

Cassandra Crossing/ L’Inquisizione in Rete

(94)—La riservatezza delle password non è una banalità, è al centro di ciò che distingue una democrazia compiuta da un regime...

Cassandra Crossing/ L’Inquisizione in Rete



(94)—*La riservatezza delle password non è una banalità, è al centro di ciò che distingue una democrazia compiuta da un regime totalitario. Nel Regno Unito hanno deciso di cancellarlo. A quando in Italia?*

5 ottobre 2007—Inquisizione in Rete. No, non si tratta di un nuovo sito dedicato alla storia delle religioni. Si tratta della logica, seppur poco evidente, estrapolazione delle conseguenze potenziali dovute alla notizia riportata nell’ottimo articolo di Gaia Bottà.

In breve, nel Regno Unito è stata emanata la RIPA, una legge che obbliga, sotto certe condizioni, chi detenga chiavi o password che proteggono informazioni crittografate alla consegna delle stesse, per non incorrere in una pena detentiva fino a due anni di reclusione. Sia chiaro, il reato punito con due anni non è il nascondere foto pedofile o piani di attentati terroristici in un file crittografato, è il semplice fatto di non consegnare la password alla richiesta di un giudice. Anche se dentro il file c’è semplicemente la stesura del romanzo che state scrivendo. E se l’avete persa o dimenticata?

Beh, e semplice, questo vuol dire che se usi la crittografia rischi comunque la galera. Risultato: solo i criminali useranno la crittografia, fregandosene allegramente di un reato in più, ed il legislatore otterrà quello che è lo scopo reale, cioè un maggior controllo sui sudditi cittadini.

L'importanza di questo discorso merita anche una risposta seria e metodica, legata ai principi che distinguono i paesi in cui si rispettano i diritti della persona (una volta erano scontati in quelle che si chiamavano "democrazie") dagli altri (dittature, tirannie etc.). Questi diritti sono la libertà di espressione ed il diritto a non autoaccusarsi.

La Costituzione Americana, che è redatta spesso mescolando norme disomogenee nei contenuti, ha due emendamenti che riguardano anche (ma non solo) questi diritti.

Il Primo Emendamento stabilisce che la libertà di parola è assoluta, fino a quando le "parole non diventano armi"; ad esempio se qualcuno dice "Impiccate tutti gli informatici" da Bruno Vespa lo può fare, mentre se lo dice ad una folla che ne ha appena catturati due e sta preparando dei nodi scorsoi non lo può fare.

La Corte Suprema ha spesso sentenziato in favore del primo caso quando non era provato in maniera assolutamente palese l'attributo "armi" delle "parole". Da noi non sarebbe così pacifico, come le cronache insegnano, ma qui la storia italiana recente sarebbe argomento fuori tema. Il Quinto Emendamento stabilisce che nessuno può essere costretto ad autoaccusarsi. L'Inquisizione spagnola solleva appunto torturare le persone finché non si autoaccusavano, magari con delle aggravanti; lo scopo finale della tortura era infatti quello di redimere il peccatore facendolo pentire, cosa possibile solo DOPO aver "sinceramente" ammesso le proprie colpe.

Anche in Italia un accusato può tacere anzi, di più, può mentire per proteggersi, senza per questo commettere ulteriori reati. Negli Stati Uniti un indiziato può appellarsi al Quinto Emendamento per non autoaccusarsi senza per questo ammettere nessuna colpa. Non può però mentire per difendersi, e non può rifiutarsi di rispondere se non è accusato ma solo testimone o persona informata sui fatti.

Con la nuova legge inglese l'equivalente di un questore e di un giudice durante un'indagine possono richiedere a chiunque la consegna delle chiavi crittografiche se il server che contiene i dati si trova nel Regno Unito.

E' probabile che le banche inglesi, se non esentate, dovranno migrare i propri datacenter all'estero; qualunque giudice potrebbe infatti improvvisamente richiedere la consegna delle chiavi di interi sistemi informativi.

Ma nel caso di individui in possesso di chiavi crittografiche che bloccano dei dati cosa può succedere? Facciamo qualche esempio.

Bin Laden, se arrestato col suo portatile cifrato negli UK potrebbe essere costretto, sotto minaccia di due anni di galera, a consegnare la password della sua chiave Pgp. Lo farebbe? Mah... Ma anche un pedopornografo arrestato nel Regno Unito con il suo portatile dotato di partizioni cifrate piene di foto indescrivibili potrebbe ricevere la stessa richiesta. Lo farebbe? Con quello che rischia? Mah...

Una persona qualsiasi, che difende i propri dati personali e la propria privacy usando Pgp o Truecrypt su file e posta, fermato (non arrestato) negli UK per un messaggio ricevuto da un indagato potrebbe ricevere la stessa richiesta. Lo farebbe? Eh, beh....

Un sistemista qualsiasi che per lavoro fosse in possesso di chiavi lo farebbe? Certo, ma allora che senso avrebbe affidargliele? Qualunque chiave o password sarebbe violabile, anche con giustificazioni banali.

Concludendo: a chiunque può essere richiesto l'accesso ai propri dati crittografati senza nessuna accusa, sotto pena del gabbio. Che senso avrebbe perciò usare la crittografia per i cittadini, visto che se questo approccio legale diventasse normale qualunque persona potrebbe essere costretta a rivelare tutti i propri (ed altrui) dati criptati e, se colpevole di qualcosa, ad autoaccusarsi?

Si ripresenterebbe, con un'evoluzione storico-tecnologica di cui Campanella se potesse ci avvertirebbe, la situazione del Se-non-ti-accusi-da-solo-ti-torturo, con l'unica differenza che, essendo la tortura ancora vietata nelle democrazie (con qualche eccezione qua e là) la si sostituisce con la galera.

Equivarrebbe, non potendo vietare la crittografia di per sé, a renderla inutilizzabile per aziende e cittadini onesti, lasciandola a disposizione solo dei criminali. Con buona pace di essenziali diritti civili come la tutela della propria privacy.

Con buona pace del Quinto Emendamento e del diritto di non autoaccusarsi.

Con buona pace della libertà di espressione che è fatta anche della libertà di non esprimersi.

Con buona pace di chi non trova niente di male nel rinunciare ad un altro pezzo della propria ed altrui libertà.

Tanto... *“chi non ha niente da nascondere non ha niente da temere.”* (Adolf Hitler—“Mein Kampf”—1925–1926)

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica “Quattro chiacchiere con Cassandra”
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

Licenza d'utilizzo: *i contenuti di questo articolo, dove non diversamente indicato, sono sotto licenza Creative Commons Attribuzione—Condividi allo stesso modo 4.0 Internazionale (CC BY-SA 4.0), tutte le informazioni di utilizzo del materiale sono disponibili a questo link.*

By Marco A. L. Calamari on September 18, 2023.

Canonical link

Exported from Medium on January 2, 2024.