

informazioni da loro raccolte in tempi brevi, dell'ordine di non più di 3 anni dal momento della rivelazione delle informazioni al management aziendale. Il Partito dei Pirati intende chiedere che il ricercatore sia tenuto per legge a divulgare immediatamente ogni informazione che possa contribuire a salvare vite umane o che possa evitare danni alla salute dei cittadini od all'ambiente in cui essi vivono.

6. Diritto di Accesso alla Tecnologia

Il Partito dei Pirati intende ottenere il riconoscimento legale del diritto del cittadino ad accedere alla Tecnologia che è disponibile in ogni singolo momento storico nel suo paese. Il Diritto di Accesso alla Tecnologia viene violato ogni volta che una azienda si rifiuta di produrre un oggetto di cui possiede i brevetti per ragioni economiche (scarsa remuneratività) o strategiche (logiche di scambio con altre aziende). In questo caso, la responsabilità è dell'azienda e l'intervento dovrà essere teso all'esproprio del brevetto. Il Diritto di Accesso alla Tecnologia viene violato ogni volta che un cittadino non può accedere ad una tecnologia di carattere medico, e di rilevante importanza per la qualità della sua vita, per ragioni economiche o di altro tipo. In questo caso, la responsabilità è dello Stato e l'intervento dovrà essere teso alla copertura dei costi ed alla soluzione dei problemi tecnici di fornitura.

7. Diritto di Accesso alla Cultura

Il Partito dei Pirati intende ottenere il riconoscimento legale del diritto del cittadino ad accedere alla Cultura che è disponibile in ogni singolo momento storico nel suo paese. Il Diritto di Accesso alla Cultura viene violato ogni volta che una casa editrice, od un altro operatore economico, si rifiuta di produrre e/o distribuire un'opera di cui possiede i diritti per ragioni economiche (scarsa remuneratività) o strategiche (logiche di scambio con altre aziende). In questo caso, la responsabilità è dell'azienda e l'intervento dovrà essere teso all'esproprio dei diritti. Il Diritto di Accesso alla Cultura viene violato ogni volta che un cittadino non può accedere ad un'opera, per ragioni economiche o di altro tipo. In questo caso, la responsabilità è dello Stato e l'intervento dovrà essere teso alla copertura dei costi ed alla soluzione dei problemi tecnici di fornitura. Naturalmente, lo Stato ha tutto il diritto di decidere i tempi ed i modi dell'Accesso (Differita TV, DVD, visione/ascolto presso una mediateca, prestito gratuito od a prezzo politico, etc.).

8. Diritto ad una Fornitura Leale

Il Partito dei Pirati intende ottenere il riconoscimento legale del diritto del cittadino ad ottenere una fornitura di Beni e Servizi che sia caratterizzata dalla massima lealtà nei suoi confronti da parte del Fornitore. Il Diritto ad una Fornitura Leale viene violato ogni volta che vengono imposti dei limiti arbitrari al Bene od al Servizio che viene fornito. Consideriamo casi eclatanti di violazione di questo diritto le limitazioni sul traffico Internet imposte dai fornitori di accesso ("Traffic Shaping" e "Filtering") e le limitazioni imposte al funzionamento dei PC da parte dei produttori grazie a molte tecnologie di tipo DRM (Digital Rights Management) e di tipo Trusted Computing. Consideriamo assolutamente inaccettabili le limitazioni d'uso imposte ai sistemi per pure ragioni di marketing, come la limitazione d'uso a sola Game Console della Xbox di Microsoft (che, di fatto, è un vero PC). Consideriamo assolutamente inaccettabili le limitazioni d'uso imposte ai sistemi per pure ragioni di strategia aziendale, come l'uso di formati proprietari che limitano la possibilità di interazione con sistemi equivalenti prodotti dalla concorrenza e come l'assenza delle opportune funzioni di import/export necessarie a scambiare dati con sistemi equivalenti prodotti dalla concorrenza. La fornitura di un Bene o di un Servizio deve essere improntata alla sua massima utilizzabilità sul mercato ed alla sua massima versatilità d'impiego.

9. Diritto alla Libertà di Scelta e di Azione

Il Partito dei Pirati intende ottenere il riconoscimento legale del diritto del cittadino ad avere la più totale libertà di scelta nell'acquisto di Beni e Servizi e nel loro uso dopo l'acquisto. Il Diritto alla Libertà di Scelta e di Azione viene violato ogni volta che il cittadino/consumatore viene obbligato o condizionato ad un acquisto a causa della esistenza di vincoli imposti dai suoi fornitori. Consideriamo un esempio eclatante di violazione di questo diritto la politica di molte aziende che non forniscono strumenti adatti per l'interazione dei loro sistemi con sistemi prodotti dalla concorrenza o la integrazione dei loro sistemi in sistemi di complessità superiore ("scarsa o nulla interoperabilità"). Il Diritto alla Libertà di Scelta e di Azione viene violato ogni volta che al cittadino/consumatore viene negato un particolare tipo di utilizzo di un bene regolarmente acquistato senza che questo utilizzo rappresenti un danno diretto per il fornitore. Consideriamo un esempio eclatante di violazione di questo diritto la negazione del diritto al Reverse Engineering dei sistemi quando questa attività non è rivolta al superamento dei sistemi di protezione del diritto d'autore (DRM) ma invece alla interazione con altri sistemi od alla integrazione in sistemi di complessità superiore.

10. Diritto alla Privacy

Il Partito dei Pirati intende pretendere il riconoscimento concreto del diritto del cittadino alla privacy, già più volte enunciato nelle Costituzioni Italiana ed Europea ed ancora largamente negato proprio ad opera di quei Governi che dovrebbero garantirlo. In particolare, il Partito dei Pirati intende rivolgere la propria attenzione alla riservatezza delle comunicazioni ed intende ottenere la equiparazione di qualunque tipo di comunicazione (audio, telefonica, radio, digitale, etc.) alla comunicazione postale che è, tradizionalmente, l'oggetto di elezione di questo diritto all'interno della legislazione esistente. Il Partito dei Pirati intende anche richiedere l'esplicito riconoscimento del diritti del cittadino ad usare sistemi crittografici per garantire la riservatezza della proprie comunicazioni.

11. Diritto alla Comunicazione

Il Partito dei Pirati intende ottenere il riconoscimento legale del diritto del cittadino a comunicare con qualunque altra persona in qualunque momento ed in qualunque modo. Il Diritto alla Comunicazione viene violato ogni volta che al cittadino viene negato l'uso di un canale di comunicazione per ragioni tecniche o commerciali risolvibili con ragionevole facilità. Consideriamo un esempio eclatante di violazione di questo diritto la negazione del libero uso di sistemi Wi-Fi dentro e fuori del domicilio privato. Consideriamo un esempio eclatante di violazione di questo diritto la negazione o la limitazione dell'uso di sistemi di File sharing (Peer-to-Peer) già messa in atto da alcuni governi.

12. Diritto alla Espressione

Il Partito dei Pirati intende pretendere il riconoscimento concreto del diritto del cittadino alla libertà di espressione, già più volte enunciato nelle Costituzioni Italiana ed Europea ed ancora largamente negato proprio ad opera di quei Governi che dovrebbero garantirlo. In particolare, il Partito dei Pirati intende chiedere la modifica della legislazione esistente in fatto di attività giornalistica in modo da liberare la figura emergente del "blogger" dai vincoli che erano stati pensati per i giornalisti professionisti. Chi parla a proprio nome, od a nome di una associazione di qualunque tipo, e non a nome di un giornale, deve essere libero di dire ciò che vuole, nel modo e nei tempi che ritiene più opportuni. L'unico limite accettabile a questo diritto è quello rappresentato dal reato di diffamazione e dall'offesa personale.

Normalmente, le proposte di standard provenienti dall'industria vengono fatte proprie dall'ETSI dopo solo qualche ritocco cosmetico. Di conseguenza, è facile prevedere che tra pochissimi anni gli standard DVB avranno una patina di valore legale nonostante il fatto che sono stati sviluppati da un consorzio di aziende nel chiuso dei loro uffici e bandando solo agli interessi delle industrie stesse. Questa patina di valore legale servirà poi come base per una direttiva europea che, a sua volta, obbligherà i governi nazionali ad adottare questa tecnologia, e le leggi volute dal DVB Project, da MPAA e da RIAA come standard tecnici e leggi nazionali. Che fare? Nessuno dei vincoli previsti dallo standard DVB può essere aggirato, rimosso od invalidato neanche a livello teorico con l'uso di strumenti tecnici (modchip, crack od altro). Questo notevole risultato è ottenuto grazie al largo uso di dispositivi crittografici implementati in hardware, tra cui è ipotizzato anche l'uso del TPM usato dalle Trusted Platform (cioè il Fritz Chip della tecnologia Palladium). Di conseguenza, l'unico modo di difendersi da questa aggressione tecnologica è la via politica: si deve riuscire ad impedire l'approvazione di questi standard, la loro accettazione sul piano legale, la produzione e lo smercio di questi dispositivi prima che sia troppo tardi. Per ottenere questo risultato è necessario porre i nostri uomini politici nella posizione di non poter vendere il proprio voto alle aziende del settore senza essere poi costretti a fare i conti con il proprio elettorato. Questa battaglia sarà molto dura a causa del fatto che la stragrande maggioranza dei cittadini, e persino la stragrande maggioranza degli specialisti, ignora o sottovaluta enormemente il rischio rappresentato dalla rivoluzione digitale nella televisione. Per questo motivo, è necessario dare la massima diffusione a queste notizie, ad esempio usando la tecnica del Google Bombing. Il Google Bombing è una tecnica, del tutto legale e del tutto corretta, che consente di far apparire una certa pagina, chiamata "pagina target", tra le prime voci elencate da Google quando l'utente cerca un determinato termine, chiamato "parola chiave". Nel nostro caso, cercheremo di far apparire questa pagina che state leggendo tra le prime 10 voci elencate da Google quando l'utente cerca la parola chiave "Televisione Digitale". In questo modo speriamo di portare la minaccia del DVB project a conoscenza della maggior parte delle persone che si occupano, per un motivo o per l'altro, di televisione digitale. In particolare, speriamo di riuscire ad informare i giornalisti e le persone che agiscono come consiglieri tecnici dei politici. Come aderire al nostro Google Bombing.

Per favore, pubblicate un articolo su questo tema, anche di sole tre righe ma scritto di vostra mano, su un qualunque sito web a cui abbiate accesso. Inserite all'interno del vostro articolo un link a questa pagina. Per favore usate come testo ancora (cioè come "parola chiave") del link il termine "televisione digitale". Se proprio non sapete come fare visitate il nostro sito. Questo documento è pubblicato sotto una apposita Licenza Creative Commons in modo che lo possiate ripubblicare, inalterato, dovunque vogliate. Potete usare a questo scopo anche un semplice blog gratuito, come quelli che potete creare a www.wordpress.com e www.blogger.com. Che altro fare? Per favore, diffondete questa notizia il più ampiamente possibile tra amici e conoscenti. Se potete farlo, pubblicate i vostri articoli su questo tema sul web o, meglio ancora, sulla stampa cartacea. Se avete accesso ad una radio od una televisione, parlatene. Se conoscete qualche politico, informatelo della questione. L'unica cosa che vi chiediamo è di non spedire messaggi su questo tema ad estranei (uomini politici o giornalisti) via e-mail o via posta tradizionale. Non c'è un motivo al mondo di infastidire in questo modo persone che conoscete solo di fama. Puoi ripubblicare liberamente questa pagina sul tuo sito web o su un documento cartaceo, a condizione che non la modifichi e che non la usi a scopi commerciali. Le fonti

Non stiamo delirando o, se stiamo delirando, siamo in buona compagnia. Le nostre fonti sono le seguenti.

<http://www.dvb.org/index.xml>
http://www.eff.org/IP/DVB/dvb_briefing_paper.php
<http://www.eff.org/IP/broadcastflag/>
http://www.eff.org/IP/broadcastflag/three_minute_guide.php
http://www.boingboing.net/2007/03/13/eff_reveals_plot_to_.html
<http://punto-informativo.it/p.aspx?id=1925073&r=PI>
<http://it.wikipedia.org/wiki/DVB>
<http://en.wikipedia.org/wiki/DVB>
http://en.wikipedia.org/wiki/Broadcast_flag
http://it.wikipedia.org/wiki/Broadcast_flag
http://it.wikipedia.org/wiki/Diritto_d%27autore
http://it.wikipedia.org/wiki/Convenzione_di_Berna_per_la_protezione_delle_opere_letterarie_e_artistiche
 Articolo di EE Times
<http://defectivebydesign.org/>
http://en.wikipedia.org/wiki/Defective_by_

Programma del Partito - Pirata Italiano

Il Partito-Pirata si attiva politicamente per la difesa dei diritti dei cittadini in particolar modo è interessato alla Cultura libera, al Diritto d'Autore e alla Privacy dentro e fuori la rete ed enuncia i seguenti punti per i quali intende operare:

1. Principio di Legalità

Il Partito dei Pirati non promuove e non appoggia, nè esplicitamente nè implicitamente, nessuna azione che violi le leggi esistenti. Il Partito dei Pirati promuove invece la modifica delle leggi esistenti al fine di salvaguardare i diritti dei cittadini, dei consumatori, degli autori e degli operatori economici in modo equilibrato e socialmente accettabile. Il Partito dei Pirati si riserva il diritto di promuovere delle azioni dimostrative tese a mettere in evidenza le contraddizioni di una legge, od i suoi effetti negativi sull'individuo o sulla società, nei limiti di una normale ed accettabile dimostrazione democratica a carattere episodico e limitata nel tempo.

2. Ri Forma del Copyright

Il Partito dei Pirati intende promuovere una estesa e radicale azione di riforma della legislazione che riguarda il Diritto d'Autore (Copyright), al fine di ripristinare l'equilibrio ora perduto tra gli interessi degli operatori economici, quelli dei consumatori, quelli degli autori e quelli della società nel suo complesso. L'elemento fondante di questa riforma dovrà essere il concetto che i materiali protetti da copyright rappresentano la Cultura di una Nazione e come tale possono essere sottoposti a vincoli di utilizzo solo per brevi periodi di tempo e solo per determinate applicazioni di carattere commerciale. L'accesso a questi materiali deve essere garantito anche per coloro che non possono permettersi l'accesso al mercato per ragioni economiche, ad esempio grazie ad opportune sovvenzioni o attraverso l'opera di pubbliche mediateche. In particolare, è nostra intenzione affrontare il tema del "corretto uso" dei materiali coperti da diritto d'autore ("Fair Use"), il tema della creazione e dell'uso di copie per uso personale ed il tema dell'uso di sistemi DRM per la protezione dei contenuti. Su tutti questi temi è nostra intenzione chiedere modifiche, anche estese e radicali, alla legislazione esistente.

segue dalla prima

INFORMETICA

Una community di questo genere potrebbe produrre e raccogliere materiali utili a chiarire alcune questioni ancora oggi non risolte. Essendo l'etica una caratteristica individuale, sarà necessario raccogliere il maggior numero di adesioni e sottoscrizioni per poter avere un'idea sociale condivisa. Se dagli studi emerge ad esempio che il P2P piace molto al popolo italiano, allora risulterebbe "fuori luogo" una legge che considera illegale questa tecnologia. Dunque il numero di partecipanti ad una community di questo genere risulta di primaria importanza. Concordo che sia troppo superficiale pretendere di creare un movimento in grado di cambiare la sorte di una nazione, però nulla ci vieta di discutere e sensibilizzare i nostri animi al fine di limitare quantomeno che scenari da "1984" diventino ben presto la nostra routine.

Le mani sulla TV digitale



(e, in momenti diversi, in tutta Europa ed in USA). Sia la televisione satellitare, sia la televisione digitale terrestre, sia la televisione via cavo, sia la televisione via Internet, sia la televisione su dispositivi mobili utilizzano infatti un protocollo di trasmissione digitale del segnale. Gli standard necessari vengono sviluppati da un consorzio chiuso di aziende chiamato DVB Project. Il consorzio DVB raccoglie oltre 260 aziende di tutto il mondo e definisce gli standard per la trasmissione digitale di audio e video sui sistemi della prossima generazione. Gli standard che il DVB Project ha sviluppato sono i seguenti.

* DVB-S ("Satellite"):

standard usato per la televisione via satellite

* DVB-C ("Cable"): standard usato per la televisione via cavo

* DVB-T ("Terrestrial"):

standard usato per la televisione digitale terrestre

* DVB-H ("Handheld"):

standard usato per la televisione su sistemi mobili (telefoni cellulari ed affini)

Ciò che questo consorzio decide, nel chiuso delle sue riunioni tra aziende, è già adesso legge per chiunque voglia trasmettere o ricevere segnali audio e video digitali nel mondo,

semplicemente perchè gli strumenti tecnici prodotti da queste aziende rispondono a questi standard ed a nient'altro. Queste 260 aziende rappresentano la stragrande maggioranza dei produttori mondiali per cui, di fatto, il consorzio definisce standard di portata globale a cui è impossibile sottrarsi. Come vedremo nel seguito di questo documento, persino nella remota ipotesi che un produttore indipendente decidesse di opporsi a questo dominio, lo standard definito dal DVB Project prevede strumenti e tecniche adatti a rendere la sua ribellione del tutto inutile. EFF e il DVB Project

La Electronic Frontier Foundation si è iscritta al consorzio DVB, pagando la quota di iscrizione di 10.000 euro, ed ha partecipato alle sedute. La possibilità di divulgare informazioni è pesantemente limitata dalle clausole del contratto di adesione al consorzio per cui la EFF non può, legalmente, divulgare le informazioni di dettaglio che riguardano questo consorzio, il suo modo di lavorare, le posizioni delle diverse aziende che ne fanno parte ed il loro voto. Tuttavia, la EFF ha potuto pubblicare un rapporto di massima su ciò che il DVB Project sta preparando. Il Progetto CPCM

Ciò che il DVB Project sta studiando, sin dal 2003, è qualcosa che non piacerà agli "spettatori" europei ed italiani. Questo qualcosa si chiama CPCM, cioè "Content Protection and Copy Management". Questo standard permetterà ai produttori di programmi televisivi di imporre le seguenti limitazioni.

NOTA: Per quanto folli e vessatorie possano sembrare queste limitazioni, sono comunque reali. Non stiamo delirando e non ci siamo inventati nulla. Potete controllare voi stessi leggendo le fonti che elenchiamo in calce a questo documento.

Divieto di registrazione.

Questo standard permette di vietare la registrazione di un programma televisivo attraverso il sintonizzatore TV. Non potranno più essere registrati i film, i telefilm od altri programmi televisivi, né su cassetta, né su CD o DVD, né su disco fisso. Questo divieto non è aggirabile in nessun modo perchè implementato sia con dispositivi software che hardware.

Divieto di copia.

Questo standard permette di vietare la creazione di copie di un CD o DVD. Non potranno più es-

sere create copie di film, di telefilm od altri programmi televisivi, né su cassetta, né su CD o DVD, né su disco fisso, nemmeno per uso personale o per backup. Questo divieto non è aggirabile in nessun modo perchè implementato sia con dispositivi software che hardware.

Divieto di trasferimento.

Questo standard permette di vietare il trasferimento di un programma televisivo attraverso una rete di computer, ad esempio dal sintonizzatore TV che si trova in salotto al display del laptop che si trova in camera da letto. Questo standard permette di vietare la fruizione del programma televisivo fuori da una certa nazione, grazie ad un apposito marcatore digitale inserito nei dispositivi (simile al codice regionale dei DVD ma, a differenza di esso, assolutamente non aggirabile). Questo standard permette anche di vietare la fruizione del programma televisivo fuori da un determinato locale, ad esempio il salotto di casa, grazie ad un apposito ricevitore GPS integrato nei dispositivi (naturalmente pagato da chi acquista il dispositivo). Questo divieto non è aggirabile in nessun modo perchè implementato sia con dispositivi software che hardware. **Divieto di condivisione.**

Questo standard permette di vietare la condivisione di un programma con altre persone che risiedono nella stessa abitazione od in altri contesti, attraverso la definizione di appositi "domini di autorizzazione". Il DVB Project ha persino speso una quantità di tempo significativa per stabilire cosa deve essere dei DVD di una coppia in caso di divorzio! Questo divieto non è aggirabile in nessun modo perchè implementato sia con dispositivi software che hardware.

Obbligo di aggiornamento dell'hardware.

Questo standard permette di vietare la visione di un programma su dispositivi che il DVB Project ritiene non abbastanza fiscali nel rispetto dei suoi standard. Questo divieto non è aggirabile in nessun modo perchè implementato sia con dispositivi software che hardware e comporta la sostituzione del dispositivo, con i costi facilmente immaginabili.

Oscureamento dei canali liberi esistenti.

In futuro, questo standard dovrebbe persino permettere di imporre la cifratura al momento della ricezione (cioè sul TV Tuner del salotto) dei programmi trasmessi in chiaro. In questo modo, sarà possibile applicare le limitazioni espresse in precedenza persino ai programmi che il distributore ha deliberatamente deciso di distribuire in chiaro, senza alcuna limitazione. Si noti che il distributore, per legge, ha pagato per questo diritto ed ha firmato un contratto in cui questo diritto gli veniva riconosciuto. In alcuni casi, il distributore del programma potrebbe

La sicurezza nell'informatica

basandosi sia su componenti hardware (chip) che software, utilizza meccanismi crittografici tramite i quali permette di controllare lo stato di fiducia del sistema.[10] Le caratteristiche principali del TC sono le seguenti: -- I/O sicuro: tutte le informazioni che transitano nei circuiti del sistema sono cifrate crittograficamente per mezzo di opportune chiavi di cifratura non appannaggio del legittimo proprietario del sistema. - - Memory curtaining: ad ogni processo è assegnata una zona di memoria e non può interferire con altre zone di memoria utilizzate da altri processi (questa funzionalità è già presente, in maniera meno restrittiva, praticamente in tutti gli attuali sistemi operativi). Questo potrebbe addirittura impedire al sistema operativo stesso l'accesso a determinate aree di memoria, creando problemi con lo sviluppo ed il test del software. - - Sealed storage: le informazioni sono memorizzate sul sistema in maniera cifrata con una chiave che dipende dallo stato del sistema stesso, cioè dipende sia dall'hardware che dal software utilizzato nel momento della memorizzazione. Questo potrebbe rendere impossibile fruire di informazioni salvate con determinati programmi, per mezzo di altri programmi e da qui il passo potrebbe facilmente estendersi a pratiche anticompetitive, in maniera da rendere praticamente impossibile per gli utenti la migrazione da un software ad un suo concorrente. - - Remote attestation: un meccanismo che consente di verificare, da parte degli altri utenti collegati tramite la rete, lo stato di fiducia di un sistema. Questo porta alla perdita del beneficio della non conoscenza del software che è in esecuzione sui sistemi degli altri: la non conoscenza limita il controllo che si può avere sugli altri. Il cuore di tutto il TC risiede nel TPM (Trusted Platform Module, chip di cui sono dotati vari PC già in commercio) il quale detiene la chiave di cifratura detta Endorsement Key, che lo identifica univocamente, inserita al suo interno prima della vendita all'utente finale e non accessibile da quest'ultimo che quindi non può controllare appieno il sistema. Ovviamente il TPM da solo non è sufficiente affinché il sistema funzioni con i criteri del TC, ma è necessario che vi sia un opportuno BIOS (il programma che viene eseguito all'avvio della macchina), un opportuno boot loader (il programma che avvia il sistema operativo scelto dall'utente) ed un opportuno sistema operativo, tutti realizzati in maniera tale da colloquiare con il TPM. Un altro dei fattori più critici del TC è il fatto che l'implementazione delle specifiche del TCG è lasciata ai produttori di TPM: chi ci assicura

funzionalità non documentate o delle backdoor? E chi stabilisce quale software potrà essere eseguito dal sistema (poiché ritenuto fidato dal sistema operativo con le indicazioni del TPM)? Il legittimo proprietario del sistema viene trattato dal TC alla stregua di un possibile nemico del sistema stesso. Ma se i produttori non si fidano del consumatore, perché quest'ultimo dovrebbe fidarsi dei produttori, visto che alcuni dei loro maggiori esponenti non sono nuovi all'utilizzo di sistemi poco ortodossi per la protezione dei propri interessi? Dato che tutta l'elettronica digitale ne è coinvolta, l'introduzione del TC potrebbe portare gli utenti finali a non avere più il pieno controllo dei propri dispositivi. Inoltre il TC potrebbe essere utilizzato per attuare una censura dei contenuti elettronici (siti web, blog, documenti, ...) ritenuti "scomodi" per chi detiene il controllo, oppure per attuare una fidelizzazione forzata degli utenti di determinati software, obbligando quest'ultimi ad acquistare le versioni più aggiornate del software in questione pena il non funzionamento della versione più datata e l'impossibilità di riutilizzare i dati salvati con quel software con un altro dello stesso tipo. Con l'avvento del TC gli standard per l'interscambio delle informazioni rischiano seriamente di crollare. Insomma, il TC è davvero la soluzione definitiva alla sicurezza informatica? Secondo me no, anzi va a limitare la libertà del legittimo proprietario del dispositivo digitale e lo priva del pieno controllo dello stesso. Pertanto inviterei ad essere più critici di fronte all'acquisto di dispositivi digitali avendo coscienza di ciò che possono contenere al loro interno: se non si vogliono il TC o il DRM, si può semplicemente evitare di acquistare la tecnologia che li supporta. Concludo parafrasando Benjamin Franklin, per riflettere sull'impotanza della libertà e della sicurezza, poiché "chi è disposto a rinunciare alle proprie libertà fondamentali in cambio di briciole di sicurezza, non merita né la libertà né la sicurezza."

[1] http://i.t.wiki.pedi.a.org/wi/ki/Software_1_i_bero
<http://www.gnu.org/philosophy/free-sw.it.html>
 [2] <http://i.t.wiki.pedi.a.org/wi/ki/Crittografia>
 [3] http://i.t.wiki.pedi.a.org/wi/ki/Principi_o_di_Kerckhoffs
 [4] http://www.interlex.it/Testi/141_633.htm
 [5] http://en.wiki.pedi.a.org/wi/ki/European_Copy-right_Directive
<http://en.wiki.pedi.a.org/wi/ki/DMCA>
 [6] <http://blogs.technet.com/markrussi/2005/10/31/sony-rootkit-ts-and-digital-rights-management-gone-too-far.aspx>
 [7] http://www.economist.com/daily_story.cfm?story_id=4342418
<http://www.hwupgrade.it/articoli/sicurezza/1377/sony-1-ombra-dei-rootkit-t-sul-la-tecnologia-dm-3.html>
 [8] http://www.lastampa.it/web/cmstp/templ_rubriche/tecnologia/grubrici.asp?ID_blog=30&ID_articolo=1962
 [9] <https://www.trustedcomputinggroup.org>
 [10] http://i.t.wiki.pedi.a.org/wi/ki/Trusted_computing
<http://www.no1984.org>
<http://vandal.it.org/Dani/elmasini/notc.php>

dalla prima

Autore, Opera e Licenza
 Funzionava così:

1) L'autore infilava una copia della sua opera in una busta sigillata. Poteva trattarsi di una copia su carta di un romanzo, di uno spartito o di una sceneggiatura ma anche di un disco (vinile), di un nastro magnetico o di una "pizza" di pellicola. In ogni caso, la busta doveva essere sigillata e firmata dall'autore.

2) L'autore spediva la busta in questione a sé stesso usando le Poste. Le Poste, per regolamento, devono apporre il timbro del giorno di ricezione sulle lettere. In questo modo si stabiliva un momento nel tempo, valido a tutti i fini legali, in cui l'opera esisteva già.

3) L'autore conservava la busta sigillata in cassaforte. Nel caso che fosse necessario andare in tribunale per dimostrare la paternità dell'opera, la busta veniva aperta dai periti del tribunale ed il suo contenuto veniva confrontato con ciò di cui si voleva dimostrare la paternità. Da quando esistono i computer ed Internet, questa procedura è stata "dematerializzata" ed ora funziona più o meno in questo modo:

1) L'autore converte la sua opera in un formato digitale adatto. Si noti che può anche non essere l'opera come tale ad essere "digitalizzata" ma semplicemente una sua rappresentazione. In altri termini si può usare un file CAD 3D per descrivere una scultura. Questo è possibile perché anche nella registrazione tradizionale si fa comunque uso di rappresentazioni. Il testo scritto su carta, infatti, non è il romanzo ma una sua specifica implementazione, uguale a qualunque altra copia stampata dall'editore.

2) Usando una Smart Card, l'autore firma digitalmente l'opera e vi appone una marca temporale. In questo modo, si può dimostrare che quel file era in possesso dell'autore prima del momento segnato sulla marca temporale.

3) Il file risultante viene conservato da qualche parte per usi futuri in tribunale. Le Smart Card
 Le Smart Card usate a questo scopo non sono altro che rettangolini di plastica, molto simili alle normali carte di credito, che possono essere usate insieme ad un normale PC grazie ad un apposito lettore. Sono dotate al loro interno di un microprocessore (grande quanto un grano di sale)

continua a pag.5

La sicurezza nell'informatica

Gli apparecchi digitali sono accomunati dal fatto che i circuiti che si trovano al loro interno (hardware) funzionano secondo una logica programmata generalmente dal costruttore, ovvero il loro funzionamento è governato dal software, i programmi: dal sistema operativo fino all'applicativo per compiere una determinata operazione come ad esempio inviare un messaggio di posta elettronica o navigare sul web. Vista la loro enorme diffusione, è sempre più sentita l'esigenza di sicurezza nell'utilizzo degli apparecchi digitali, intesa come sicurezza sui dati o, come più in generale viene indicata, sicurezza informatica. Nell'ambito informatico il termine sicurezza sottintende i concetti di protezione e controllo. Inoltre, esso è legato a vari aspetti: la protezione del sistema da eventuali attacchi esterni (o interni), la protezione delle informazioni (contenuti) e la protezione dei diritti sui contenuti digitali. Il primo aspetto riguarda le politiche di accesso al sistema, il firewalling e la qualità del software che vi gira sopra. Il software, ovvero i programmi che sono in esecuzione su un sistema rappresentano un aspetto fondamentale per il suo corretto funzionamento: essi determinano le operazioni compiute dal sistema stesso. Spesso però l'utente percepisce soltanto quello che vede sullo schermo ma il software può effettivamente fare qualcos'altro e l'unico modo per scoprirlo è quello di analizzarne le relative istruzioni, ovvero verificare quello che viene chiamato codice sorgente (anche se non si è personalmente in grado di comprendere il codice sorgente, ci sono moltissimi programmatori che lo sanno fare). Purtroppo questo non sempre è possibile poiché per far eseguire un programma ad un elaboratore elettronico il codice sorgente non è necessario. Quindi, se si vuol avere un maggiore controllo del sistema si dovrebbe preferire l'utilizzo di software del quale si può analizzare il codice sorgente, ovvero si devono prendere in considerazione i programmi ed i sistemi operativi liberi come Firefox, OpenOffice, GNU/Linux, FreeBSD, ... [1] Il secondo aspetto riguarda l'utilizzo dei sistemi crittografici[2]. Per mezzo di tali sistemi è possibile cifrare (cammuffare) una informazione e poterla successivamente rileggere in chiaro soltanto se si è in possesso di una particolare chiave di decifrazione. Anche in questo caso l'esperienza ha dimostrato che l'utilizzo di algoritmi di cifratura noti assicura una migliore protezione delle informazioni in quanto quest'ultima dipende dalla segretezza della chiave e non dall'algoritmo (principio di Kerkhoffs)[3]. Va da sé che il controllo sulle informazioni cifrate ri-

detiene la chiave per poterle decifrare. Per capire il terzo degli aspetti della sicurezza informatica è opportuno chiarire cosa si intende per contenuto digitale. Sui sistemi digitali le informazioni vengono generalmente memorizzate sottoforma di file, una sorta di contenitore generico il cui contenuto (digitale) può essere di varia natura: un documento di testo, un'immagine, una melodia, un film, ... Tali contenuti, analogamente ai libri, sono opere dell'ingegno e come tali sottostanno alla legge che regola il diritto d'autore, che per l'Italia è la legge n. 633 del 22 aprile 1941 e successive modificazioni[4]. Essa prevede che i diritti si suddividano in diritti morali, inalienabili, che conferiscono in perpetuo la paternità dell'opera all'autore che l'ha realizzata, ed i diritti di utilizzazione economica, che possono essere ceduti ed hanno una durata limitata nel tempo: 70 anni dalla morte dell'autore. La durata di quest'ultimi, che copre un arco di tempo di due o tre generazioni, limita notevolmente lo sviluppo tecnico: quando si applica la legge sul diritto d'autore ad un programma, ad esempio, si impedisce ad un'altra persona di riutilizzare quel programma per poterne realizzare un altro che magari ne estende le funzionalità, per un arco di tempo notevolmente più esteso rispetto al periodo di obsolescenza dei prodotti digitali stessi (un PC, ad esempio, diventa obsoleto dopo circa 1 anno). Un software è un elenco di istruzioni che servono per risolvere un determinato tipo di problema. Esso potrebbe essere paragonato alla stesura di un teorema di matematica: descrive i passi necessari alla risoluzione di un problema per mezzo di un elaboratore elettronico. In Europa è stata tentata più volte l'introduzione dei brevetti sul software, come già avviene negli Stati Uniti. Ma ha senso brevettare le idee? Se ha senso brevettare uno specifico prodotto come un determinato modello di sedia, con caratteristiche specifiche, ha senso brevettare l'idea generale di sedia in maniera tale che nessuno ne possa più produrre alcuna? Inoltre, per proteggere i diritti degli autori, spesso si favoriscono di gran lunga gli editori/distributori delle opere piuttosto che gli autori stessi. Il copyright dovrebbe supportare la creatività, non foraggiare le aziende dell'intrattenimento. Per proteggere le copie abusive (si parla essenzialmente di contenuti multimediali quali film, musica e giochi) alcuni produttori utilizzano i DRM (Digital Restriction Management), meccanismi, protetti dalla EUCD (che per l'Europa ricalca il DMCA statunitense)[5], che consentono la fruizione del contenuto soltanto per mezzo di

che consentono la fruizione del contenuto soltanto per mezzo di appositi programmi e/o dispositivi (a tal proposito si ricordi, ad esempio, lo scandalo relativo alla scoperta del rootkit di Sony nell'ottobre del 2005[6]). Essi costituiscono una sorta di copyright all'infinito sul contenuto digitale stesso e quasi sempre vengono utilizzati in maniera silente nei confronti dell'utilizzatore finale coerentemente con quanto asserito da un dirigente Disney qualche anno fa (settembre 2005), "se i consumatori sapessero che esiste un DRM, cos'è e come funziona, noi avremmo già fallito."[7]. Viene certo da chiedersi come mai chi si intrufola nei sistemi altrui viene giudicato in modi differenti: chi riesce a introdursi in sistemi governativi viene rinchiuso in galera, mentre chi manomette milioni di PC, non riceve praticamente alcuna pena esemplare. Addirittura, per mezzo di un meccanismo come quello dell'equo compenso, che prevede il pagamento preventivo alla SIAE di una tassa contestualmente all'acquisto di un supporto vergine (CD, DVD, cassette), si arrivano a colpire direttamente i consumatori anche se quest'ultimi non fanno uso del supporto per effettuare copie (lecite) di contenuti digitali protetti dalla SIAE. "Nessuno è riuscito a proporci un sistema valido per differenziare i vari usi del supporto, così la legge applica un criterio che apparentemente presenta discrasie ingiustificate, ma è inevitabile." afferma a tal proposito Giorgio Assumma (presidente della SIAE) in un'intervista pubblicata il 12 marzo 2007 su "La Stampa"[8]. Come è facile rendersi conto c'è un grande sforzo da parte degli editori/distributori nel garantirsi la tutela dei contenuti digitali, come già avviene per i libri. Ma la natura dei contenuti digitali è differente da quella della carta stampata: infatti una copia di un contenuto digitale è perfettamente identica all'originale stesso e da esso indistinguibile. Pertanto dovrebbero essere previste regolamentazioni diverse per le due tipologie di opere. Nell'ottica di garantire maggiore sicurezza ai sistemi digitali, il TCG (Trusted Computing Group), consorzio non-profit (così si legge sul sito[9]) nato nel 2003, di cui fanno parte praticamente tutte le più grandi industrie mondiali legate al campo informatico, ha redatto specifiche hardware e software che vanno sotto il nome di TC (Trusted Computing). Si tratta di una piattaforma tecnologica che,

(continua a pag.4)