiemi elettronici" specifici di applicazione, moduli o circuiti integrati che assicurano la "sicurezza dell'informazione", e loro componenti appositamente progettati: a. per utilizzare la "crittografia" con l'impiego di tecniche numeriche per assicurare la "sicurezza dell'informazione"; b. progettati o modificati per effettuare le funzioni crittoanalitiche; c. progettati o modificati per utilizzare la "crittografia" con l'impiego di tecniche analogiche per assicurare la "sicurezza

[547] Cfr. C. SARZANA DI S. IPPOLITO, *I riflessi normativi dell'uso dei sistemi crittografici in Italia*, in Internet sul sito http://www.sisde.it, (sito Internet visitato il 20 luglio 2002).

dell'informazione". d. progettati o modificati per sopprimere le emanazioni compromettenti di segnali portatori di informazioni; e. progettati o modificati per utilizzare tecniche crittografiche per generare il codice di estensione per "spettro esteso" o il codice per il salto di frequenza per i sistemi con "agilità di frequenza"; f. progettati o modificati per assicurare una "sicurezza a più livelli" o un isolamento dell'utente certificati o certificabili a un livello superiore alla Classe B2 della norma *Trusted Computer System Evaluation Criteria* (TCSEC) o norma equivalente; g. sistemi di cavi di telecomunicazione progettati o modificati, utilizzando mezzi meccanici elettrici o elettronici, per rilevare intrusioni surrettizie.

11. Le funzioni dell'Autorità Nazionale di Sicurezza (ANS) e dell'Ufficio Centrale per la Sicurezza (UCSi).

In Italia l'organizzazione nazionale per la sicurezza fa capo alla Presidenza del Consiglio dei Ministri. Il Presidente del Consiglio delega l'esercizio della tutela del segreto di Stato ad un alto funzionario dello Stato che assume la denominazione di Autorità Nazionale per la Sicurezza (ANS). L'ANS, per l'esercizio delle sue funzioni, si avvale dell'Ufficio Centrale per la Sicurezza (UCSi).
Nell'ambito dell'UCSi è istituita la Direzione Sicurezza Tecnica (DST), la quale: elabora la normativa nazionale nel campo della sicurezza tecnica; partecipa ai comitati di sicurezza nelle sedi NATO; controlla, certifica e omologa i sistemi LCT ed EAD che trattano informazioni classificate.
La DST, per lo svolgimento delle sue funzioni, è articolata su tre Sezioni: Sezione Segreteria e Coordinamento; Sezione Sicurezza TLC; Sezione Sicurezza EAD.
La Sezione (EAD) svolge i seguenti compiti: elaborazione e aggiornamento della normativa nazionale; emanazione di circolari e direttive attinenti la sicurezza hardware e software la certificazione e omologazione di Centri EAD; l'esame e la valutazione di progetti relativi alla protezione dei Centri EAD ai fini della certificazione/omologazione.
All'interno degli Enti e delle Ditte interessate, è stata prevista un'apposita struttura di responsabilità per gestire nel migliore dei modi il problema Sicurezza EAD.
Nell'ambito ani della Pubblica Amministrazione, sono stati individuati l'Organo Centrale di Sicurezza, con funzioni direttive, e l'Incaricato alla sicurezza EAD, con funzioni di controllo, mentre nelle industrie le medesime responsabilità sono devolute al Legale Rappresentante e all'apposita figura dell'Incaricato alla sicurezza EAD .
Nel 1994 il Presidente del Consiglio ha emanato un'ultima Direttiva riguardante, fra l'altro, i requisiti minimi da accettare per garantire la sicurezza delle informazioni classificate (COSMEC) trattate con apparecchiature o sistemi elettronici.

Una parte della Direttiva si occupa, specificamente, della sicurezza crittografica, intesa come quella componente della sicurezza delle comunicazioni derivante dalla adozione di sistemi crittografici tecnicamente appropriati, che deve essere conforme alle specifiche operative e alle prescrizioni generali.
L'ANS, inoltre, fornisce agli Enti della Pubblica Amministrazione istruzioni aggiornate sugli apparati Crypto, sui materiali Tempest, sui dispositivi Cosmec e logiche crittografiche approvate dalla stessa ANS da utilizzare per la trattazione, protezione e trasmissione di informazioni classificate.

Capitolo Ventiduesimo

Crittografia e sicurezza dei protocolli di rete

SOMMARIO: 1. Crittografia e protocolli di rete sicuri. – 2. Protocollo IP (*Internet Protocol*) e sicurezza. – 3. Crittografia e protocollo SSL (*Secure Socket Layer*).

1. Crittografia e protocolli di rete sicuri.

Prima di affrontare, anche se solo per sommi capi, l'argomento dei protocolli di rete sicuri, è necessario analizzare alcune caratteristiche del TCP/IP (*Transmission Control Protocol / Internet Protocol*), ovvero del gruppo di protocolli che viene utilizzato per la comunicazione tra macchine collegate ad Internet.
Innanzitutto, il TCP/IP è un protocollo di tipo *multilayer*, ovvero strutturato su più livelli, secondo un modello che viene definito 'ISO/OSI'.
La caratteristica fondamentale di questa struttura è che ogni livello mette a disposizione dei livelli superiori i servizi che gli sono propri, in una costruzione che, volendola rappresentare graficamente, sarebbe quella di una torta a più strati. In questo modo, le applicazioni (l'*application layer* è, infatti, lo strato più in alto) riescono ad interfacciarsi con i protocolli sottostanti e, così, a veicolare le informazioni.
I *layer* – o 'strati' - del TCP/IP sono cinque, e precisamente: 1) il livello fisico (i mezzi trasmissivi veri e propri quali, ad esempio, le fibre ottiche, le comunicazioni *wireless*, ecc.); 2) il *network layer* (che contiene le informazioni per far connettere il protocollo alla rete di trasporto: ad esempio il PPP); 3) l'*internetwork layer* (che gestisce l'indirizzamento dei pacchetti mediante il protocollo IP ed il protocollo ICMP); 4) il *transport layer* (che si occupa della sincronizzazione, nella fase di ricezione e trasmissione dei pacchetti, mediante il protocollo TCP ed UDP); 5) l'*application layer* (che è il livello dedicato alle applicazioni, e su cui girano i protocolli che caratterizzano i servizi di Internet quali l'HTTP, l'SMTP, il NTTP, ecc.).
Questa premessa sul funzionamento e la struttura del TCP/IP era indispensabile, dal momento che tutti i protocolli studiati per instaurare delle comunicazioni sicure si vanno a collocare in qualcuno dei *layer* sopra descritti e, a seconda del livello nel quale vengono collocati, presentano proprie caratteristiche e specificità.

2. Protocollo IP (*Internet Protocol*) e sicurezza.

Questa ricerca costante di protocolli in grado di garantire margini assai ampi di sicurezza si è resa necessaria nel momento in cui si è diffusa sul mercato la parte più commerciale di Internet. Il protocollo IP, infatti, per sua natura, è un protocollo assolutamente aperto, e non contiene, di fatto, alcuna accortezza in tema di sicurezza. I datagrammi del protocollo IP circolano 'in chiaro' lungo la Rete, per cui non è particolarmente complesso né leggerli, né modificarli, né cancellarli.
Se tutto ciò poteva essere sufficiente agli albori della diffusione della comunicazione telematica, oggi, sicuramente, non può più essere così, considerata la mole di informazioni personali e di alto valore che transita in Rete.
Per questo motivo, diversi studiosi hanno affrontato il problema su come rendere sicura la comunicazione e le soluzioni proposte sono state molteplici. Si è pensato, ad esempio, di creare dei protocolli specifici per la sicurezza che si andassero a collocare tra il *transport layer* e l'*application layer*, quali, ad esempio, IPSEC o SSL. Si è, d'altro canto, proposta una sicurezza incentrata sull'applicazione, con la creazione del S-HTTP per le transazioni via Web o dell'S/MIME per la posta elettronica. Si è, infine, superato il livello dell'*application layer* creando *software ad hoc* per le comunicazioni sicure, ed è il caso del già citato programma per la cifratura della posta elettronica 'PGP'.
Le metodologie di sicurezza legate ai protocolli di comunicazione più conosciute e diffuse sono le seguenti: IPSEC, SSH, SSL, S-HTTP, SET e S/MIME.
Il protocollo IPSEC è salito alla ribalta di recente, da quando è stato inserito come *standard* all'interno dell'IPv6, ovvero la versione 6 del protocollo IP che, oltre a consentire di indicizzare un maggior numero di indirizzi IP, presenta molte altre caratteristiche innovative, tra cui la previsione espressa di *policy* di sicurezza per il protocollo stesso.
In effetti, mediante IPSEC si riescono a stabilire delle *rules*[548] per i diversi pacchetti, per cui si potrà decidere quale pacchetto IP proteggere e quale no, cosa prima assolutamente impensabile.
Tutto ciò viene realizzato mediante due *header*[549] che vengono inseriti nel pacchetto IP, ossia l'*Autentication Header* (AH), che garantisce l'identità del mittente e l'integrità del *datagram*, e l'*Encapsulating Security Payload* (ESP), che garantisce la confidenzialità[550] del *datagram*.

---

[548] Si tratta delle regole mediante le quali si definisce il grado di protezione da assegnare al pacchetto e le parti che possono essere interessate dallo scambio dei pacchetti.
[549] Ogni pacchetto IP è costituito da un *header* e da una parte di dati. Nell'*header* sono contenuti diversi campi fondamentali per processare correttamente il pacchetto quali, ad esempio, la lunghezza, l'identificazione, l'indirizzo sorgente e di destinazione, ecc.
[550] Per 'confidenzialità' si intende la proprietà per cui l'informazione non viene resa disponibile a soggetti non autorizzati.

Questi due meccanismi fanno capo al concetto di *Security Association*, che consiste in un accordo tra due o più soggetti in materia di parametri di sicurezza da condividere: possono essere, ad esempio, l'algoritmo di cifratura da impiegare nell'AH, la durata delle chiavi di cifratura o il grado di sicurezza che i dati trasmessi richiedono.
La decifrazione del pacchetto IP incapsulato mediante IPSEC sarà possibile solo se il ricevente appartiene alla stessa SA del mittente.
Nel pacchetto IP è, poi, contenuto il *Security Parameters Index* (SPI) che scaturisce in sede di negoziazione e contiene i parametri propri della SA.
Dal momento che tutto il sistema IPSEC si basa su un metodo di cifratura a chiave simmetrica, si rendeva necessario implementare un meccanismo di scambio sicuro delle chiavi.
Si è optato, allora, per l'*Internet Key Management* (IKE), il quale altro non è che l'evoluzione di altri tipi di protocolli simili già noti[551].
L'SSH, invece, acronimo di *Secure Shell*, nasce col preciso scopo di poter operare su una macchina remota mediante una *consolle* tipo *telnet*, ma sfruttando un canale comunicativo sicuro. La sicurezza del canale, nel caso dell'SSH, è data dalla doppia autentificazione che viene operata durante una sessione SSH, per cui si garantisce sia l'identità dei soggetti sia l'integrità dei dati transitanti nel canale SSH.
La porta sulla quale si svolge la comunicazione mediante SSH è, di norma, la numero 22.
L'identificazione tra *server* e *client* funziona nel modo seguente: il *client* invia una richiesta di autenticazione al *server* che risponde inviando la *host public key* e la *server public key*. Il *client*, a questo punto, come prima cosa confronta la *host public key* inviatagli dal *server* con quella che ha memorizzata nella propria banca dati di chiavi; altrimenti, può anche memorizzare la suddetta chiave qualora gli risulti sconosciuta. Successivamente, il *client* utilizzerà la *host publick key* per inviare al *server* una chiave crittografata a 256 *bit*, detta *session key*. Questa sarà, da quel momento in poi, la chiave che verrà utilizzata per cifrare tutta la comunicazione tra *server* e *client*. Come algoritmo di cifratura se ne utilizzerà uno tra quelli supportati da entrambe le parti, riferendosi al concetto di *chiper suite*[552], per cui si potranno adoperare algoritmi quali il DES, il Triple-DES, il DSA, ecc.
L'autenticazione dal lato *client* potrà avvenire mediante *password* che, ovviamente, transiterà sul canale sicuro instaurato dall'SSH oppure mediante autenticazione RSA, sfruttando la tipologia di autenticazione dei sistemi a chiave asimmetrica.
L'unica pecca dell'SSH è data dal fatto che utilizza una distribuzione manuale delle chiavi, per cui i *server* dovranno necessariamente essere noti. Diversamente sarebbe stato, invece, se si fosse adottato un sistema di gestione delle chiavi mediante certificati.

---

551 Per l'esattezza, si tratta dei protocolli *Oakley*, SKEME e dalle specifiche definite dall'*Internet Security Association and Key Management Protocol*.

552 Per *chiper suite* si intende quell'insieme di algoritmi di cifratura che sono supportati sia dal *server* sia dal *client*. In sede di *handshaking* si eleggerà un algoritmo di cifratura per crittare la comunicazione tra il *client* ed il *server*.

3. Crittografia e protocollo SSL (*Secure Socket Layer*).

L'SSL (*Secure Socket Layer*), invece, è stato realizzato dalla *Netscape Corporation* ed è un protocollo che si colloca al di sopra del *transport layer*, così da poter essere utilizzato a prescindere dall'applicazione. È un protocollo che ha conosciuto un discreto successo, dal momento che può essere utilizzato da qualunque applicativo che si basi su TCP/IP, così come mantiene una piena compatibilità anche con altri metodi di autenticazione. In particolare, consente di avere i tre requisiti minimi necessari affinchè una comunicazione possa dirsi sicura, ossia 1) l'autenticazione fra le parti; 2) la confidenzialità dei dati; 3) l'integrità dei dati stessi.
La comunicazione mediante SSL si realizza attraverso una procedura di *handshaking* tra *client* e *server* e, per l'esattezza, attraverso dieci *step* ben definiti[553].
Innanzitutto il *client* manda al *server* il numero della versione di SSL adoperata, il tipo di algoritmo di cifratura da utilizzare, alcuni dati generati casualmente e altre informazioni necessarie per stabilire la comunicazione.
Successivamente, il *server* invia, a sua volta, quanto inviato dal *client* (numero di versione di SSL, algoritmo di cifratura, ecc.) oltre ad un certificato che lo identifica. Nel caso il *client* chieda qualcosa che necessiti di un autenticazione dal lato *client*, richiederà il certificato del *client*.
A questo punto, il *client* utilizzerà le informazioni ricevute dal *server* per autenticare il *server*. Nel caso il *server* non possa essere autenticato o vi siano altri tipi di problemi, l'utente sarà informato del problema, altrimenti il *client* passerà ad utilizzare i dati finora ricevuti in fase di *handshaking* per generare la *premaster secret*, che verrà cifrata mediante la chiave pubblica del *server* ed inviata al *server* stesso. Nel caso il *server* abbia richiesto al *client* un certificato, questo certificato verrà inviato insieme alla *premaster secret* e ad una porzione di dati firmati digitalmente dal *client*.
A questo punto, se il *server* ha richiesto l'autenticazione del *client* e questa non può avvenire, la comunicazione si chiude con un messaggio d'errore. Nel caso, invece, il *client* venga autenticato, il *server* userà la sua chiave privata, unitamente alla *premaster secret*, per generare la *master secret*.
Sia il *server* sia il *client*, quindi, utilizzeranno la *master secret* per generare le *session keys*, ovvero la coppia di chiavi simmetriche che saranno utilizzate per cifrare e decifrare le informazioni transitanti tra il *server* ed il *client* nell'ambito della comunicazione instaurata mediante SSL.
Il *client* invierà un messaggio, informando il *server* che, da quel momento in poi, le comunicazioni saranno cifrate mediante la *session key* frutto della negoziazione appena illustrata e invierà, inoltre, un messaggio cifrato separato per indicare che la porzione di *handshaking* di sua spettanza è terminata. Il *server*, a sua volta, invierà il messaggio per avvisare che anch'esso inizierà a cifrare

[553] Questi *step* si riferiscono alla versione 3.0, che è la versione corrente, al 15 luglio 2002, di SSL.

conformemente alla *session key*, ed informa il *client* che anche la sua porzione di *handshaking* è terminata.
Una volta compiuti questi *step*, la comunicazione sicura mediante SSL può iniziare.
La minuziosità nella descrizione della procedura di *handshaking* potrebbe far ritenere l'SSL un protocollo estremamente laborioso ma, in realtà, la comunicazione si stabilisce in pochi secondi ed è connotata da un elevato grado di sicurezza. Questi sono i motivi per i quali l'SSL sta conoscendo una discreta applicazione e diffusione in ambito Internet.
Al momento, è allo studio la nuova versione di SSL, che si chiamerà TSL, anche se finora è stata solo presentata una *draft-version* delle specifiche del protocollo all'attenzione della IETF[554].
Analogo per molti aspetti, ma totalmente differente nelle finalità, è il protocollo S-HTTP (*Secure Http*).
Anche questo protocollo serve per cifrare le comunicazioni, in particolare quelle transitanti sul protocollo HTTP che è il protocollo del Web, però si differenzia per molti aspetti dall'SSL. Quest'ultimo, infatti, tende a diventare un protocollo generico di sicurezza delle comunicazioni, senza restare necessariamente legato al livello delle applicazioni.
La riprova di ciò sta nel fatto che la stessa Netscape, società che detiene i diritti sull'SSL, nell'ultima versione del suo *browser* ha supportato l'S-HTTP e non l'SSL.
L'S-HTTP è dotato di una tipologia di cifratura simmetrica, e utilizza algoritmi *standard* di cifratura. La particolarità che maggiormente interessa è la sua estrema flessibilità.
Basti pensare che, in fase di autenticazione, non è strettamente necessario il possesso di un certificato, ma il protocollo è in grado di scegliere altre strade per arrivare, comunque, a garantire una comunicazione sicura, pur senza passare per la fase di autenticazione mediante certificato.
Inoltre, è connotato da estrema libertà per quanto riguarda la gestione della chiave di cifratura, le politiche di sicurezza, ecc. Ciò consente sia al *client* sia al *server* di essere molto 'liberi' nello stabilire le modalità mediante le quali instaurare la comunicazione e da ciò discende l'elevata flessibilità del protocollo in esame.
Per il resto, l'instaurarsi di una comunicazione mediante S-HTTP è un procedimento molto semplice, che si riassume in tre passi. Inizialmente, si invia un messaggio in chiaro, dopodiché il *server* invierà le proprie preferenze crittografiche, e il *client*, successivamente, farà lo stesso. Tale semplicità e flessibilità gli hanno consentito di essere scelto dal W3C[555] come *standard* per la sicurezza del Web.
Il protocollo SET, di contro, consente, oltre che di cifrare la comunicazione, anche di firmarla elettronicamente mediante apposizione della firma digitale dell'utente, così da accertare l'identità dello stesso. Esso utilizza un algoritmo a

---

554 *Internet Engineering Task Force,* ovvero l'organismo che si occupa di vagliare gli RFC (*Request For Comment*) che sono dei *paper* contenenti le specifiche degli *standard* utilizzati in Internet.
555 *World Wide Web Consortium,* cioè il consorzio che si occupa di stilare gli *standard* per la comunicazione mediante Web in Internet.

chiave simmetrica, il DES, per crittografare i messaggi e, invece, usa l'RSA per effettuare operazioni quali lo scambio della chiave segreta tra *client* e *server*, la firma digitale della comunicazione e la certificazione del *server*. Tuttavia il SET richiede che sul computer *client* sia installato un certificato digitale rilasciato dagli appositi enti certificatori individuati per legge.
Sicuramente, questo protocollo presenta delle migliorie rispetto, ad esempio, all'SSL, ma risente della sua giovane età, per cui è ancora utilizzato in via sperimentale e non molto diffuso. È un protocollo specificamente studiato per le applicazione di *e-commerce* e di *on-line banking* e sta di fatto che, quando sarà correttamente implementato, questo protocollo conoscerà sicuramente una vasta diffusione, viste le sue peculiarità. Esso consente, infatti, di garantire la confidenzialità nelle transazioni, l'autenticazione del cliente e del venditore, l'interoperabilità tra diversi *software* (ad esempio, tra diversi programmi di gestione dei movimenti bancari) ed è indipendente dal protocollo deputato a garantire la sicurezza a livello di trasporto.
L'ultimo protocollo da prendere in considerazione è l'S/MIME. Esso nasce come protocollo specifico per garantire la sicurezza della posta elettronica, e in ciò si distingue da altri prodotti quali, ad esempio, PGP, che sono degli applicativi e non dei protocolli. Utilizza le specifiche MIME per la creazione del messaggio e divide il messaggio in due sezioni: *header* e testo. L'*header* sarà la parte del messaggio che conterrà tutte le informazioni di cifratura del messaggio, del mittente del messaggio, ecc. In particolare, implementa una procedura di firma digitale, onde garantire l'integrità del messaggio ed una procedura successiva di cifratura del messaggio stesso, onde renderlo illeggibile per chiunque se non per il legittimo destinatario.
Gli algoritmi utilizzati per la procedura di firma digitale sono l'MD5 e l'RSA, mentre per la cifratura si avvale del DES, del Triple-DES o dell'RC2. Si tratta di un protocollo in grado di garantire un buon grado di sicurezza e, soprattutto, di utilizzare, senza alcuna limitazione, lo strumento della posta elettronica. Mediante S/MIME, infatti, sarà possibile trasmettere in maniera sicura anche *file* allegati al messaggio di posta elettronica.