V. Rizzo (a cura di), "Documento informatico, firma digitale e commercio elettronico"
Collana ITTIG-CNR, Serie "Studi e documenti", n. 2, Napoli, ESI, 2000, pp. 101-110

La crittografia è un'arma? Il difficile bilanciamento fra diritti individuali e interessi pubblici

ANDREA MONTI[1]

SOMMARIO: *1. Premessa - 2. Alcune definizioni - Gli ambiti di applicazione - 3.1. La tutela della proprietà intellettuale - 3.2. I contratti on-line - La sicurezza nazionale.*

1. PREMESSA

Questo intervento poco avrà di giuridico e molto di politico, perché su una materia così delicata come la regolamentazione della crittografia il legislatore ha certamente "saltato un passaggio". Nel senso che si è immediatamente proiettato[2] ad affrontare una serie di questioni tecniche[3], ma non ha compiuto una scelta di fondo: quella di stabilire un quadro di riferimento organico che tenesse conto sia degli aspetti di rango costituzionale, sia di quelli legati all'impatto sul sistema normativo ordinario.

Esposto sinteticamente il punto di partenza del ragionamento, prima di procedere oltre, e per inquadrare correttamente i termini del problema, si rende necessaria un'altrettanto sintetica ma importante definizione terminologica.

L'esiguità degli spazi a disposizione impone di dare per scontata una conoscenza - peraltro ormai diffusa - dei fondamenti sul funzionamento della crittografia e di limitarsi a ricordare che con questo termine si intende quella branca della matematica che studia i sistemi per rendere non comprensibile un messaggio a chiunque non sia in possesso della chiave per "svelare l'arcano".

---

[1] lawfirm@andreamonti.net

[2] probabilmente, sulla spinta del regime dell'emergenza che caratterizza ora mai la produzione normativa in àmbito informatico.

[3] Come per esempio l'introduzione della firma digitale e delle relative norme tecniche, il regolamento sulle misure minime di sicurezza per la legge sui dati personali (che contribuisce ad elevare la crittografia ad un rango estremamente elevato nell'àmbito delle problematiche giuridiche).

2. ALCUNE DEFINIZIONI

Dato un testo in chiaro, cioè il testo comunemente intelligibile, si chiama cifratura l'operazione che lo trasforma in testo in cifra, cioè in una sequenza di simboli, intelligibile esclusivamente a chi ne possiede l'algoritmo decifrante (la chiave).

L'operazione inversa, cioè la traduzione del testo in cifra in testo in chiaro tramite l'applicazione della chiave, si chiama decifratura.

L'operazione, invece, con la quale si risale dal testo in cifra al testo in chiaro, senza avere la chiave[4] si chiama crittanalisi.

Un altro elemento fondamentale è la distinzione fra crittografia a chiave simmetrica e crittografia a chiave asimmetrica (o pubblica)

La crittografia, come la conosciamo dai tempi di Cesare e prima ancora da quelli degli antichi greci[5], è definita a chiave simmetrica perché la stessa chiave pone il testo in chiaro in testo in cifra e viceversa.

Al contrario, la crittografia a chiave pubblica - nata negli anni '70[6] - è un nuovo sistema studiato esplicitamente per la trasmissione dei dati su canali insicuri mediante un doppio sistema di chiavi. La prima (chiave pubblica) viene usata per cifrare, e una volta che ciò è stato fatto è impossibile decifrare il messaggio a meno di non avere la seconda (chiave privata).

Dal che si capisce perché si chiama crittografia asimmetrica: le due chiavi sono assolutamente indistinguibili rispetto alla funzione nel senso che - date due chiavi A e B - se cifriamo con A, decifriamo con B o viceversa[7]. Ma una volta impiegatane una, soltanto l'altra consentirà di decifrare il messaggio.

Un'altra importante questione terminologica riguarda i concetti di *Key Recovery* e *Key Escrow*.

---

[4] Quindi utilizzando una serie di sistemi di attacco, che vanno dal cosiddetto "attacco a forza bruta" ad una serie di tecniche molto più complesse sotto il profilo matematico

[5] Il testo più completo ed autorevole sulla storia della crittografia rimane ancora D. Kahn, *The Codebreakers*, New York 1967-1996.

[6] Peraltro c'è anche un'interessante querelle sull'effettiva paternità dell'invenzione, perché sembra che in realtà l'elaborazione di questo algoritmo, non sia americana ma sia inglese i biografi ci daranno la risposta

[7] Vedi ampiamente sul punto C. Giustozzi, A. Monti, E. Zimuel, *Segreti, spie, codici cifrati*, Milano 1999

Il *Key Recovery* è un sistema che consente il recupero della chiave[8] necessaria per decifrare il messaggio anche ad un soggetto diverso da quello che lo ha originariamente cifrato. Questa tecnologia si rivela particolarmente utile in tutti quegli ambiti - come quello aziendale, per esempio - dove non è possibile che circolino informazioni con modalità che le rendono (potenzialmente) inintelligibili al loro legittimo titolare[9].

Il *Key Escrow* è un concetto diverso di natura più giuridica che tecnica, perché implica la consegna volontaria ad una terza parte fidata della chiave (o di parte di essa) che consente la decifrazione[10].

Qui anticipo già quello che dirò successivamente, e cioè che questo è uno dei problemi fondamentali sui quali poi si dibatte quando si deve andare a parlare dei limiti in cui consentire l'utilizzo della crittografia a livello diffuso.

Key Escrow e *Key Recovery* sono di fatto il problema centrale sul quale si sta combattendo una battaglia silenziosa, ma non per questo meno cruenta.

3. Gli ambiti di applicazione

Fino a pochissimi anni fa, fino al 1997, oserei dire, si è trascorso il tempo pensando alla crittografia come ad una cosa da spie o da diplomatici e quindi tutto sommato confinata così in un ambiente abbastanza ristretto.

Le cose oggi non stanno più in questo modo e la crittografia è applicata in maniera talmente ampia da andare a toccare dei settori che normalmente non avremmo mai nemmeno pensato di associare a questa tecnologia.

3.1. La tutela della proprietà intellettuale

In questo settore la digitalizzazione delle opere dell'ingegno sta ponendo grossi problemi in termini di repressione dei fenomeni di duplicazione abusiva e di utilizzo illecito di servizi. Se le soluzioni tecniche che

---

[8] Quindi vale sia in àmbito di crittografia a chiave simmetrica, sia a chiave pubblica

[9] Anche questo è un terreno molto insidioso. Da un lato, è oramai un dato acquisito dal legislatore e dalla giurisprudenza che non è lecito utilizzare sistemi di monitoraggio a distanza delle attività dei lavoratori.

[10] Cfr. W. Diffie, S. Landau, *Privacy on the line*, Boston 1998.

si stanno affermando sono tutte orientate all'impiego di "sigilli crittografici" in grado di distinguere la copia dall'originale o di inibire l'alterazione dell'opera, quelle giuridiche sono al limite della costituzionalità. Non si può pensare altrimenti quando si sente proporre di sanzionare penalmente addirittura il semplice scambio di informazioni tecniche relative agli algoritmi di cifratura e agli apparati di decifratura[11].

3.2. I contratti *on-line*

Un'altra problematica rilevante è quella della stipulazione dei contratti per via telematica.

Da un lato, la firma digitale introdotta dalla legge Bassanini - quando funzionerà - consentirà di stipulare anche contratti a forma vincolata dotati di efficacia piena. Ma è anche vero che rimane non pienamente risolto il problema della tutela e dell'imputabilità della manifestazione di volontà di un soggetto che comunica in Rete e che è un discorso che prescinde dalla firma digitale[12]. Ciò vale in modo particolare per un altro ampio settore che non è regolato necessariamente dalla normativa sulla firma digitale. Si tratta dei contratti a forma libera, che possono essere validamente stipulati, proprio perché non ci sono requisiti formali stringenti posti dalla legge, anche mediante scambi di manifestazioni di volontà a distanza purché la manifestazione di volontà sia attribuibile, imputabile al soggetto che l'ha formata.

In questo senso la crittografia, anche non facente parte della costruzione normativa di cui al D.P.R. 513/97, ha un suo ruolo importante, perché in questo caso non stiamo parlando di firma digitale e di documento informatico, ma dell'attribuzione di valore giuridico ad una manifestazione di volontà. Cioè di un sistema che in qualche modo può sostituire l'identificazione personale diretta.

Quando due persone si trovano una di fronte all'altra si riconoscono somaticamente, e più in generale secondo una serie di criteri, grazie ai quali è possibile riferire univocamente le reciproche manifestazioni di volontà. Se viene meno questa prossimità fisica, c'è bisogno di un qual-

---

[11] Cfr. quanto previsto dal ddl C.4953, a proposito del quale vale la pena di ricordare le considerazioni critiche mosse dall'associazione ALCEI (http://www.alcei.it/sequestri/9903_diriautore_sequestri.htm)

[12] Vedi sul punto A. Monti, *L'volontà, dichiarazione e responsabilità nella comunicazione elettronica interattiva*, in *Il commercio elettronico* a cura di V. G. Scott, Torino, 1999

cosa che la possa sostituire, recuperando un affidamento altrimenti perduto per sempre. È a questo punto che l'impiego dei sistemi di crittografia a chiave pubblica (non necessariamente coerenti con il sistema del D.P.R. 513/97) può rivelarsi decisivo, nel momento in cui consente di riferire in modo univoco il contenuto non alterabile della manifestazione di volontà ad un soggetto.

3.3. La sicurezza nazionale

Al vertice di questa piramide di valori ci sono sicuramente gli interessi superiori dello Stato, che, per alcuni, si pongono in opposizione frontale con la tutela dei diritti individuali. A tal proposito, uno degli argomenti più utilizzati per invocare limitazioni nell'utilizzo della crittografia è quello che vede in limiti e divieti l'unico sistema per contenere lo strapotere della grande criminalità organizzata. Che diversamente si troverebbe in una sorta di universo parallelo di comunicazioni totalmente impenetrabile ai sistemi tradizionali. La scelta fondamentale da compiere, si dice, quindi, è quella fra crittografia forte e crittografia debole.

Sì, perché non esiste una sola crittografia, ma tante. La crittografia in sé è soltanto un'idea che poi deve essere applicata concretamente in base alle scelte politiche e normative del momento. Ecco dunque il primo nodo da sciogliere: vogliamo una crittografia debole, cioè una crittografia abbastanza robusta ma non tanto da resistere ad "attacchi" di una certa potenza, oppure vogliamo una crittografia forte? Vogliamo una fortezza inespugnabile o una casa (ma quanto?) sufficientemente protetta che però alla prima raffica di vento viene giù?

L'Italia è fortemente in ritardo su questo dibattito politico, ecco perché dicevo che il legislatore si è preoccupato più di aspetti tecnici, ma non ha dato sufficiente spazio ad un dibattito molto più ampio, come invece è accaduto oltre confine.

Gli Stati Uniti, al contrario, si sono occupati di questo problema da moltissimo tempo e per ovvi motivi[13], ma con una normativa particolarmente schizofrenica. Perché se all'interno del patrio suolo è assolutamente legittimo per qualsiasi cittadino americano utilizzare crittografia

[13] essendo il Paese nel quale all'inizio del secolo la crittografia è letteralmente fiorita con la creazione della Black Chamber che di fatto fu l'antesignana dell'attuale National Security Agency, cioè del più grande apparato di ricerca e sviluppo in materia di sicurezza e di crittografia e di criptoanalisi

forte (anche quella teoricamente inviolabile), nel momento in cui si passa all'estero questo discorso cambia radicalmente e non è possibile esportare dagli Stati Uniti della crittografia veramente forte. Anche se questi vincoli sono stati molto allentati nel corso degli ultimi anni, si deve considerare che fino al '96 la crittografia esportabile era di robustezza veramente scarsa. Inoltre per garantirsi che l'applicazione di questi divieti di esportazione fosse effettivamente messa in pratica è stato predisposto un sistema normativo che ha equiparato le tecnologie di cifratura alle munizioni da guerra. Questo perché esportare armi verso paesi "nemici" - e dunque pure "macchine cifranti" - è un reato gravissimo negli Stati Uniti.

Poi è anche vero - per esempio - che siccome nessuno vieta di esportare libri, succede sistematicamente che i codici sorgenti di programmi di crittografia venissero stampati in un libro e poi spediti all'estero[14]. D'altra parte credo ci si troverebbe in enormi difficoltà nel dover spiegare ad un giudice statunitense le ragioni del divieto di esportazione di un testo, specie a fronte della forte tradizione di tutela della libertà di espressione che si è sviluppata in questo Paese.

Un altro esempio abbastanza interessante è quello della Francia che è stata protagonista a oltre duecento anni dalla prima, di una nuova rivoluzione.

Questo Paese per anni ha avuto un regime assolutamente draconiano sull'utilizzo della crittografia a scopo privato, che era praticamente vietata per qualsiasi cosa. Salvo poi[15] annunciare una rivoluzione copernicana della politica di settore, che nel giro di pochissimo tempo è passata da un regime proibizionista ad un sistema estremamente elastico che va verso ulteriori allentamenti delle maglie normative.

Vediamo ora che cosa è successo in Italia.

Sarà curioso per voi sapere che forse la prima applicazione normativa della crittografia risale al 1924, quando un Regio Decreto impediva ai

---

[14] In particolare c'è una società americana che produce la versione commerciale di uno dei più noti *software* di crittografia attuale disponibili sul mercato e per uso personale gratuitamente, che fa esattamente in questo modo: realizza la versione americana, stampa i codici li manda in Olanda o in Svizzera, i codici vengono acquisiti con uno scanner e poi il programma viene ricompilato e reso disponibile con la sigla ! accanto al nome, che identifica la versione, in un modo del tutto lecito

[15] La stampa ha attribuito questa decisione al così detto scandalo Echelon, cioè della presa di coscienza a livello planetario, dell'esistenza di un network di intercettazioni gestito dai paesi di lingua anglosassone

professori di tenere il registro di classe con dei segni crittografici, evidentemente per ottemperare ad un dovere di trasparenza in caso di controlli.

Ma escludendo questo antico precedente, si potrebbe pensare che la crittografia in Italia non sia stata oggetto di attenzione normativa se non con il D.P.R. 513/97.

Non è vero, perché se leggete le norme in materia dell'esercizio di attività di radioamatore (può sembrare un settore totalmente scollegato da quello di cui stiamo parlando), scoprirete che ai radioamatori è assolutamente vietato parlare in codice. Devono assolutamente comunicare in chiaro, non solo, non possono nemmeno parlare in lingua straniera, hanno un parco di cinque lingue che possono utilizzare e nessun'altra.

La domanda spontanea è: come fanno ad accorgersene se invece di parlare italiano, spagnolo, tedesco, inglese, francese e russo parlano in cinese o polacco?

Risposta: ci vuole un organismo di controllo e la polizia postale è nata per questo. La cosiddetta *escopost* era l'organo di polizia che doveva sovraintendere al controllo dei radioamatori e chi ha un minimo di esperienza nel settore sa che negli anni '70 chi aveva questa passione è stato oggetto di vere e proprie "persecuzioni".

Da quanto sopra emerge chiaramente che il Legislatore italiano ha storicamente orientato in senso repressivo la regolamentazione dei sistemi di protezione delle comunicazioni.

La cosa strana, invece, facendo un salto di venti anni in avanti, è che quando si è passati all'Internet nessuno si è sconvolto dell'impiego così diffuso della crittografia negli ambiti più disparati (commercio elettronico, transazioni *on-line*, ecc.).

Questo è il segnale piu evidente della schizofrenia normativa che anima il legislatore, quello stesso legislatore che addirittura, sempre in materia di protezione delle comunicazioni, sottopone l'allevamento dei colombi viaggiatori al controllo della polizia militare.

Sta di fatto che Legislatore e Stato si rendono perfettamente conto che sistemi di comunicazione liberamente disponibili e fuori dal controllo possono essere chiaramente utilizzati dalla grande criminalità o a scopo terroristico.

Anche se su questo permettetemi di avanzare qualche dubbio, se è vero che fino al 1994 negli Stati Uniti non si è verificato un solo caso, in cui un'indagine di polizia sia stata messa in nulla dall'impiego da parte dei delinquenti di strumenti crittografici[16].

Magari la situazione sarà anche cambiata nel frattempo, però è abbastanza indicativo che nel Paese che ha, sicuramente, il più alto tasso di evoluzione tecnologica nel settore specifico, la criminalità organizzata non abbia mai utilizzato, almeno fino al '94, sistemi di questo tipo in modo tale da inficiare le attività di immagine della polizia.

Tutto questo credo che dovrebbe farci riflettere, perché tuttora in Italia il livello del dibattito, e qui vengo a riprendere l'inizio del mio discorso, vede replicare in modo anche abbastanza settario e apodittico i due grandi apparati concettuali e ideologici che si sono scontrati in America.

Da un lato ci sono quelli che io ho chiamato *national security advocate*, secondo i quali se le persone utilizzassero crittografia debole sarebbe più facile svolgere indagini, diversamente, si creerebbero grossi problemi.

Dall'altro c'è il *privacy guardian party*, che invece rivendica il diritto all'anonimato assoluto, il diritto a rivelarsi selettivamente al mondo.

Ora ai primi è abbastanza semplice obiettare che quand'anche lo Stato vietasse certe forme di crittografia o consentisse soltanto l'impiego di sistemi a crittografia debole, la grossa criminalità non avrebbe nessun problema ad "affittare" un matematico bulgaro per farsi fare un programma *ad hoc* anche al di fuori dei limiti imposti dalla legge.

Non mi sembra, appunto, che l'esistenza di norme che vietano certi comportamenti sia un limite per la criminalità.

C'è anche da dire che imporre per legge una crittografia debole equivarrebbe a chiedere alle persone di non installare porte blindate troppo resistenti nelle case, perché se un domani si dovesse aver bisogno di fare un irruzione di emergenza per un qualsiasi motivo, non sarebbe possibile entrare.

Anche qui è abbastanza chiaro che in attesa di un'eventualità che potrebbe non accadere mai, schiere di malintenzionati vi avranno già svuotato la casa più e più volte. Perché voi - in pieno adempimento di una

[16] Cfr. B. Schneier, D. Banisar, *The Electronic Privacy Papers*, 1997 J. Wiley & Son

norma così discutibile - avrete sistematicamente installato una porta sempre più debole.

D'altro canto, agli strenui sostenitori della riservatezza a tutti i costi c'è anche da dire che è antistorico pensare che lo Stato non possa dotarsi degli strumenti più avanzati per reprimere forme di criminalità sempre più pericolose.

Allora come si cava il ragno dal buco?

Anche qui credo che la soluzione in realtà sia già nelle cose, come dimostra in parte l'esperienza degli Stati Uniti.

Non è ovviamente l'unica soluzione possibile - e non è questo il migliore dei mondi possibili - però è una proposta che potrebbe funzionare.

I cittadini americani hanno la possibilità di utilizzare crittografia forte per uso civile, ma è anche vero che lo Stato americano si è dotato del più imponente apparato di cifratura e crittanalisi, cioè la *National Security Agency*. Cioè a dire: libertà, diritto del cittadino di tutelare la propria riservatezza, ma diritto dello Stato di dotarsi degli strumenti che consentono di violare tecnicamente questo tipo di protezioni (posto che ci riescano), nel caso in cui questo sia necessario.

Ma non a scopo preventivo, perché questo è il nodo della questione. Finché le regole saranno quelle che sono, le indagini preventive non sono ammesse; il nostro, fino a prova contraria, è un diritto penale del fatto, non della condotta, né tantomeno dell'atteggiamento interiore.

E allora se rimane fermo - e non vedo come sia possibile il contrario - il principio della materialità della condotta illecita e quindi della necessità di un fatto di reato, perché poi si possa attivare un'indagine di polizia non posso accettare in una prospettiva costituzionale[17] che possano esistere degli strumenti che preventivamente indeboliscono i diritti dei cittadini.

Anche perché la Storia ci ha insegnato che quello che è stato possibile (ed è tuttora possibile) fare distorcendo l'applicazione di strumenti investigativi.

Allora a questo punto è inutile pensare a delle norme formali sganciate dalla realtà dei fatti, sganciate da un dibattito ampio, che consenta

[17] Perché a questo punto non stiamo più nemmeno parlando né di interessi individuali né di interessi dello Stato.

di costruire quelle salde strutture d'assieme sulle quali poi erigere un apparato normativo - ancorché articolato - sicuramente coerente.

È su questo auspicio che io concludo questa mia relazione e vi ringrazio.