ANDREA GIANNACCARI

LA CRITTOGRAFIA COME STRUMENTO PER GARANTIRE LA RISERVATEZZA DELLE COMUNICAZIONI

SOMMARIO: 1. Cenni storici ed introduttivi. — 2. La crittografia negli Stati Uniti: le norme vigenti. — 3. La crittografia nel diritto internazionale. — 4. L'Unione Europea. — 5. La crittografia in Italia.

1. Cenni storici ed introduttivi.

Il termine « crittografia » deriva etimologicamente dalle parole *kryptós* e *graphía* in uso nella Grecia antica e significa letteralmente 'scrittura nascosta': infatti, si definisce tale ogni metodologia utile a rendere incomprensibile un qualsiasi tipo di scrittura allo scopo di renderla leggibile soltanto a chi possieda la corretta chiave di interpretazione.

La crittografia risale, come si evince dalla stessa etimologia, alla notte dei tempi e lascia intuire il legame che esiste tra questa forma di scrittura e le problematiche connesse all'esercizio del potere ed alle operazioni militari. I più antichi esempi di crittografia, infatti, si trovano in alcuni geroglifici egiziani, dove però l'operazione effettuata, consistente nella sostituzione di simboli comuni con altri inconsueti, aveva per scopo non la segretezza, ma la preziosità estetica o il conferimento di un senso di mistero: tale uso della 'crittografia' riguardava soprattutto le iscrizioni tombali.

Le prime notizie sicure sono quelle sulla *scìtala lacedemonica*, di cui parla Plutarco (I secolo *d.C.*), il famoso storico greco, nell'opera *Vite Parallele*: egli afferma che questo metodo era in uso probabilmente già ai tempi di Licurgo (IX secolo *a.C.*), ma sicuramente al tempo di Lisandro (400 *a.C.*), famoso generale e politico spartano. Tale metodo che, come ci racconta lo stesso Plutarco, era utilizzato dal governo spartano per trasmettere ai generali messaggi segreti, consisteva in un cilindro (solitamente di legno, la scitala appunto) sul quale il mittente avvolgeva a spirale un nastro di pergamena o di cuoio: sul nastro si scriveva per colonne parallele all'asse del bastone, lettera per lettera, il messaggio segreto. Quando il nastro veniva tolto dal bastone, il testo vi risultava trasposto in modo regolare, ma ciò era sufficiente per 'evitare' la lettura da parte di chi fosse sprovvisto di un cilindro con la stessa circonferenza di quello del mittente: il possessore di un bastone uguale a quello del mittente era appunto il legittimo destinatario del messaggio (o almeno questo era l'auspicio). La crittografia impiegata per uso militare è però molto spesso citata anche nelle *Storie* di Erodoto, in Tucidide e Senofonte e del suo sviluppo in Grecia testimoniano anche le accurate descrizioni contenute negli scritti di Enea il Tattico e Polibio.

Anche più diffusa sembra essere la crittografia nel mondo romano: lo stesso Giulio Cesare (100-44 *a.C.*) afferma, nel *De bello gallico*, di essersene ampiamente servito sia per le comunicazioni militari, sia per le corrispondenze con i familiari. Svetonio ce ne dà conferma nel *De vita Caesarum*, il suo lavoro più importante sulle vite degli imperatori, nel quale spiega i sistemi di cifratura adoperati da Cesare e da Ottaviano Augusto. Il cifrario di Cesare si otteneva, ad esempio, scrivendo l'alfabeto cifrato sotto l'alfabeto in chiaro: il cifrato era il risultato dello spostamento delle lettere a sinistra di tre posizioni. Quest'ultimo veniva utilizzato per le operazioni di cifratura: alla lettera 'a' corrispondeva la lettera 'd', alla lettera 'b' corrispondeva la lettera 'e' e così di seguito; sostituendo le lettere del testo in chiaro con le omologhe dell'alfabeto cifrato si otteneva un messaggio comprensibile solo ai due interlocutori. Chiunque avesse intercettato la corrispondenza senza conoscere il sistema di codifica (e decodifica) non avrebbe potuto comprenderne il significato.

Dopo l'oscurantismo medievale ci fu un risveglio dell'interesse per la crittografia, dovuto essenzialmente all'inizio degli scambi diplomatici fra i vari staterelli europei e all'istituzione delle prime ambasciate. Nello stesso periodo inizia a svilupparsi l'uso della crittografia nell'ambiente ecclesiastico: numerosi furono i crittologi che lavorarono per vescovi, cardinali e Papi; non fu per caso che il vescovo Antonio Elio istituì, nel 1540, il primo « ufficio cifra » regolare presso il Vaticano, con un secolo di anticipo rispetto a quello fondato dal cardinale Richelieu in Francia alla Corte del Re Luigi XIII.

Tra la fine del '700 e la metà dell''800, la crittografia non conosce un'evoluzione degna di nota, eccezion fatta per il codice di Jefferson: tale codice prende il nome dal suo inventore Thomas Jefferson, autore della Dichiarazione d'Indipendenza e Presidente degli Stati Uniti nel mandato del 1801.

Un poderoso utilizzo della crittografia è, al contrario, da ascriversi all'interno dei due conflitti mondiali. La Grande Guerra fu la prima ad essere combattuta nell'era della radio: essa, infatti, garantiva maggiore rapidità nella circolazione delle informazioni; in tempo reale era possibile conoscere gli spostamenti delle truppe o delle flotte. Ma la radio palesava un grande problema: tutti erano in grado di ascoltare le comunicazioni altrui. Fu per tale motivo che chi non era crittograficamente attrezzato all'inizio del conflitto cercò di rimediare a guerra ormai iniziata: così fecero la Germania, l'Inghilterra e l'Italia.

Gli studi e le implementazioni crittografiche del Primo Conflitto mondiale costituirono la base delle applicazioni della Seconda Guerra Mondiale, vera e propria 'guerra dei codici'. Gli americani furono i più abili sia nello sviluppo di tecniche di protezione che in quelle di attacco (vale a dire di decrittazione). Sul versante difensivo, il crittosistema *Sigaba* riuscì a compiere il suo dovere poiché non fu possibile per gli avversari la sua decrittazione; sul lato offensivo, l'*intelligence* statunitense contribuì ampiamente alla vittoria sia sull'Atlantico che sul Pacifico. I crittologi americani riuscivano sistematicamente a leggere il sofisticato traffico commerciale e militare dei Giapponesi e collaboravano intensamente con gli Inglesi per intercettare e leggere le comunicazioni dei Tedeschi.

Inoltre gli Americani furono i primi ad applicare la crittografia alle comunicazioni telefoniche: i tecnici d'oltre atlantico riuscirono a mettere a punto il primo telefono 'sicuro', il *Sigsaly*. Questo telefono, sviluppato

presso i laboratori della Bell, si avvaleva di tecnologia digitale che commutava la voce in una stringa di 2400 *bit* al secondo, che veniva successivamente cifrata. Poiché, però, l'attrezzatura che consentiva di effettuare queste operazioni era molto voluminosa, oltre che particolarmente costosa, solo due persone sul pianeta furono in grado di adoperarla: Franklin Roosvelt e Winston Churchill. I successi delle operazioni americane di *communication intelligence* costituirono la base per la successiva espansione ed il consolidamento delle strutture di spionaggio che, oggi più di allora, sono appannaggio quasi esclusivo degli Stati Uniti.

Questo fugace *excursus* storico, dal quale un'organica tassonomia risulta compromessa, vuole evidenziare due aspetti intimamente correlati: il primo è relativo al fatto che la crittografia è stata a fianco del Potere per circa 2800 anni. L'*habitat*, nel quale essa è nata e si è sviluppata, è stato quello dell'Imperatore e del Re prima e del Palazzo e della mensa del Principe, laico od ecclesiastico che fosse, dopo.

La precisazione ci conduce a riflettere sulla seconda peculiarità della crittografia: essa è stata ed è adoperata per garantire, principalmente, la riservatezza (segretezza) delle comunicazioni. La puntualizzazione può sembrare pleonastica, ma ci aiuta a fugare i dubbi apportati dalla moderna crittografia, quella asimmetrica, inventata nel 1976 dall'allora dottorando a Stanford Whitfield Diffie e dal suo relatore Martin Hellman e divulgata, per la prima volta, nell'ormai celebre articolo « *New Directions in Cryptography* ». La crittografia asimmetrica, che si basa sull'adozione di due chiavi (una pubblica ed una privata), può essere utilizzata per assolvere più scopi: il primo, quello che identifica la funzione classica della crittografia è la *riservatezza*, cioè garantire agli interlocutori — con un grado di ragionevole certezza — che il sistema di codifica del messaggio sia abbastanza robusto da inibire a terzi la decrittazione dello stesso e garantire, invece, ai soli interlocutori la decifrazione e quindi la comprensione del testo. Una seconda funzione è quella di assicurare *l'integrità* del messaggio: in caso di intercettazione dello stesso non deve essere possibile una sua alterazione senza che il legittimo destinatario possa immediatamente accorgersene.

Una terza funzione è quella di garantire *l'autenticazione* degli interlocutori, vale a dire la possibilità di accertare — per ciò che riguarda la provenienza del documento — che colui che si dichiara essere l'autore, sia effettivamente il legittimo mittente e non altri che abusivamente ne utilizzi l'identità[1]. L'ultimo 'compito' della crittografia è quello di assicurare il *non-ripudio*, che in altri termini significa che il mittente del messaggio non deve essere in grado di negare di averlo trasmesso.

Queste sono le potenzialità della crittografia, ma bisogna sottolineare che, mentre per le ultime tre funzioni (integrità, autenticazione e non ripudio, che sono quelle necessarie per la creazione della firma digitale) c'è un'ampia convergenza di orizzonti a livello mondiale e una relativa facilità normativa, l'esatto contrario possiamo dire per la riservatezza, che invece ha creato e continua a creare diatribe e conflitti apparentemente insormontabili. Adoperando una metafora, si può sottolineare che è la riserva-

[1] Il problema è relativo alla tutela del diritto al nome.

tezza l'elemento chiave, la discriminante che differenzia la crittografia alla quale, solitamente, ci si rapporta discettando di firma digitale. In quest'ultimo caso, il documento al quale viene apposta la firma digitale (ottenuta cifrando, con la propria chiave privata, un estratto del documento stesso) percorre le vie digitali o telematiche 'in chiaro': se una terza parte (un organo inquirente provvisto di mandato di intercettazione o un « Grande Fratello » all'ascolto) intercettasse la comunicazione, sarebbe in grado di leggere il contenuto del messaggio.

Faremo, quindi, riferimento alla crittografia adoperata per garantire la riservatezza delle comunicazioni; la centralità e l'importanza di questo aspetto sono ormai evidenti e sempre più di pubblico dominio, anche in relazione alla nascente *new economy*: la fine della « guerra fredda », il ridimensionamento dell'Unione Sovietica sul piano sia politico che militare e la caduta del muro di Berlino hanno, infatti, fatto sì che la crittografia uscisse dai circuiti militari e diplomatici per diventare una disciplina in gran voga negli ambienti dell'informatica e delle telecomunicazioni. La politica, con il fisiologico ritardo con il quale (in)segue il fenomeno tecnologico ed economico, sta cercando di comporre i diversi interessi in gioco senza menomare in alcun modo quella « ragion di Stato » che, secondo l'interpretazione che ne diede Campanella, mira da sempre a mantenere il controllo della popolazione. La crittografia è l'unico strumento capace di garantire la riservatezza delle comunicazioni all'interno di percorsi che sono, in molti casi, fuori dal controllo sia del mittente che del destinatario. Nelle comunicazioni mobili e satellitari, poi, essa rappresenta il solo mezzo di difesa; nel mondo fisico si chiudono le porte, ci si dota di finestre e si parla sottovoce se non si vuole essere ascoltati: nel mondo digitale si deve cifrare. Sebbene, tuttavia, la transnazionalità, propria sia dei moderni sistemi di comunicazione che della crittografia utilizzata per garantire la riservatezza dei messaggi nei percorsi telematici, limita le attitudini regolatorie di interventi normativi di tipo municipale, credo sia opportuno volgere lo sguardo agli Stati Uniti. L'informatica è nata oltreoceano, *internet* si è sviluppato nelle stanze del Pentagono, il *DES* (il più noto programma di crittografia) è stato realizzato dalla IBM e fu adottato dal settore finanziario di tutto il mondo; in altre parole, in questo settore, la capacità professionale, la competenza specifica e le strutture di cui gli americani sono dotati hanno qualche lustro di vantaggio sugli altri Paesi. Anche le ripercussioni giuridiche apportate dalla crittografia sono all'attenzione dei circuiti politici, accademici ed industriali già da qualche anno: cerchiamo quindi di capire qual è, oltreoceano, lo stato dell'arte a livello legislativo.

2. La crittografia negli Stati Uniti: le norme vigenti.

Anzitutto credo sia importante sottolineare che non esiste alcun tipo di limite o di vincolo per quanto concerne l'uso di crittografia da parte dei cittadini americani residenti negli USA: l'uso di crittografia, di qualsiasi tipo e quindi con chiavi di qualsiasi lunghezza è consentito senza alcuna restrizione.

Analoga libertà è garantita per ciò che attiene alle importazioni di crittografia: relativamente a queste ultime, il Presidente degli Stati Uniti ha una *statutory authority*, che permette di porre dei vincoli, qualora lo ri-

tenga opportuno, ma attualmente non esiste alcun tipo di restrizione delle importazioni.

Considerato, però, che gli Stati Uniti sono il Paese all'avanguardia per ciò che concerne la produzione dei prodotti crittografici e, quindi, della relativa vendita all'estero, rivestono una particolare importanza le norme relative all'esportazione di *crittografia*.

Tutte le esportazioni che vengono effettuate dagli Stati Uniti sono soggette a due leggi: l'*Arms Export Control Act* (*title* 22 U.S.C., *sections* 2571-2794, rubricato con il nome « *Arms control and disarmament* ») e l'*Export Administration Act* (*title* 50 U.S.C. App. 2401-2420, rubricato con il nome « *War and national defense* »). La crittografia, quindi, è una di quelle materie che beneficiano di una competenza legislativa federale: ciò perché la Costituzione americana conferisce al Congresso solo alcune attribuzioni. Più precisamente l'articolo I, sezione XIII, punto 3 della Costituzione prevede che il Congresso « disciplini il commercio con le Nazioni estere e fra i diversi Stati dell'Unione (...) »: l'*Export Administration Act*, infatti, è volto a disciplinare le esportazioni. L'altra legge, l'*Arms Export Control Act*, è da ascriversi alla competenza legislativa federale *ex* articolo I, sezione XIII, punto 18 della Costituzione, che prevede che il Congresso legiferi relativamente alle questioni afferenti la guerra.

L'*Arms Export Control Act*, infatti, conferisce al *Department of State* l'autorità di regolare le esportazioni di tutto ciò che è considerato un'arma di guerra (il termine corretto è *munition*). Le armi da guerra — *munitions* — richiedono, per essere esportate, una licenza che ne approvi l'esportazione, ma che indichi anche chi sia l'acquirente, l'uso al quale sono destinate, il modo di trattamento e le condizioni per un'eventuale cessione. La crittografia destinata ad uso militare è disciplinata, relativamente alle esportazioni, da questa legge, poiché è inserita nella *United States Munitions List* amministrata dal *Department of State*.

Ciò che, invece, non è considerata strettamente un'arma da guerra, ma che può essere adoperata, come la crittografia, anche per scopi militari, viene individuata con il nome *dual-use item*: con questo termine, infatti, si rintracciano gli strumenti che possono essere utilizzati per applicazioni sia civili che militari.

Se il *Department of State* decide che uno strumento è da classificarsi come *dual-use item*, ne trasferisce la giurisdizione, relativamente alle esportazioni, al *Department of Commerce*, che è l'ente che ha la potestà sull'*Export Administration Act* e che, quindi, può emanare gli *Export Administration Regulations* (EAR). Questi ultimi sono i Regolamenti Governativi attraverso i quali l'Amministrazione può 'operare'. Il *Department of Commerce* amministra una lista, denominata *Commerce Control List*, nella quale sono presenti tutti i *dual use items*, fra i quali la crittografia adoperata per usi civili.

Questo *status quo* è il portato di alcuni cambiamenti di competenze che sono stati introdotti nell'ambito dell'Amministrazione americana dall'Executive Order 13026 emesso dal Presidente Clinton il 15 novembre del 1996: precedentemente, infatti, le esportazioni erano regolate anche dall'oramai emendato *International Traffic in Arms Regulation* (ITAR).

Il meccanismo attuale è, nel suo complesso, relativamente semplice: i regolamenti sulle esportazioni emanati dal *Department of Commerce* (più precisamente dal *Bureau of Export Administration*, la struttura del *Department of Commerce* che si occupa dei regolamenti sulle esportazioni

di crittografia) stabiliscono i limiti, relativamente alla lunghezza delle chiavi ed al tipo di prodotti per i quali non deve richiedersi, al Dicastero del Commercio, una licenza che ne autorizzi l'esportazione. Alcuni prodotti, o prodotti che garantiscono un livello di riservatezza alto (dotati evidentemente di chiavi di cifratura molto lunghe) necessitano, al contrario, del *placet* ministeriale che si sostanzia nel rilascio di una licenza. I regolamenti, emanati dal *Department of Commerce*, sono inseriti nel *Code of Federal Regulations*: la crittografia è disciplinata nel *title* 15, *parts* 740 e seguenti.

Dal 15 novembre del 1996, giorno in cui Clinton ha trasferito la potestà legislativa sulla crittografia civile dal *Department of State* al *Department of Commerce*, quest'ultimo ha già emanato tre regolamenti sull'esportazione di prodotti crittografici da destinarsi ad applicazioni civili, manifestando una ipertrofia legislativa più prossima alla nostra tradizione, che non a quella nordamericana. Brevemente: i regolamenti del 30 dicembre 1996 elevavano a 56 *bit* (l'ITAR prevedeva 40 *bit)* la lunghezza delle chiavi dei prodotti che necessitavano di licenza all'esportazione, ma con una procedura di rilascio della stessa particolarmente snella. Il 31 dicembre del 1998 furono modificate alcune previsioni con l'emanazione di un nuovo regolamento: i prodotti a 56 *bit* potevano essere esportati dopo una semplice « *one-time review* », così anche i prodotti di crittografia asimmetrica fino a 1024 *bit*. Inoltre, venivano allentati i vincoli per i prodotti destinati al commercio elettronico, alle succursali estere di multinazionali americane ed ai prodotti dotati della caratteristica di essere *key escrow*[2].

---

[2] Il 16 aprile del 1993, la Casa Bianca annunciò la *Escrowed Encryption Initiative*: il programma prevedeva il miglioramento della sicurezza e della riservatezza delle comunicazioni telefoniche (grazie all'utilizzo di sistemi crittografici), ma, nel contempo, anche l'accessibilità dei messaggi, in chiaro, alle varie agenzie di polizia. Il trucco era rappresentato dal meccanismo di « *key escrow* ». Stando agli attuali orientamenti e tralasciando i trascorsi governativi relativi alla promozione di tali meccanismi, possiamo dire che il sistema vaticinato dal Governo si basa sulla creazione di una struttura, la « *Escrow Agency* », che avrebbe il compito di conservare la chiave per decifrare le comunicazioni o le informazioni cifrate. Ogni utente dovrebbe condividere la chiave privata con gli *escrow agents*, i quali, a seguito del rilascio di un mandato di intercettazione emesso da un giudice, dovrebbero consegnarla agli organi inquirenti che utilizzerebbero la chiave per decifrare le comunicazioni.

Questi sistemi, però, sollevano una coltre densa di problematiche che possiamo cercare di suddividere tra tecniche e giuridiche. Per ciò che riguarda il primo aspetto, dobbiamo sottolineare che i sistemi di *key escrow* presentano il rischio che qualcuno — gli *escrow agents* — possano abusare della loro posizione violando la fiducia riposta nei loro riguardi. Inoltre, verrebbero a crearsi delle strutture che susciterebbero un interesse smisurato, da parte dei criminali informatici e non: la conservazione centralizzata degli strumenti, che consentono di comprendere ogni tipo di comunicazione riservata, costituisce un obiettivo di grande valore. Ci sono, poi, tutta una serie di difficoltà e di costi legati alla gestione di un'impalcatura di sicurezza caratterizzata dalla condivisione della chiave privata con degli organi pubblici o privati come gli *escrow agents*. Poiché, infatti, le *law enforcement agencies* devono poter accedere, in qualsiasi momento, alle chiavi di decifratura, viene snaturata la caratteristica primaria garantita dalla cifratura asimmetrica: il completo controllo, da parte dell'utente, della sua chiave privata e la sua non condivisione con alcuno. In tal senso A.A.V.V., « *The risks of key recovery, key escrow and trusted third-party encryption* », rapporti del 1997 e del 1998.

Inoltre i sistemi di *key escrow* sollevano, e veniamo al secondo aspetto, alcuni importanti quesiti costituzionali: una persona, al fine di proteggere le proprie comunicazioni, deve consentire a qualcun altro (gli *escrow agents*) di poterne comprendere il relativo significato. Possiamo affermare

Il 14 gennaio di quest'anno, infine, il *Bureau of Export Administration* ha, con il terzo regolamento, reso più semplice l'esportazione di molti prodotti, soprattutto di quelli destinati al mercato di massa, che può avvenire « *after a technical review* ». Inoltre, i prodotti fino a 64 *bit* sono « *freely exportable* », anche se, nella maggioranza dei casi, si è obbligati a notificare al *Bureau of Export Administration* i codici sorgente dei programmi, vale a dire l'esatto funzionamento degli stessi. Si deve, inoltre, aggiungere che per la concessione delle licenze e per il vaglio dei prodotti, il *Bureau of Export Administration* è coadiuvato dalla competenza tecnica della *Natinal Security Agency*[3] e ciò in virtù dell'Executive Order 13026 emesso dal Presidente Clinton il 15 novembre del 1996.

La domanda che ci si potrebbe porre, prima di analizzare le ripercussioni giudiziarie legate agli *export controls*, è quella relativa alla *ratio* stessa di questi regolamenti. In altre parole, non essendoci limiti all'uso e all'importazione di prodotti crittografici, perché gli osservatori sono così critici nei riguardi delle disposizioni sull'esportazione, che sembrerebbero avere un risibile carattere preclusivo?

Le risposte sono diverse, ma tutte importanti:

a) Il primo obiettivo è quello di limitare la disponibilità all'estero di sistemi crittografici di « *strategic capability* », gli unici a porre seri problemi crittanalitici alle *US intelligence agencies*.

che il punto nodale è costituito dal bilanciamento di due interessi contrapposti: i cittadini hanno dalla loro parte le ragioni, forti, del Primo e del Quarto Emendamento, tuttavia l'interesse del Governo alla sicurezza nazionale, avallato dalla pratica e dalle più recenti interpretazioni costituzionali, supera di gran lunga e riesce a comprimere oltremodo il diritto alla riservatezza delle persone. Il delicato bilanciamento di tali diritti sarà, forse, di competenza dei giudici, che si troveranno a decidere se acconsentire, sempre e comunque, alla consegna della chiave alle *law enforcement agencies*, oppure se adottare un'interpretazione costituzionale, più restrittiva, che tenga in maggiore considerazione i diritti dei cittadini.

Vorrei chiudere la lunga parentesi riportando la frase del Giudice della Corte Suprema William Brennan:

« *The concept of military necessity is seductively broad, and has a dangerous plasticity. Because they invariably have the visage of overriding importance, there is always a temptation to invoke security "necessities" to justify an encroachement upon civil liberties. For that reason, the military-security argument must be approached with a healthy skepticism: its very gravity counsels that courts be cautions when military necessity is invoked by the Government to justify a trespass on (Constitutional) rights.* ».

Ho la sensazione, però, che tali suggerimenti saranno disattesi poiché gli sforzi che il Governo sta profondendo nel settore crittografico, che oggi sono rappresentati dal CESA Act in discussione al Congresso e volto a disciplinare i sistemi di *key escrow*, tralasciando tuttavia adeguati presidi legislativi a difesa dei cittadini, evidenziano come, sul diritto alla riservatezza dei cittadini, stia calando, lentamente, il sipario.

[3] La *National Security Agency* (*NSA*) è l'agenzia responsabile della crittografia nazionale statunitense, ma anche e soprattutto della intercettazione e decrittazione delle comunicazioni: fu istituita nel Novembre del 1952 con atto diretto del Presidente Harry Truman. L'esistenza della NSA fu negata fino al 1972, quando l'agenzia fu riorganizzata in seguito alla costituzione del CSS (*Central Secutity Service*), organismo militare responsabile della *signal intelligence* dei servizi segreti militari. Nel 1984 fu assegnato alla NSA il compito di provvedere anche alla sicurezza dei sistemi informativi connessi alla sicurezza nazionale; nel 1986, infine, la NSA divenne « *a combat support agency of the Department of Defense* ». La NSA ha sede a Fort George G. Meade nel Maryland; il suo direttore, Kenneth Minihan, è anche capo del CSS. Per inciso, la NSA è l'agenzia che ha amministrato e amministra quella rete di spionaggio ed intercettazione mondiale nota con il nome di Echelon, della quale la Commissione Europea ed il Parlamento Europeo fanno finta, oggi, di occuparsi.

b) Un secondo obiettivo, particolarmente rilevante, è quello di rallentare la diffusione mondiale di sistemi crittografici sufficientemente forti e tali da rappresentare un serio sbarramento per la selezione del traffico[4]. È evidente, quindi, che lo scopo è quello di prevenire l'esportazione di prodotti crittografici che non possono essere 'aperti' in tempo reale dalle *law enforcement agencies*. Questa considerazione, che nel tempo è diventata una convinzione di quasi tutti i commentatori, induce ad affermare che il *Department of Commerce* (leggi NSA) allenti i limiti all'esportazione solo se le agenzie di sicurezza sono in grado di 'fare i conti' con le nuove disponibilità crittografiche che si consente di esportare e, quindi, di usare. Il corollario fisiologico del ragionamento induce ad affermare che sul mercato, 'drogato' dalla volontà governativa, non siano presenti prodotti che garantiscano un adeguato livello di sicurezza.

c) Un ulteriore obiettivo è quello di impedire l'adozione di un sistema crittografico che si imponga come uno *standard*: l'emanare o l'annunciare, ogni dieci mesi, un cambiamento del regime delle esportazioni, rende la situazione instabile ed evita che ci si doti di un qualche sistema di protezione. L'effetto secondario di questa pratica è quello di mantenere lo *status quo* crittografico: gli utilizzatori di crittografia rimangono, numericamente, pochi e ciò consente alle *law enforcement agencies* di 'monitorare' più efficacemente il traffico di informazioni. Qualora fossero in molti ad utilizzare crittografia forte, le difficoltà delle agenzie crescerebbero esponenzialmente: questo è un risultato che si vuole evitare.

d) L'ultimo obiettivo è quello di avere, da parte della NSA, il controllo sul funzionamento di tutti i prodotti che vengono esportati dagli Stati Uniti. Poiché, per la maggior parte dei sistemi, è richiesto che i produttori rendano noti, al *Department of Commerce*, i dettagli ed i meccanismi degli strumenti che intendono esportare, ciò consente alla NSA di conoscere, in modo preciso, ogni sistema di cifratura e, quindi, di negare o di consentire l'esportazione dei singoli prodotti sulla base di conoscenze puntuali. Anche il rapporto del *National Research Council* — « *Cryptography's Role in Securing the Information Society* »[5]— sottolinea che questo è uno degli obiettivi più importanti delle politiche sull'esportazione dei prodotti crittografici.

Quest'ultima considerazione ci induce ad approfondire un ulteriore aspetto: i controlli sulle esportazioni hanno limitato e limitano la vendita dei prodotti americani sui mercati esteri.

---

[4] Questi obiettivi vengono evidenziati, anche, da due attenti osservatori: Whitfield Diffie, l'inventore della crittografia asimmetrica, e Susan Landau. Cfr. *Privacy on the line*, M.I.T. Press, paperback edition, 1999.

[5] Nel 1994 il Congresso incaricò il *National Research Council* (NRC) di effettuare una « *comprehensive indipendent review of national encryption policy* »; il NRC, per avere la pluralità di opinioni richiesta, formò un gruppo di studio, presieduto da Kenneth Dam, costituito dai massimi esperti sull'argomento, che portarono ognuno le istanze e le esigenze del settore che rappresentavano: Stato, industria ed università. Il rapporto, consegnato nel 1996, dopo due anni di lavori, è diventato lo stesso anno una pubblicazione essenziale per la comprensione della crittografia. Kenneth W. Dam and Herbert S. Lin, Editors; Committee to Study National Cryptography Policy, National Research Council, « *Cryptography's Role in Securing the Information Society* », 1996.

Le società americane produttrici di *software* crittografico, infatti, si sono trovate ed in parte si trovano tuttora in grande difficoltà: ciò perché, per sviluppare un prodotto, occorrono capitali, risorse, tempo e, a causa delle restrizioni sulle esportazioni, bisogna considerare che gli sforzi potrebbero risolversi in un nulla di fatto. I limiti all'esportazione, e quindi la necessità di dover ottenere una licenza, creano un'alea di incertezza, che 'obbliga' le aziende a non investire per migliorare, implementare o realizzare nuovi prodotti. È evidente che, con questo meccanismo, si mettono fuori gioco le aziende americane.

Questo risultato ha connotati di particolare successo, per il Governo americano, poiché le aziende statunitensi, produttrici di *software* crittografico, sono *leader* nel mondo, nel settore della sicurezza.

La scelta delle aziende americane potrebbe essere quella di sviluppare due diversi tipi di prodotti, uno destinato al mercato interno ed un altro a quello estero, ma anche nel caso in cui le aziende producessero due differenti versioni di un prodotto, quasi nessuno si doterebbe della versione con potenzialità usufruibili solo entro i patri confini[6]. Il problema, però, non si pone perché le aziende non vogliono rischiare di realizzare prodotti ai quali potrebbe essere negata la licenza all'esportazione: vengono, infatti, utilizzati dei sistemi che hanno un livello di protezione medio-basso, sui quali la NSA ha un totale controllo, che ottengono facilmente la licenza per essere esportati o che necessitano di una semplice « *technical review* » e che, di conseguenza, sono acquistati anche dai cittadini americani.

I vincoli all'esportazione servono, quindi, anche per 'drogare' il mercato nord-americano evitando che vengano sviluppati ed adottati sistemi che garantiscano un livello di protezione maggiore.

Questi sono gli obiettivi dei regolamenti sulle esportazioni, che tuttavia stavano spiazzando le aziende statunitensi nei confronti di quelle europee: è per tale motivo che i regolamenti emanati il 14 gennaio scorso hanno reso più agevole e snella l'intera disciplina delle esportazioni escludendo, in alcuni casi, l'adempimento della licenza[7]. Le nuove disposizioni sulle esportazioni devono, probabilmente, leggersi come tentativo, per altro pienamente riuscito, di ingraziarsi la 'Silicon Valley' e di riammettere le aziende americane all'interno di un mercato concorrenziale. Le disposizioni, eccessivamente restrittive, delle esportazioni, avevano messo fuori gioco le aziende 'di casa'; questi cambiamenti le riabilitano pienamente e le collocano nel posto che compete loro: *leader* nel mondo del settore informatico. Il Governo, dal canto suo, ha ottenuto un buon tornaconto: in cambio di questa concessione, infatti, continua ad avere il controllo sui prodotti[8], grazie alla possibilità di concedere o negare le licenze e, comunque, ad avere la conoscenza degli stessi in base al fatto che i produttori

[6] Ciò è testimoniato dal caso della Netscape: la società aveva sviluppato due versioni del *browser* « *Netscape navigator* ». Una era fruibile in rete e, quindi, scontava i vincoli all'esportazione, mentre l'altra garantiva una protezione maggiore, ma poteva essere acquistata solo negli Stati Uniti. Tutti si sono dotati, negli Stati Uniti, della versione destinata al mercato estero poiché l'altra versione garantiva un livello di riservatezza non condivisibile da chi si trovava all'estero.

[7] Il sistema delle licenze è particolarmente complicato, non mi addentro nelle specifiche tecniche e rimando al testo di legge: *Federal Register, 15 CFR Parts 734, 740, et al. Revisions to Encryption Items; Interim Final Rule.*

[8] Dotati di crittografia forte.

sono obbligati a consegnare le specifiche tecniche che rendono noto il funzionamento dei meccanismi di cifratura.

Prima di concludere l'analisi sugli *export controls*, vorrei accennare brevemente alle sanzioni che sono previste per chi non rispetti l'*Export Administration Act* (EAA) o gli *Export Administration Regulations* (EAR). La violazione, per colpa, dell'EAA o degli EAR comporta una sanzione che oscilla tra i $10.000 e i $100.000; se chi esporta era a conoscenza dei divieti (necessità della licenza o consegna delle specifiche tecniche o altro ancora) e non li ha rispettati, la sanzione non può essere superiore a 5 volte il valore dei prodotti esportati o $50.000 e sarà comminata quella più onerosa tra le due. In questo caso, però, è prevista anche una responsabilità penale che comporta una detenzione massima di 5 anni.

Chi, infine, viola l'EAA o gli EAR in modo premeditato, esportando i prodotti in regioni geografiche a rischio, sarà obbligato a corrispondere la somma maggiore tra 5 volte il valore dei prodotti esportati o $1.000.000. Inoltre è prevista, in aggiunta, una responsabilità penale che può dar luogo ad una detenzione massima di 10 anni.

Queste, in estrema sintesi, le sanzioni che possono essere comminate anche a chi non rispetta le disposizioni sull'esportazione di prodotti crittografici[9] e non sembrano essere particolarmente indulgenti.

Il caso Bernstein.

I regolamenti sulle esportazioni sono stati forieri di varie controversie giudiziarie. Sebbene alcune delle decisioni giurisprudenziali abbiano importanti ripercussioni costituzionali, il Governo non sembra essersene avveduto: l'emanazione degli *Export Administration Regulations* del 14 gennaio scorso costituiscono la prova più evidente.

Il caso che ha suscitato maggiore interesse è stato quello che ha visto come attore il Professor Daniel Bernstein che tiene un corso di *crittografia* presso l'Università dell'Illinois: questi aveva sviluppato un algoritmo di cifratura e lo voleva rendere pubblico insieme ad un volumetto, che ne consentiva una comprensione più agevole.

I regolamenti sulle esportazioni avevano, secondo Bernstein, impedito sia la pubblica discussione del suo algoritmo, sia anche la pubblicazione dello stesso; il risultato fu che « *he has been unable to advance his professional reputation and career by publishing and discussing his work with his professional peers and others.* »[10]. Questo è stato (ed è) il nodo dell'intera controversia: il Professore si lamentava dei vincoli sulle esportazioni di crittografia, sostenendo che questi limitavano la sua libertà di parola, secondo il dettato del Primo Emendamento. In altre parole, Bernstein affermava che il suo algoritmo, lo *Snuffle*, rappresentava una espressione personale e, come tale, doveva essere libera di poter essere veicolata in tutti i consessi che egli riteneva opportuno e con le forme (anche la stampa) che reputava più congeniali.

---

[9] Per maggiore completezza si veda il *Federal Register*, *15 CFR*, §764.3.

[10] Cfr. « *Bernstein complaint* » in Bernstein v. United States Dep't of State, 922 F.Supp. 1426 (N.D. Cal. 1996) (Bernstein I).

Il Giudice Patel dell'*U.S. District Court for the Northern District of California*, il 25 agosto del 1997, emise una sentenza, storica, a detta di molti, che si incentrava sulla incostituzionalità degli *Export Administration Regulations* (EAR). Nelle « *Conclusion* » si legge: « *For the aforementioned reasons, (...) the court declares that the Export Administration Regulations, 15 C.F.R. Pt. 730 et seq.(1997) and all rules, policies and practices promulgated or pursued thereunder insofar as they apply to or require licensing for encryption and decryption software and related devices and technology are in violation of the First Amendment on the grounds of prior restraint and are, therefore, unconstitutional as discussed above, and shall not be applied to plaintiff's publishing of such items, including scientific papers, algorithms or computer programs* »[11]. I motivi per i quali il Giudice giunse a tale decisione sono ben argomentati nella sentenza. Sostanzialmente, comunque, Patel ha riscontrato che, nel campo delle scienze applicate e, quindi, della crittografia, le idee non sono espresse in astratto, in termini teorici, ma, al contrario, vengono inserite all'interno di precise applicazioni come gli algoritmi. Sulla base di questa considerazione, il Giudice ha sottolineato che i vincoli, peraltro estremamente vaghi, all'esportazione, frustrano la possibilità di comunicare le proprie idee e di condividerle con gli altri: l'insegnamento, le videoconferenze e le discussioni su *internet*, intesi come strumenti per avviare un proficuo confronto, sono negati.

La vicenda non si concluse il 25 agosto poiché il Governo, tre giorni dopo, presentò ricorso presso la *Ninth Circuit Court of Appeals*: il 6 maggio del 1999 la Corte si è pronunciata.

La Corte ha affermato che « *Because the prepublication licensing regime challenged by Bernstein applies directly to scientific expression, vests boundless discretion in government officials, and lacks adequate procedural safeguards, we hold that it constitutes an impermissible prior restraint on speech. We decline the invitation to line edit the regulations in an attempt to rescue them from constitutional infirmity, and thus endorse the declaratory relief granted by the district court* »[12]. I Giudici, quindi, hanno dato fede all'interpretazione costituzionale di Patel affermando che « *the EAR regulations on encryption software were intended to slow the spread of secure encryption methods to foreign nations, the government is intentionally retarding the progress of the flourishing science of cryptography* ». Come si vede la Corte ha fatto riferimento alle disposizioni EAR nella loro interezza ed è per tale motivo che i Giudici hanno sentenziato « *To the extent the government's efforts are aimed at interdicting the flow of scientific ideas (whether expressed in source code or otherwise), as distinguished from encryption products, these efforts would appear to strike deep into the heartland of the First Amendment. In this regard, the EAR regulations are very different from content-neutral time, place and manner restrictions that may have an incidental effect on expression while aiming at secondary effects* »[13].

---

[11] Vedi — II. Prior Restraint — in Bernstein v. United States Dep't of State, 974 F.Supp. 1288 (N.D.Cal. 1997) (*Bernstein III)*.

[12] Cfr. CONCLUSION, in Bernstein v. United States Dept. of Justice et al.; F.3d (9th Cir.1999).

[13] Cfr. — C. Concluding comments — in Bernstein v. United States Dept. of Justice et al.; F.3d (9th Cir.1999).

L'affermazione è perentoria, oltre che estremamente chiara, ma una precisazione importante deve essere fatta e riguarda il *source code*. Il Professor Bernstein, infatti, aveva intentato la causa poiché il *Department of State*, prima, e il *Department of Commerce*, poi, gli avevano negato la possibilità di pubblicare il suo algoritmo *Snuffle*: la decisione dei Giudici, quindi, è relativa unicamente a questo algoritmo e non agli *object code* (vale a dire i programmi di cifratura). La puntualizzazione è d'obbligo perché l'incostituzionalità è stata riscontrata relativamente al caso di Bernstein e solamente per il suo algoritmo: le nuove disposizioni sulle esportazioni, infatti, prevedono che siano esportati solo alcuni *source code* e non tutti indistintamente.

Sebbene, quindi, la sentenza sia importante soprattutto per la presa di posizione relativa agli *export control*[14] ed al loro latente obiettivo di rallentare la diffusione della crittografia, il Presidente prima (in un documento del 16 settembre 1999[15]) e il *Department of Commerce* (con i regolamenti del 14 gennaio 2000) poi, hanno continuato ad insistere con le politiche dell'esportazione.

Il Governo (il *Department of Justice*), tuttavia, aveva presentato, il 21 giugno del 1999, una mozione[16] alla Corte d'Appello per far riesaminare il caso: la motivazione si basava sul fatto che i tre Giudici non erano stati tutti concordi[17]. La richiesta era stata accordata ed un gruppo di 11 Giudici della Corte d'Appello avrebbe dovuto riesaminare il caso. Poiché nel frattempo il *Department of Commerce* ha emanato, il 14 gennaio scorso, i nuovi regolamenti sulle esportazioni, il Professor Bernstein ha chiesto ed ottenuto che il caso tornasse ad essere dibattuto presso il Giudice di prima istanza (vale a dire presso la *U.S. District Court for the Northern District of California*).

In conclusione, possiamo sottolineare che il nodo gordiano della questione è rappresentato dall'algoritmo e soprattutto dal fatto che questo possa essere considerato *free speech* e ricadere nell'alveo del Primo Emendamento, oppure che possa considerarsi un *conduct* non ascrivibile tra le *personal expressions*. La vicenda di Bernstein, tuttavia, ha evidenziato anche che gli stessi regolamenti sulle esportazioni presentano caratteri di incostituzionalità. Vedremo se la Corte Suprema reciderà il nodo (che è, effettivamente, gordiano) con la stessa abilità della quale fu capace Alessandro Magno.

---

[14] Fra l'altro il Giudice Bright, il Giudice che insieme a Fletcher ha accolto le ragioni di Bernstein, ha invitato la Corte Suprema a prendere posizione sulla questione, poiché, pur non condividendo l'opinione del Giudice dissenziente Nelson, sottolineava che l'importanza del caso, oltre alla complessità dello stesso, necessitasse del giudizio della Corte Suprema Federale. Cfr. BRIGHT, Circuit Judge, separately concurring, in Bernstein v. United States Dept. of Justice et al.; F.3d (9th Cir.1999).

[15] Cfr. THE WHITE HOUSE, « *Preserving America's privacy and security in the next century: a strategy for America in cyberspace* », 16-9-1999.

[16] Cfr. PETITION FOR PANEL HEARING AND REHEARING EN BANC, No. 97-16686.

[17] « *The divided panel decision in this case presents compelling grounds for further review by this Court* »: queste le parole con le quali David Ogden, Acting Assistant Attorney General, giustificava la richiesta di un riesame.

3. La crittografia nel diritto internazionale.

L'ACCORDO DI WASSENAAR. Il Wassenaar Arrangement è un accordo internazionale, sottoscritto da 33 Paesi[18], il cui obiettivo è quello di limitare l'esportazione di armi convenzionali e di tecnologie « *dual-use* »[19] (tra le quali sappiamo rientrare la crittografia) verso Paesi 'a rischio'. Questo Accordo deriva da un altro, più datato, Agreement che aveva il nome di *Coordinating Committee on Multilateral Export Controls* (COCOM): il COCOM, nato all'alba del Patto di Varsavia, era stato sottoscritto da 17 Paesi allo scopo di impedire l'esportazione di prodotti crittografici verso i « *dangerous countries* ». Questi Paesi pericolosi erano quelli che si supponeva avessero dei legami con le organizzazioni terroristiche internazionali, alcuni dei quali erano la Libia, l'Iraq, l'Iran e la Corea del Nord. Tuttavia, il 16 novembre 1993 i rappresentanti di Governo delle 17 Nazioni firmatarie decisero che era giunto il momento di pensionare il vetusto accordo e di emanarne un altro allargando la partecipazione a molti altri Paesi: il 19 dicembre del 1995 è stato sottoscritto, da 28 nazioni, il Wassenaar Arrangement.

L'obiettivo principale è quello di rafforzare i controlli relativi al traffico di armi di distruzione di massa ed alle tecnologie *dual-use* nelle zone 'calde' del pianeta.

Un altro obiettivo, che costituisce un complemento del primo, è quello di promuovere, tra i Paesi firmatari, una maggiore cooperazione per prevenire l'acquisizione di armamenti e di tecnologie da Nazioni situate in regioni geografiche a rischio. A tal fine, viene ribadito nel testo, non c'è una preclusione *a priori* nei confronti di uno Stato o di un gruppo di Stati e non vengono impedite le « *bona fide civil transactions* »[20]. Si aggiunge anche che non si interferisce con il legittimo diritto degli Stati di acquistare armamenti per la difesa nazionale e ciò in ossequio all'articolo 51 della Carta delle Nazioni Unite.

Già da queste prime considerazioni possiamo osservare che l'accordo sembra essere una dichiarazione di intenti tra i Paesi firmatari in vista, unicamente, di una cooperazione che appare oltremodo fragile poiché viene demandata l'osservanza delle previsioni pattizie ad ogni singola Nazione senza prevederne obbligo alcuno.

Per ciò che riguarda il nostro oggetto di indagine dobbiamo, tuttavia, volgere lo sguardo alla *dual-use goods and technologies list*: in questa lista sono elencate tutte le applicazioni che possono avere usi militari, ma anche civili e, come sappiamo, la crittografia è tra queste. Nella lista, aggiornata periodicamente, vengono disciplinati i criteri per consentire o negare la licenza all'esportazione per i prodotti che sono in essa presenti. La - *Category 5 - Part 2* - della *Dual-use list*, denominata « *Information security* »,

[18] Più precisamente: Argentina, Australia, Austria, Belgio, Bulgaria, Canada, Repubblica Ceca, Danimarca, Finlandia, Francia, Germania, Grecia, Ungheria, Irlanda, Italia, Giappone, Lussemburgo, Olanda, Nuova Zelanda, Norvegia, Polonia, Portogallo, Repubblica della Corea, Romania, Federazione Russa, Repubblica Slovacca, Spagna, Svezia, Svizzera, Turchia, Ucraina, Regno Unito e Stati Uniti.

[19] Vale a dire dei prodotti che possono essere adoperati sia per usi civili che militari.

[20] Cfr. Initial Elements - I. Purposes (punto 4).

riguarda unicamente la crittografia. Il 3 dicembre del 1998 questa lista è stata aggiornata ed i punti principali possono essere così sintetizzati: tutti i prodotti a crittografia simmetrica fino a 56 *bit* e a crittografia asimmetrica fino a 512 *bit* sono liberamente esportabili. Così pure i prodotti destinati al mercato di massa dotati di crittografia simmetrica fino a 64 *bit*. Tutti gli altri prodotti crittografici, che garantiscono un livello di riservatezza maggiore poiché utilizzano chiavi di cifratura più lunghe di quelle considerate, richiedono una licenza all'esportazione. Questi sono i punti chiave dell'accordo che, tuttavia, non brillano né per chiarezza né, tantomeno, per completezza: non vengono elencati i prodotti ed inoltre c'è confusione nel delineare i criteri in base ai quali individuare le varie componenti crittografiche. Un punto che, forse, meriterebbe attenzione e che invece è stato tralasciato riguarda l'esportabilità dei prodotti attraverso *internet*: spigolando, infatti, tra le disposizioni non si trova traccia di alcuna regolamentazione del settore[21].

La puntualizzazione che, tuttavia, vorrei tracciare riguarda il carattere dell'Accordo di Wassenaar; in altre parole, come si può inquadrare questo patto fra gli strumenti del diritto internazionale? Si conforma un accordo di tal guisa alla regola *pacta sunt servanda* prevista dall'art. 26 della Convenzione di Vienna del 1980?

Ritengo che il Wassenaar Arrangement sia da ascriversi tra gli « accordi internazionali non vincolanti ». Una risoluzione, adottata il 29 agosto del 1983 dall'*Institut de Droit International*, riguardante i testi internazionali di questo tipo, così si esprime: « gli Stati adottano frequentemente, sotto diverse denominazioni, dei testi per mezzo dei quali accettano, nelle loro relazioni reciproche, degli impegni per i quali essi convengono, espressamente o implicitamente, che non abbiano carattere giuridico o il cui carattere e portata sono difficili da determinare. »[22]. Sembrerebbe, quindi, che l'accordo abbia un carattere eminentemente politico e che, in caso di non osservanza, non generi alcuna responsabilità internazionale. È, comunque, importante soffermarsi sul fatto che il Wassenaar Arrangement non può essere codificato come un trattato internazionale e neppure come una legge applicabile agli Stati firmatari dell'accordo.

Possiamo quindi affermare che la sua funzione effettiva è solamente quella di scambiare, tra i partecipanti che si uniscono in periodici consessi viennesi[23], dei punti di vista e delle informazioni circa il traffico internazionale di armi e di *dual-use goods and technologies*. Il fatto che gli Stati convergano nell'adottare delle politiche sull'esportazione, non implica automaticamente che ci sia un obbligo di cristallizzare tali previsioni in successive legislazioni nazionali: tale eventualità sembra essere assolutamente discrezionale e facoltativa. Questo per testimoniare l'importanza di tale accordo e della sua (non)osservanza sulla scena internazionale.

---

[21] Negli Stati Uniti, infatti, le controversie giudiziarie relative alla crittografia, che vedono come attori, oltre al Professor Bernstein, il programmatore Philip Karn ed il Professor Peter Junger, ruotano attorno alla mancata concessione di pubblicare in rete i programmi di cifratura.

[22] Cfr. GIULIANO, SCOVAZZI, TREVES, *Diritto Internazionale* - Parte Generale - Giuffrè, Milano 1991.

[23] È lì infatti che risiede il Secretariat del Wassenaar Arrangement.

OECD - Guidelines for cryptography policy. L'*Organization for Economic Cooperation and Development* è un organismo internazionale, istituito nel 1960 e composto dai rappresentanti di 29 Paesi, che ha tra gli obiettivi quello di promuovere il commercio internazionale e liberalizzare il flusso dei capitali, rimuovendo tutti gli ostacoli che impediscano il raggiungimento di tali fini. La crittografia si innesta in quest'ultima previsione poiché rappresenta, anche, uno strumento di particolare importanza nello sviluppo di un'architettura di sicurezza nella quale possa inserirsi il commercio elettronico.

Nel 1996, infatti, si costituì un gruppo di studio, composto da rappresentanti governativi, personale delle *law enforcement agencies*, emissari dei settori del commercio, dell'industria e del settore privato, il cui compito era quello di esaminare le politiche crittografiche adottate dai Paesi membri dell'OECD e quindi, grazie agli strumenti comparatistici, di rintracciare una *policy guideline*. Gli Stati Uniti erano rappresentati da personale dell'FBI, della NSA e del *Department of Justice*: l'attività intrapresa dai funzionari americani era quella di costringere l'OECD ad adottare il meccanismo di *key escrow* quale *standard* internazionale. Questa posizione era osteggiata da vari Paesi: il Ministro del Commercio e dell'Industria Giapponese si opponeva fermamente ai *dictat* nordamericani (supportati dai Francesi e dagli Inglesi); i Paesi Scandinavi affermarono che un qualsiasi meccanismo di *key escrow* avrebbe frustrato la fiducia che occorre nel commercio internazionale, ma soprattutto nel costituendo commercio elettronico. I rappresentanti del settore privato sottolinearono l'esigenza ed il diritto di poter scegliere qualsiasi sistema di protezione che risultasse loro maggiormente conveniente. Poiché l'*empasse* non ha trovato una adeguata soluzione, il risultato si è tradotto in un accorciamento dei tempi di studio ed in *guidelines* che lasciano ampia possibilità di scelta dei sistemi da adottare, compresi quelli di *key escrow*.

COUNCIL OF EUROPE. Il Consiglio d'Europa è un'organizzazione internazionale fondata il 19 dicembre 1954 tra 14 Paesi che nel tempo sono diventati 41. Il compito principale di questo organismo è quello di rafforzare la democrazia, far rispettare i diritti umani e promuovere l'adozione di legislazioni uniformi tra gli Stati membri. Il documento più importante, ad oggi prodotto relativamente alla crittografia, è stata la *Recommendation R (95) 13 Concerning Problems of Criminal Procedure Law Connected with Information Technology* dell'8 settembre 1995. Nel secondo paragrafo del testo si sottolinea l'esigenza di dotare gli organi di polizia, nazionali ed internazionali, di tutti gli strumenti tecnici che possano coadiuvare le attività investigative indirizzate alla lotta al crimine. A tal fine, il documento si dilunga — era il 1995 — nell'evidenziare che la mancanza di appropriati sistemi informatici da destinare alle *law enforcement agencies* può rendere impari il 'confronto' con le organizzazioni criminali internazionali, le quali sono sempre pronte a dotarsi delle tecnologie più avanzate. I contenuti di questa *recommendation* sono estremamente vaghi poiché non si esplicita né quali siano le misure concrete per consentire alle *law enforcement agencies* di portare a termine con successo le indagini investigative, né come si debba trovare il bilanciamento tra il diritto alla riservatezza dei cittadini ed i diritti e doveri degli organi di polizia. In altre parole, non si affronta il problema sollevato dai meccanismi di *key escrow*. Siccome, però, il Consiglio d'Europa non ha tra i suoi membri gli Stati Uniti, la scelta di limitare l'uso di crittografia forte — questo sembra essere

il significato della *recommendation* — fa allertare i sensi in modo preoccupante. Tuttavia, mi permetto di aggiungere che il Consiglio non ha l'autorità di rendere obbligatorie le sue raccomandazioni, anche se è raro che queste vengano rigettate dai Paesi membri.

4. L'UNIONE EUROPEA.

Le disposizioni comunitarie disciplinano unicamente l'esportazione di crittografia, che ha i suoi due pilastri legislativi nella « *Council Regulation (EC) No. 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods* » e nella « *EU Council Decision No. 94/942/CFSP* ».

Ambedue i documenti sono stati approvati il 19 dicembre del 1994 e sono in vigore dal 1 luglio del 1995. Queste norme comunitarie sono direttamente applicabili ai Paesi dell'Unione Europea non solo perché sono fonti primarie (per le quali la nostra Costituzione prevede un obbligo di adattamento automatico del diritto interno), ma anche perché la Corte di giustizia si è pronunciata due volte, nell'ottobre del 1995, affermando che la Comunità Europea ha una giurisdizione esclusiva per ciò che riguarda queste materie.

Il regolamento del Consiglio sappiamo essere obbligatorio in tutti i suoi elementi ed è « direttamente applicabile in ciascuno degli Stati membri » (art. 189, 2° comma del Trattato CE).

L'obiettivo del *Council Regulation (EC) No. 3381/94* è quello che si legge in uno dei paragrafi iniziali « *this system represents a first step towards the establishment of a common system for the control of exports of dual-use goods which is complete and consistent in all respects; (…) it is desirable that the authorization procedures applied by the Member States should be harmonized progressively and speedily* »[24]. Il testo di legge non si occupa di individuare tutto ciò che può costituire *a dual-use good* (questo ruolo è demandato all'altro documento), al contrario cerca di definire un complicato sistema di licenze, valido sia per le esportazioni tra i Paesi facenti parte della Comunità, sia per quelle indirizzate verso i Paesi non membri. In sostanza, si prevedono tre tipi di licenze: *individual*, *global* e *general*, a seconda del bene che si vuole esportare e del luogo di destinazione. Per ciò che riguarda l'esportazione di *dual-use goods* verso Paesi facenti parte dell'Unione Europea è necessario munirsi di una licenza generale rilasciata da una competente autorità del proprio Paese: questo documento, consegnato senza effettuare particolari controlli, permette di esportare quasi tutti i tipi di beni con la caratteristica di avere utilità sia civile che militare.

Se ora proviamo a leggere l'altro documento, che è, in pratica, una lunghissima lista di prodotti, ci accorgiamo che la crittografia è presente in quel paragrafo denominato *Annex I*. Al punto 31, infatti, si afferma che « *Cryptography means the discipline which embodies principles, means and methods for the transformation of data in order to hide its informa-*

[24] Cfr. *Council Regulation (EC) No. 3381/94.*

tion content, prevent its undetected modification or prevent its unauthorized use. "Cryptography" is limited to the transformation of information using one or more secret parameters (e. g. crypto variables) or associated key management »[25]. Come si vede, l'accezione che si dà della crittografia è quella che a noi interessa, vale a dire di uno strumento che consente di rendere incomprensibile una comunicazione attraverso una qualsiasi trasformazione alfanumerica.

La *decisione* del Consiglio consiste, come abbiamo già detto, in una lunghissima lista di prodotti, sottoposti alle disposizioni del regolamento tra i quali figura, nel paragrafo *Annex I*, la crittografia: la *decisione* corrisponde, in sostanza, all'atto amministrativo dei sistemi giuridici nazionali e rappresenta, anche in questo caso, lo strumento utilizzato dal Consiglio per applicare il diritto comunitario a fattispecie concrete.

Comunque, poiché la crittografia è inserita nella lista dei beni che necessitano di licenza all'esportazione, sia all'interno che all'esterno dell'Unione, chiunque voglia esportare un prodotto crittografico, sia *hardware* che *software*, deve procurarsi una « *general licence* ». Analogo tipo di licenza — che è quella che prevede un numero minore di adempimenti e che viene più facilmente rilasciata — è prevista per l'esportazione di prodotti crittografici verso sette « *friendly countries* »: Australia, Canada, Giappone, Nuova Zelanda, Norvegia, Svizzera e Stati Uniti.

Queste, in linea di massima e senza addentrarmi troppo nelle specifiche tecniche dei 24 articoli che costituiscono la *Council Regulation 3381/94*, le indicazioni da seguire per l'esportazione di crittografia: l'unica eccezione, che prevede non si debba avere alcuna licenza, è stabilita per il *mass-market and public-domain software*.

Tuttavia, il 28 maggio del 1998, la Commissione ha prodotto un documento noto come « *Report to the european parliament and the council on the application of regulation (EC) 3381/94 setting up a community system of export controls regarding dual-use goods* », nel quale viene bocciato il sistema vigente prevedendo che si debbano introdurre nuovi e più agili meccanismi per consentire l'esportazione dei prodotti, ivi compresi quelli crittografici. Il documento è importante perché, oltre a puntare il dito contro le storture e le difficoltà di cui sono stati forieri gli attuali regolamenti, apre la strada ad una nuova proposta denominata « *Proposal for a Council regulation (EC) setting up a Community regime for the control of exports of dual-use goods and technology* »[26]. Prima di vedere come si sostanziano le differenze — ribadisco comunque che quest'ultima è solo una proposta — gradirei rilevare le deficienze dell'odierno regime delle esportazioni, coadiuvato, in questo compito, dall'analisi svolta dalla stessa Commissione Europea.

La lacuna maggiore, che ha mostrato l'attuale regime e che ha contribuito a creare l'odierno stato di *empasse*, è rappresentata dal fallimento dell'obiettivo primario della *Council Regulation 3381/94*: come ho già sot-

[25] Cfr. « *94/942/CFSP: Council Decision of 19 December 1994 on the joint action adopted by the Council of the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods* ».

[26] Cfr. COMMISSION OF THE EUROPEAN COMMUNITIES, Brussels, COM(1998) 257 final 98/0162 (ACC).

tolineato, il ruolo principale di questa legge era quello di incentivare una armonizzazione delle legislazioni nazionali sulle esportazioni. Ma, come recita il documento della Commissione Europea, « *In terms of harmonisation of policies, the legislation is limited to the strict minimum necessary to allow free movement of dual-use goods inside the Community. The system does not constitute a common export policy for dual-use goods. It is a common framework, but for national policies which continue to differ, in some aspects significantly* ». Cosa direbbe René David a tal proposito? Forse penserebbe che un '*droit commun de la cryptographie*' sarebbe auspicabile almeno fra i Paesi membri dell'Unione Europea.

Ma su questo punto il rapporto della Commissione è ancora più preciso perché afferma « *The Regulation and the way it has been applied in practice has not succeeded in creating an effective common export control regime which is both easy to administer and cost-effective to comply with. In particular, due to an insufficient convergence of national policies and practices, the system is too complex to be routinely enforced by customs with a sufficient degree of automaticity* »[27]. Il documento si dilunga anche nel sottolineare che molte aziende, ascoltate nel 1996 da un *Coordinating Group* della Commissione, hanno evidenziato che trovavano difficile, ed a volte impossibile, operare in modo economicamente efficiente con una legislazione sulle esportazioni così farraginosa. Le difficoltà sono ascrivibili a tre fattori: le differenze nelle legislazioni nazionali, la presenza della *catch-all clause* ed, infine, i problemi di carattere amministrativo.

Per ciò che riguarda il primo aspetto, la Commissione Europea così si esprime: « *The problem is one of delays at borders because customs officials do not know the licensing systems of other Member States, and therefore need to make inquiries about the validity of a given export authorization. Many exporters have concluded from such delays that the system is actually inapplicable and have become reluctant to export from one Member State with a licence provided by another, because even if the licence is ultimately recognized and the export finally goes ahead, the loss of time incurred is far too costly* »[28]. Non credo sia opportuno aggiungere dei commenti poiché è la Commissione stessa che stigmatizza in modo chiaro il suo pensiero.

Il secondo motivo di difficoltà riguarda la *catch-all clause*: in altre parole, la *Council Regulation 3381/94* prevede che qualsiasi bene debba essere soggetto ad una licenza che ne autorizzi l'esportazione qualora colui che esporta il prodotto venga informato — dalle autorità del suo Paese — o sia a conoscenza[29] che il bene potrebbe essere utilizzato in relazione ad un ipotetico programma sovversivo. Non mi dilungo nell'analizzare questo aspetto, che ha introdotto ulteriori motivi di difficoltà, e do evi-

---

[27] Cfr. « Deficiencies and problem areas » in « *Report to the european parliament and the council on the application of regulation (ec) 3381/94 setting up a community system of export controls regarding dual-use goods* », Bruxelles, 28 maggio 1998.

[28] Cfr. « *Report to the european parliament and the council on the application of regulation (ec) 3381/94 setting up a community system of export controls regarding dual-use goods* », Bruxelles, 28 maggio 1998.

[29] Nella legge si utilizza la parola *aware* senza ulteriori precisazioni. Cfr. art. 4, punti 1 e 2.

denza dell'ultimo ingranaggio che non ha funzionato, vale a dire la cooperazione tra le strutture amministrative nazionali. Volendo, si può considerare quest'ultimo punto come un corollario del primo: gli uffici preposti alla concessione delle licenze hanno operato come cellule separate l'una dalle altre, interpretando i regolamenti in modo differente e senza avviare quel processo di mutua assistenza che sarebbe stato necessario per un più corretto svolgimento dei traffici economici[30].

Queste difficoltà hanno spinto la Commissione ad avanzare la proposta che dovrebbe sostituire l'attuale *Council Regulation 3381/94*, vale a dire la « *Proposal for a Council regulation (EC) setting up a Community regime for the control of exports of dual-use goods and technology* ». Il nuovo regolamento sarebbe dovuto entrare in vigore il 1 gennaio del 1999, ma, ad oggi, non si è ancora raggiunto un accordo fra i Paesi dell'Unione per consentire il passaggio del testimone della politica delle esportazioni per i *dual-use goods*. Ciò detto, la proposta mutua molti dei 26 articoli dei quali è composta la *Council Regulation 3381/94*. Per l'esportazione di crittografia dovrebbe essere necessaria una *notification* e non l'ottenimento di una licenza. Poiché, però, si fa riferimento unicamente alla crittografia utilizzata per le applicazioni bancarie e commerciali, mentre non viene presa in considerazione la crittografia adoperata per le ordinarie comunicazioni, forse, per quest'ultima, non sembrerebbe bastare una semplice *notification*.

Questo è, in estrema sintesi, lo stato dell'arte a livello comunitario. Devo tuttavia aggiungere che gli studi[31], i *meeting* e gli incontri, sia a livello nazionale che comunitario, sono stati improntati da una certa approssimazione. Un possibile nucleo comune, che si può rintracciare da una disamina più approfondita, mette in evidenza due aspetti particolarmente preoccupanti: il primo è che sembrerebbe sussistere una *liaison* tra la crittografia ed i sistemi di *key escrow*; il secondo è che si fa riferimento, quasi sempre, alla crittografia come strumento utile per il commercio elettronico o per il commercio in sé[32].

---

[30] Per maggiori delucidazioni vedi « *Problems of administrative cooperation* » in « *Report to the european parliament and the council on the application of regulation (ec) 3381/94 setting up a community system of export controls regarding dual-use goods* », Bruxelles, 28 maggio 1998.

[31] Tra il 1996 e il 1997 la Commissione Europea ha pubblicato cinque rapporti nei quali si discettava anche di crittografia. Cfr. Ake Nilson, *Final report — european trusted services (ets) — RESULTS OF 1995 TTPS PROJECTS*, Marinade Limited, aprile 1997; Despina Polemi, « *Biometric techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable* »,*institute of communication and computer systems national technical university of athens*, aprile 1997; ISTEV, « *Legal and Regulatory Issues for the European Trusted Services Infrastructure - ETS*, giugno 1997; HARTMUT POHL, « *Guidelines for the Use of Names and Keys in a Global TTP Infrastructure* », ISIS - Institute for Information Security, Essen, Germany, maggio 1997; infine ANDREW COLLERAN, « *Final report — Standardisation Issues for the European Trusted Services* — ETS », maggio 1997.

[32] Nel senso che si considera la crittografia proficua in quanto è essa stessa un prodotto all'interno di un mercato in forte crescita. Il riferimento è diretto al convegno ministeriale europeo dal titolo « *Global Information Networks: Realising the Potential* », organizzato congiuntamente dalla Repubblica federale tedesca e dalla Commissione europea e tenutosi a Bonn il 6,7 e 8 luglio del 1997; ai *meeting* del G-8 di Lione del 1996 e di Birmingham del 18 maggio 1998; infine al Copenhagen Hea-

Anche a livello nazionale la situazione è quanto mai confusa: appare comunque evidente che i Governi che hanno cercato di metter mano alla materia[33] si sono trovati di fronte ad un dilemma: qualunque sia la strada che si intende percorrere ci sono buone ragioni per pentirsene. Se si optasse per i meccanismi di *key escrow* l'impopolarità sarebbe evidente, poiché i lai dei cittadini non tarderebbero a farsi sentire. Se, al contrario, si scegliesse di imboccare un sentiero che andasse nella direzione di non prevedere la condivisione della chiave privata con alcuna agenzia, si dovrebbe escogitare un metodo efficace per consentire alle *law enforcement agencies* di accedere ai testi in chiaro (in presenza, ovviamente, di adeguati mandati di intercettazione). Accedere alle comunicazioni cifrate in tempi brevi e senza disporre della chiave privata è effettivamente cosa ardua. Nel galleggiare, quindi, tra questi due approcci, i Governi si sono astenuti dall'intraprendere un percorso deciso e definitivo.

Perfino l'Inghilterra si è trovata in difficoltà, stretta da una parte dalla madre patria e, quindi, dai sistemi di *key escrow*, e dall'altra dall'impopolarità che conseguirebbe scegliendo quel tipo di approccio, anche e soprattutto se l'Unione Europea dovesse adottare una soluzione differente.

Stagnante questo *status quo*, riuscire a rintracciare degli spigoli nelle confuse posizioni crittografiche nazionali necessita di una spiccata capacità di preveggenza.

Penso, allora, che la soluzione arriverà dalle istituzioni comunitarie che però non sembrano avvedersi della questione *crittografia* nella sua globalità poiché sono concentrate soprattutto sulle ripercussioni economiche. Mi rendo conto che il problema è spinoso, ma credo sia necessario, oltre che urgente, pervenire ad una soluzione[34].

Per quanto riguarda i criminali, in virtù dei quali vengono giustificati i sistemi di *key escrow*, non credo che essi si doteranno di tali meccanismi consegnando la loro chiave privata ad una terza parte o che sposeranno i sistemi (qualsiasi essi siano) che a livello nazionale od internazionale verranno propugnati. In quest'ultimo caso, anche se degli organi indipendenti dovessero testare l'affidabilità degli algoritmi promuovendone la relativa sicurezza ed assicurando l'assenza di *back-doors*, non penso che terroristi, trafficanti e manigoldi di vario genere e grado riporranno la loro fiducia nelle istituzioni che si adoperano per la legalità (la crittografia viene, infatti, maneggiata, in tutto il mondo, da strutture di *intelligence* addette alla sicurezza nazionale).

Mi limito, infine, a citare due punti della *European Council Resolution on the lawful interception of telecommunications (96/C329/01)*: questa Risoluzione del Consiglio Europeo rappresenta un viatico per le *law enforce-*

---

ring, incontro promosso dalla Commissione Europea e tenutosi a Copenhagen il 23 e 24 aprile del 1998 tra vari esperti del settore per discutere di firma digitale e crittografia.

[33] Soprattuto la Francia (che fra l'altro ha ammorbidito notevolmente, negli ultimi due anni, le norme sull'uso di crittografia), l'Inghilterra, la Germania, la Svezia e l'Olanda.

[34] Fra l'altro, nell'agenda dei lavori del Consiglio dei Ministri degli Esteri, riunitisi il 22 maggio scorso, era stato previsto di discutere della crittografia e delle difficoltà apportate dal Regolamento del Consiglio n. 3381/94 per avviare quel cambiamento che la Commissione Europea ha indicato già da qualche anno. All'ultimo momento, però, l'argomento crittografia è stato cancellato dall'ordine dei lavori mettendo in evidenza che le 'pressioni' statunitensi hanno sortito il loro effetto.

ment agencies delle varie nazioni poiché fornisce le linee guida alle quali attenersi per ammodernare le strutture tecnologiche che consentono di effettuare le intercettazioni nei moderni sistemi di telecomunicazione. Al punto 2 dei « *Requirements* » si legge che « *Law enforcement agencies require a real-time, fulltime monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination* ». Mentre qualche riga più oltre possiamo evidenziare che « *If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair* »[35]. Le parole « *en clair* » sollevano qualche preoccupazione perché aprono la strada ai meccanismi di *key escrow*. Affermare che deve essere possibile, in tempo reale, accedere alle comunicazioni, in chiaro, vuole significare che deve essere istituito un sistema che eviti il processo di decrittazione e che, al contrario, consenta di decifrare il messaggio con la giusta chiave. Gli auspici non sembrano dei migliori.

5. La crittografia in Italia.

Già siamo a conoscenza che l'esportazione di crittografia (in ambito comunitario) ha i suoi due presidi legislativi nella « *Council Regulation (EC) No. 3381/94 of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods* » e nella « *EU Council Decision No. 94/942/CFSP* ». Sappiamo che, ovviamente, tutti i Paesi membri fanno riferimento a questi due atti del Consiglio e che, però, le integrazioni apportate dalle legislazioni nazionali al regolamento, per puntualizzare le modalità di applicazione, hanno creato numerosi problemi che hanno depresso il commercio.

In Italia, la norma che integra il regolamento comunitario è il decreto legislativo n. 89 del 24 febbraio 1997 — Attuazione del regolamento CE n. 3381/94 e della decisione n. 94/942/PESC, sull'esportazione di beni a duplice uso — il quale individua, nel Ministero del Commercio con l'Estero, la struttura amministrativa detentrice del potere di negare o autorizzare l'esportazione dei *dual-use goods*. A tal fine viene creato (articolo 5) un Comitato consultivo, l'organo che si occupa direttamente delle questioni tecniche, che esprime un « parere obbligatorio ma non vincolante ai fini del rilascio, diniego, annullamento, revoca, sospensione e modifica delle autorizzazioni ».

Non credo si debba aggiungere molto altro su questo decreto legislativo, oltre al fatto che « chiunque effettua operazioni di esportazione di beni a duplice uso senza la prescritta autorizzazione ovvero con autorizzazione ottenuta fornendo dichiarazioni o documentazioni false, (...) è punito

[35] Cfr. « *Requirements* » (punto 3), European Council Resolution on the lawful interception of telecommunications (96/C329/01).

con la reclusione da due a sei anni o con la multa da lire cinquanta milioni a lire cinquecento milioni. »[36].

Per ciò che riguarda l'esportazione di prodotti crittografici, quindi, il mosaico è sufficientemente chiaro; se, invece, proviamo a rintracciare la tassonomia relativa all'uso ed all'importazione di crittografia[37], il quadro diventa incerto poiché vi è solo qualche vago accenno in alcuni testi di legge.

La parola *crittografia* la troviamo, ad esempio, nella l. 23 dicembre 1992, n. 522 — Ratifica ed esecuzione dell'accordo tra gli Stati membri delle Comunità europee sulla semplificazione e la modernizzazione delle modalità di trasmissione delle domande di estradizione, fatto a Donostia-San Sebastian il 26 maggio 1989 —. All'articolo 2 si legge che « La richiesta di estradizione ed i documenti di cui al paragrafo 1 dell'articolo 1 possono essere trasmessi a mezzo telefax (...) ». Subito dopo, all'articolo 3, si stabilisce che « per garantire sia l'origine che la riservatezza della trasmissione, si ricorrerà ad un crittografo adattato al telefax dell'autorità competente ai sensi dell'articolo 1 quando tale apparecchiatura sia utilizzata per l'applicazione del presente accordo ». Come si vede, si fa riferimento sia all'*origine* che alla *riservatezza* della trasmissione: il primo termine riconduce all'autenticazione degli interlocutori, vale a dire alla possibilità di accertare che colui il quale dichiara essere l'autore del documento sia effettivamente il legittimo mittente e non altri che abusivamente ne utilizzi l'identità. Tale funzione è propria della firma digitale e non implica la segretezza della comunicazione che, invece, è garantita dal termine *riservatezza*.

Sembra, comunque, che l'Ufficio II — Direzione Generale per gli affari penali delle Grazie e del Casellario — del Ministero di Grazia e Giustizia, la struttura che si occupa delle estradizioni, invii la documentazione per mezzo della Polizia ferroviaria senza usufruire di alcun *telefax*-crittografo.

Un ministero che, al contrario, usufruisce di un centro cifra funzionante è il dicastero degli affari esteri. L'articolo 24 del Decreto del Presidente della Repubblica del 5 gennaio 1967, n. 18, recita: « Il Ministro, sentito il Consiglio di amministrazione, stabilisce con suo decreto le norme per l'organizzazione e il funzionamento dei servizi tecnici e in particolare di quelli concernenti la cifra e le telecomunicazioni, gli archivi, la copia e riproduzione, (...). ».

All'articolo 85 si legge che « L'Amministrazione degli affari esteri è dotata di apparecchiature per la cifra e la crittografia atte a tutelare la segretezza delle comunicazioni fra il Ministero e gli uffici all'estero. L'Amministrazione degli affari esteri è altresì fornita di apparecchiature per telecomunicazioni, nonché dei relativi impianti ausiliari per il loro autonomo funzionamento atti ad assicurare rapidi e costanti collegamenti tra il Ministero e gli uffici all'estero (...) ». Il Decreto Ministeriale del 25 marzo 1968 — Organizzazione e funzionamento del centro cifra e telecomunicazioni del Ministero degli affari esteri — è l'atto a cui fa riferimento l'articolo 24 della legge testé 'analizzata'.

---

[36] Art. 7, comma 1.

[37] Nell'accezione di strumento che serve per garantire la riservatezza.

Il centro è diviso nel reparto cifra ed in quello crittografico: il reparto cifra provvede alla cifratura ed alla decifrazione dei telegrammi, attenendosi alla lettera della legge, ma sembra che il Ministero si stia attrezzando anche per garantire la riservatezza delle comunicazioni telematiche.

Il reparto crittografico, invece, assolve più compiti poiché studia e sceglie le attrezzature destinate alla cifra e alle telecomunicazioni fra il Ministero e gli uffici all'estero; provvede alla conservazione, al controllo e alla distribuzione delle attrezzature di cifra e telecomunicazioni e alla produzione, ove necessario, del materiale d'impiego ad esse relativo; il reparto provvede altresì alla compilazione, alla preparazione e all'aggiornamento dei codici e delle tabelle. Come si comprende, il Ministero degli Esteri è un polo crittografico importante non solo perché fa largo uso di sistemi di cifratura per garantire la riservatezza delle comunicazioni tra Roma e le ambasciate dislocate in tutto il mondo, ma anche perché studia, sceglie e produce i mezzi per assolvere questa delicata operazione.

La crittografia viene regolata anche in relazione all'esercizio dell'attività di radioamatore. Il Decreto del Presidente della Repubblica 5 agosto 1966, n. 1214 — Nuove norme sulle concessioni di impianto e di esercizio di stazioni di radioamatori — all'articolo 10 recita: « Le radiocomunicazioni fra stazioni di radioamatore devono essere effettuate in linguaggio chiaro e solo nella lingua italiana, francese, inglese, spagnola, tedesca e russa. È ammesso l'impiego del 'Codice Q' e delle abbreviazioni internazionali previste dall'I.A.R.U. (*International Amateur Ragio Union*) ». Le disposizioni sono, nel complesso, particolarmente restrittive: innanzitutto si vieta l'uso di tecniche di cifratura, eccezion fatta per il datato « Codice Q ». Inoltre, viene limitato il tipo di comunicazioni che è possibile effettuare: è consentito scambiarsi messaggi riguardanti unicamente aspetti tecnici, con i relativi commenti personali, che per di più vengono stigmatizzati con le parole « scarsamente importanti ».

Lo Stato fa, al contrario, largo uso di crittografia: nell'ambito, infatti, dell'attività del Comitato interministeriale per le informazioni e la sicurezza (CIIS), disciplinato dal D.P.R. 20 dicembre 1994, n. 756, viene istituita l'Autorità nazionale per la sicurezza e per la protezione delle informazioni coperte da segreto di Stato (ANS). Il compito di questa autorità è quello di gestire i codici, con le relative chiavi, utilizzati nei vari livelli della Pubblica Amministrazione; inoltre l'ANS deve assicurarsi che « l'integrazione e l'interconnessione dei sistemi informativi automatizzati degli Organismi deve avvenire secondo le procedure di sicurezza previste dall'ANS per i sistemi informatici che gestiscono informazioni classificate »[38].

Possiamo dire, quindi, che per ciò che riguarda le esigenze di segretezza e riservatezza sia del segreto di Stato, sia dei sistemi di comunicazione adoperati nelle alte sfere, bisogna attenersi alle disposizioni tecniche appositamente impartite dall'ANS, anche per la crittografia.

Il mondo bancario non poteva non dotarsi di un sistema di sicurezza basato sulla crittografia. L'articolo 8 del Decreto Ministeriale del 12 dicembre 1994, stabilisce, infatti, che « Al fine di garantire l'integrità e la riservatezza dei dati trasmessi attraverso la rete nazionale interbancaria, ver-

[38] Cfr. art. 3, comma 2 del D.P.R. 11 novembre 1994, n. 680. Vedi anche la l. 24 dicembre 1993, n. 537: articolo 1, comma 25.

ranno scambiate chiavi bilaterali di autenticazione e crittografia tra operatori e Banca d'Italia (...) ». Analoghe disposizioni sono presenti in altri Decreti Ministeriali[39] e lasciano pensare che sia in uso un sistema di cifratura simmetrico poiché il termine « bilaterale », al quale fanno riferimento tutti i Decreti, credo significhi che la stessa chiave venga adoperata sia dalla Banca d'Italia che dagli operatori[40].

Ulteriori, vaghe disposizioni relative all'uso di cifratura sono contenute nel Decreto del Presidente della Repubblica del 27 marzo 1992, n. 313 — Regolamento del servizio telex, in attuazione del libro quarto, titolo II, capo II, del testo unico delle disposizioni legislative in materia postale, di banco-posta e di telecomunicazioni, approvato con decreto del Presidente della Repubblica 29 marzo 1973, n. 156 —.

La legge disciplina l'abbonamento al servizio *telex* da parte di utenti privati, siano essi persone fisiche o giuridiche. All'articolo 10 si legge che « È consentito all'abbonato lo scambio di corrispondenza anche in linguaggio criptografico. In tal caso, l'abbonato ha l'obbligo di darne preventiva comunicazione all'Amministrazione ».

Quelle fin qui analizzate sono tutte le leggi nelle quali è presente un accenno, spesso vago, alla cifratura: il quadro che si ottiene è comunque molto confuso. Possiamo tuttavia dire che non sussistono particolari limitazioni, eccetto che per i radioamatori, all'uso di cifratura da parte dei cittadini: non sono state, infatti, regolamentate né le tecniche di cifratura per la telefonia, né quelle relative ad *internet*.

Lo Stato, al contrario, fa largo uso di sistemi crittografici per proteggere le sue informazioni: non credo, comunque, che il nostro Parlamento interverrà per regolare l'uso di crittografia entro i patri confini. Ritengo più probabile, oltre che più opportuno dal punto di vista giuridico, che gli organi comunitari si adoperino per effettuare l'agognata rivoluzione copernicana crittografica, emanando delle disposizioni comuni a tutti gli Stati membri ed evitando che questi ultimi possano integrarle creando un altro sistema nebuloso, incerto e poco snello.

---

[39] Cfr. D.M. 5 dicembre 1996 - Emissione buoni ordinari del Tesoro al portatore a partire dall'esercizio finanziario 1997 —; D.M. 28 agosto 1998 - Norme per l'emissione di buoni ordinari del Tesoro al portatore —; D.M. 19 dicembre 1998 - Modalità di emissione dei buoni ordinari del Tesoro al portatore a partire dal 1 gennaio 1999.

[40] Sembra comunque che la rete interbancaria difetti di adeguati presidi di sicurezza e che la Banca d'Italia si stia adoperando per ridurre la debolezza delle vie percorse dagli ordini di acquisto e vendita.