"Digital Rights Management Systems e opere di pubblico dominio: un difficile binomio", in *"Digitalia. Rivista del Digitale nei beni culturali"*, ICCU (Istituto Centrale per il Catalogo Unico), Roma, anno III, Numero 1, 2008, pag. 50 e ssgg.

Telesio Perfetti

Università degli Studi di Perugia

Nel novembre 2001, presso la Duke University School of Law[1] si tenne una conferenza[2] che aveva quale tema centrale il "pubblico dominio", ovverosia l'insieme delle opere dell'ingegno di carattere creativo che, spirata la tutela patrimoniale accordata ai rispettivi autori, entrano a far parte del materiale liberamente fruibile dalla collettività, senza che alcuna autorizzazione preventiva risulti più necessaria per la loro utilizzazione.

In quel contesto si discusse da un lato del ruolo centrale del pubblico dominio rispetto all'accesso alla cultura e, dall'altro, della necessità di ridefinirne la nozione sì da ampliarne i tradizionali confini.

A sette anni di distanza, le tematiche allora trattate non solo restano di assoluta attualità ma, se possibile, si arricchiscono di ulteriori temi di discussione, primo fra tutti quello della necessità della salvaguardia del pubblico dominio nei confronti della continua espansione della tutela autorale in ambienti digitali.

In tale contesto si impone con forza una riflessione sul rapporto intercorrente tra l'implementazione di Digital Rights Management Systems (DRMS) e la salvaguardia dell'ambiente culturale di cui le opere di pubblico dominio costituiscono elemento essenziale.

Dalle misure tecnologiche di protezione ai Digital Rights Management Systems (DRMS)

Negli ultimi anni, in particolar modo dopo la sottoscrizione dei trattati della World Intellectual Property Organization (WIPO)[3], recepiti in Europa tramite la direttiva 2001/29/CE, cosiddetta EUCD – *European Union Copyright Directive*[4], si è assistito a un'evoluzione delle cosiddette

[1] Il sito dell'Università è raggiungibile al seguente indirizzo http://www.law.duke.edu/ (sito consultato in data 11 maggio 2008).

[2] Maggiori informazioni sul Convegno possono essere reperite al seguente indirizzo http://www.law.duke.edu/pd/ (sito consultato in data 11 maggio 2008).

[3] I trattati in questione sono il *WIPO Copyright Treaty* (WCT) e il *WIPO Performances and Phonograms Treaty* del 1996. L'implementazione americana del WCT è costituita dal cosiddetto *Digital Millennium Copyright Act* (DMCA), divenuto nel 1998 la legge americana sul copyright digitale.

[4] Direttiva sull'armonizzazione del diritto d'autore dell'Unione Europea, recepita dal d.lgs 68/2003.

"misure tecnologiche di protezione"[5], soprattutto grazie alla spinta delle *majors* americane e giapponesi (si pensi alla Microsoft, IBM, Warner Bros, Toshiba, Sony/BMG ecc.), *leaders* indiscusse del mercato informatico, cinematografico e discografico. Da mere misure poste a tutela e protezione tecnologica dei contenuti digitali coperti da copyright, si è passati progressivamente a sistemi più complessi. La protezione resta sempre la priorità, ma a tale funzione si accompagnano oggi servizi a valore aggiunto per gli utenti. Per tale motivo non si parla più, oramai, soltanto di "misure tecnologiche di protezione" (mtp), ma di misure di gestione o di amministrazione dei contenuti digitali protetti o, come anche si dice, stando all'espressione anglosassone, di Digital Rights Management (DRM – Gestione dei diritti digitali), sistemi tecnologici mediante i quali i titolari di diritti d'autore e dei diritti connessi possono esercitare e amministrare tali diritti nell'ambiente digitale, grazie alla possibilità di rendere protetti, identificabili e tracciabili tutti gli usi in rete di materiali adeguatamente "marchiati".

I DRM presentano le seguenti caratteristiche:

- consentono di controllare l'accesso al contenuto e gli usi dello stesso;
- vengono utilizzati per identificare il contenuto, i titolari dei diritti, l'utente legittimo, nonché le regole e condizioni generali per l'utilizzo del contenuto.

[5] L'art. 6, paragrafo 3, I alinea, della direttiva EUCD stabilisce che «per "misure tecnologiche" si intendono tutte le tecnologie, i dispositivi o componenti che, nel normale corso del loro funzionamento, sono destinati a impedire o limitare atti, su opere o altri materiali protetti, non autorizzati dal titolare del diritto d'autore o del diritto connesso al diritto d'autore, così come previsto dalla legge o dal diritto sui generis previsto al capitolo III della direttiva 96/9/CE ». Ricalca tale definizione l'art. 102-quater, comma 1, della legge 22/04/1941 n. 633 e successive modificazioni: *Protezione del diritto d'autore e di altri diritti connessi al suo esercizio* (di seguito LDA).

Tali misure di protezione mirano a:

- proteggere l'opera coperta da copyright (software, banca di dati, film, compilation musicale, file audio o video o audio-video ecc.) contro la copia non autorizzata;
- rendere impossibile l'accesso a terzi non autorizzati (non titolari di una regolare licenza o comunque non possessori legittimi dei supporti) e l'inoltro verso i medesimi;
- consentire un utilizzo limitato (per es. solo per determinati periodi di tempo o per determinate destinazioni d'uso) e predefinito nella licenza d'accesso fornita agli utenti finali.

Trattasi in sostanza di dispositivi anti-copia e dispositivi sul controllo degli accessi ai contenuti.

Nel nostro ordinamento, l'art. 171-ter, lett- f-bis), la LDA punisce con la reclusione da 6 mesi a 3 anni e con la multa da € 2.592 a € 15.493 chiunque, a scopo di lucro e sempre che il fatto non sia stato commesso per uso personale, «fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure».

I DRM si avvalgono di diverse procedure per la protezione del copyright. Le principali sono:

- la DRE (Digital Rights Enforcement) usata per la protezione e l'identificazione del contenuto al fine di assicurare che questo venga utilizzato esclusivamente nei termini e nelle condizioni previste al momento dell'acquisto (per es. se esso può essere riprodotto, stampato, comunicato, messo a disposizione del pubblico, diffuso ovvero in quali luoghi o con quali apparecchi può essere reso accesibile). Per ottenere tali risultati vengono sfruttate tecnologie basate su sistemi di crittografia, di *watermarking* (filigrana digitale) o di *fingerprinting* (tracciamento). In tal senso si soddisfano le esigenze di protezione contro gli accessi non autorizzati attraverso una serie di regole per l'utilizzo del contenuto digitale, espresse in un linguaggio comprensibile al computer (Rights Expression Language)[6];
- la DPM (Digital Property Management), usata per la gestione dei diritti di proprietà intellettuale relativi a un contenuto. In esso rientrano:
  - licenze di utilizzo e accordi concernenti la cessione dei diritti da parte del titolare dell'esclusiva, ivi inclusi termini e condizioni di uso;
  - l'interazione con i sistemi di Content Management (CM – Gestione dei contenuti[7]) per la più appropriata fornitura del contenuto secondo quanto stabilito nella licenza;
  - i sistemi di riconoscimento dell'identità del fruitore (utente e macchina, sia essa PC o lettore DVD ecc.);
  - tracciamento o monitoraggio dell'attività oggetto della licenza e la raccolta dei compensi a essa relativi, implementandosi così anche prestazioni di *e-commerce*.

In sintesi:

- si offre un valore aggiunto ai consumatori, dando loro l'accesso a contenuti che, senza un'adeguata gestione dei diritti, non sarebbero disponibili al pubblico;
- vengono sviluppati modelli di business flessibili grazie all'offerta di funzioni accessorie, come la gestione dei pagamenti per ottenere forme di utilizzo dei contenuti digitali, i *video on demand* (VOD), la *pay-per-view* e altre forme di transazione.

[6] Uno dei linguaggi standard più usati e di maggior successo è l'eXtensible rights Markup Language (XrML).

[7] Sistemi utilizzati per la distribuzione dei contenuti on-line attraverso *metadata*, *id est* informazioni sui dati che descrivono come, quando e da chi un determinato insieme di informazioni è stato preparato, consentendo per es. l'individuazione del formato di distribuzione e della sua versione, le condizioni di accesso al contenuto per l'utente e così via.

Tornando per un attimo all'evoluzione delle mtp in DRM, bisogna dire che i DRM stessi sono progrediti nel tempo. E infatti la prima generazione di DRM visualizzava semplici dati del titolare dei diritti (per es. autore e nome dell'opera) oppure riproduceva accordi di utilizzo del contenuto in licenze allegate (per es. licenze d'uso del software). Una seconda generazione ha iniziato a implementare funzionalità relative alla protezione, all'identificazione e all'accesso dei contenuti. Infine, i sistemi di DRM di terza generazione (quelli di oggi) sono in grado non solo di identificare e proteggere un'opera, ma anche di gestire i rapporti tra tutti i soggetti coinvolti nell'amministrazione di essa e dei diritti alla stessa relativi. Per tali motivi si parla ormai di vere e proprie architetture digitali (composte di hardware, software e reti) utilizzate per la commercializzazione dei contenuti digitali e soggette a regole e modalità predeterminate dall'industria dei contenuti e dai costruttori dei suddetti sistemi DRM[8]. E dacché architettura non può che essere sinonimo di "sistema" (data la sua complessità), ecco che all'espressione DRM si è sostituita quella di Digital Rights Management Systems (DRMS), veri e propri sistemi per l'amministrazione digitale dei diritti onde garantire:

– sicurezza contro accessi o duplicazioni illegali;
– descrizione, identificazione, commercio, protezione, controllo e tracciamento di tutte le forme di cessione del diritto all'uso di uno specifico contenuto digitale protetto da copyright[9].

Non a caso nei *workshop* del World Wide Web Consortium (W3C)[10] del 2001, a proposito di DRM si è parlato della gestione in forma digitale di tutti i diritti e non solo della gestione dei diritti di opere digitali. La regola giuridica dunque tradotta in linguaggio comprensibile per la macchina, in modo che quest'ultima la amministri e la faccia rispettare: si è di fronte a un modello legale interamente tecnologico. Non a caso si parla di "codice macchina" o di "legge macchina" (come pure si è detto nel paragrafo introduttivo), infallibile, priva di discrezionalità, "inviolabile" (almeno apparentemente), apodittica, non interpretabile né direzionabile verso esegesi sistematiche, analogiche, estensive, restrittive o storico-evolutive. La scarna e fredda logica formalistica del

[8] V. Roberto Caso, *"Modchips" e diritto d'autore. La fragilità del manicheismo tecnologico nelle aule della giustizia penale*, versione 1.0, settembre 2006, http://www.jus.unitn.it/users/caso/DRM/Libro/mod_chips/Roberto.caso_drm_mod.chips.pdf.

[9] In tal senso, v. Andrea Marco Ricci, *Digital Rights Management: definire per essere ottimisti*, consultabile all'URL http://www.interlex.it/forum10/relazioni/8am_ricci.htm.

[10] Fondato da Tim Berners Lee nell'ottobre del 1994 presso il Massachusset Institute of Technlogy (MIT) con lo scopo di migliorare i protocolli di comunicazione e linguaggio per il Web e di aiutarlo a sviluppare tutte le sue potenzialità.

computer regna sovrana, con effetti che, come si avrà modo di vedere, non sempre sono positivi e che anzi troppo spesso si rivelano indesiderati per gli utenti e i consumatori[11], a maggior ragione quando l'opera diviene di pubblico dominio, una volta scaduto il termine legale della durata dei diritti di utilizzazione economica esclusiva del diritto d'autore, fissato dall'art. 25 della LDA al termine del settantesimo anno solare dopo la morte dell'autore.

Nel momento in cui l'opera diventa di pubblico dominio, essa è liberamente fruibile dall'utente/consumatore. In ciò sta la libertà di accedere ai contenuti, alla conoscenza, all'arte, alla cultura *tout court* considerata e che oggi Internet sta contribuendo a far crescere. L'"editoria on-line" (oggi appositamente regolamentata con la legge 7/03/2001 n. 62), i blog, i gruppi di discussione (newsgroup e forum), i sistemi di *instant messaging* (come le chat), le piattaforme digitali per la condivisione di esperienze e conoscenze (*peer-to-peer* e *file-sharing*) hanno semplificato l'esistenza delle persone, hanno cambiato i loro atteggiamenti, mode, tendenze e gusti di consumo, hanno aumentato e facilitato la capacità di comunicare con altri individui, consentendo scambi di pareri o opinioni in *real time*, senza che la distanza possa essere in alcun modo di ostacolo, hanno dischiuso nuovi orizzonti alla conoscenza e alla sete di informazione e cultura, dando così attuazione completa e definitiva a quel diritto inviolabile dell'uomo che è la libertà di manifestazione del pensiero, che la nostra Costituzione tutela e garantisce ai sensi dell'art. 21.

Tale libertà ben si sposa e si integra con altri diritti, altrettanto inviolabili e altrettanto riconosciuti, garantiti e incentivati dalla nostra Legge fondamentale, come la libertà di comunicazione (art. 15 Cost.[12]) e come il diritto di arricchire e sviluppare il patrimonio culturale della Nazione attraverso la ricerca scientifica e tecnologica, nonché di promuovere l'arte, la scienza e la libertà di insegnamento delle medesime (v. art. 9 e 32 Cost.). Una libertà di manifestazione del pensiero dunque che, così integrata e agevolata dalla rivoluzione di Internet, va oggi riconsiderata in tutti i

[11] Richard M. Stallman ha voluto sottolineare l'ubiqua invasività di molte tecnologie DRM, reinterpretando l'acronimo come Digital Restrictions Management – Gestione delle restrizioni digitali.

[12] Si ricordi che l'art. 15 Cost. tutela e riconosce come inviolabile la libertà (e la segretezza) della corrispondenza e «di ogni altra forma di comunicazione». Orbene per corrispondenza non si può non far riferimento anche a quella elettronica (per es. l'e-mail), tra l'altro pienamente parificata a quella tradizionale (cartacea) ai fini della tutela offerta dalla legge penale (v. art. 616, comma 4, c.p., così come sostituito dall'art. 5 della l. 23 dicembre 1993, n. 547, recante *Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*). Inoltre è indubbio che l'ampia formula usata dal costituente «ogni altra forma di comunicazione» è tale da ricomprendere certamente Internet attraverso tutti i suoi canali informativi e diffusivi di notizie (siti web, blog, forum di discussione ecc.).

suoi aspetti e in tutte le sue varianti e sfaccettature, vale a dire rimirata quale libertà attiva di "informare", quale libertà passiva di "essere informati" e quale libertà riflessiva di "informarsi"[13].
A fronte di tali inderogabili esigenze di libertà e crescita culturale sacrosante in una Nazione che vuol definirsi civile, in dottrina[14] non è mancato chi solleva più di qualche dubbio sul modo, proprio delle *majors*, di approcciarsi, tramite i DRMS, alle problematiche della sicurezza dei contenuti digitali, nonché della sicurezza informatica (si pensi al recente fenomeno del Trusted Computing), anche perché troppa è la differenza tra regole giuridiche e regole tecnologiche, per i seguenti motivi:

– le regole della tecnologia informatica sono "deterministiche", senza possibilità di errore o di mutamento arbitrario, sono dettate da qualcuno attraverso il "linguaggio-macchina" espresso in codice binario, per definizione non ambiguo, essendo costituito da una sequenza di simboli numerici e cioè 0 e 1 univocamente interpretabili[15]. Per certi versi (sebbene in ambito diverso) assomigliano alle leggi ferree della natura (come la gravitazione universale o il magnetismo). Inoltre la forza di una regola informatica dipende essenzialmente dalla sua efficacia tecnologica (non a caso l'art. 102-quater della LDA parla di mtp "efficaci"), nonché dal suo grado di diffusione o "standardizzazione" (si pensi alle norme dell'International Organization for Standardization – ISO), tanto da poter assurgere a regola globale o "mondiale" (si pensi per es. agli standard qualitativi della famiglia ISO 9000 oppure allo standard per la *e-security* BS 7799-01, oggi recepito nello standard ISO 27001).
– viceversa la regola giuridica è per sua definizione fallibile, interpretabile, elastica, incerta, soggetta a esegesi evolutiva, legata al contesto storico, politico, sociale e "locale" in cui si è formata, non foss'altro perché espressa nel linguaggio umano, esso stesso equivoco, approssimativo, "aperto", in continua metamorfosi e (ci si scusi il gioco di parole) "assolutamente relativo", laddove basta un minimo mutamento della società, dell'economia, delle tendenze, delle mode, delle esperienze di vita, per dare corso a una nuova parola, a un

[13] Per approfondimenti sui suddetti e altri aspetti di carattere pubblicistico e costituzionalistico in merito alle innovazioni che Internet ha apportato alla libertà di comunicazione e di manifestazione del pensiero, v. Pasquale Costanzo, *Aspetti evolutivi del regime giuspubblicistico di Internet*, http://www.interlex.it/stampa/costanz2.htm.

[14] V. Roberto Caso, *Un "rapporto di minoranza": elogio dell'insicurezza informatica e della fallibilità del diritto. Note a margine del Trusted Computing*, versione 1.0, maggio 2007, http://www.jus.unitn.it/users/caso/DRM/Libro/rapp_min/Roberto_Caso_Rapporto_minoritario.pdf.

[15] Sulla natura delle regole "incorporate" in architetture digitali v. Dan L. Burk, *Market Regulation and Innovation: Legal and Technical Standards in Digital Rights Management*, « Fordham Law Review» 74 (2005), n. 537.

neologismo. Basta uno sguardo, direbbe Werner K. Heisenberg, per mutare la posizione di un oggetto[16]!

Le implementazioni dei DRMS nell'ambito del copyright

I DRMS in realtà non pertengono solo alla materia del copyright, bensì hanno ambiti di applicazione alquanto vari (*e-commerce*; Enterprise Rights Management e cioè la gestione di documenti aziendali e soprattutto dei segreti industriali, come Information Rights Management; protezione di contenuti relativi a dati particolarmente delicati nel campo sanitario, medico e della ricerca farmacologica e biotecnologia; *e-government*, con impiego dunque nella pubblica amministrazione[17]; beni culturali e documenti conservati negli archivi, in musei e in biblioteche e più in generale all'interno di banche di dati anche elettroniche utilizzate a tal scopo).

Ma, restando alla materia del copyright, la prima azienda a implementare un DRMS per i propri software è stata la Microsoft. Si allude al Microsoft Reader, utilizzato come programma di attivazione di altri programmi o per la fruizione di determinati servizi. Tramite esso gli *e-book*

[16] Werner K. Heisenberg formulò il famoso "principio di indeterminazione", ritenuto come uno dei principi-base della fisica quantistica: «non è possibile conoscere simultaneamente posizione e quantità di moto di un dato oggetto con precisione arbitraria». Se l'attenzione è posta sulla velocità, non si riuscirà a stabilire la precisa posizione di un corpo o di una particella e viceversa. Le certezze assolute della fisica galileiana e del razionalismo cartesiano del *cogito* crollano di fronte a un semplice dato di fatto empiricamente sperimentato in laboratorio: a livello atomico basta un fotone (particella di energia luminosa) per mutare o alterare il movimento di un elettrone, allo stesso modo in cui un raggio di sole può turbare (seppur impercettibilmente) la traiettoria di un proiettile. Anche alla natura dunque non possono essere applicati rigidi schemi deterministici e meccanicistici. Conseguenza ne è che anche la natura (e la materia) è retta da leggi probabilistiche e da medie statistiche, senza possibilità di avere certezze. Il diritto non è una scienza perfetta, ma neanche l'informatica, di qui (come sostiene Roberto Caso, *Un "rapporto di minoranza"* cit.) la "fallibilità" del diritto (data sempre per scontata), ma altresì (contrariamente a quanto si pensi e nonostante gli standard ISO) l'"insicurezza" informatica!

[17] In tal senso si pensi alle disposizioni del d.lgs. 7 marzo 2005, n. 82, recante il cosiddetto *Codice delle amministrazioni digitali* (noto anche con l'acronimo CAD), come successivamente modificato dal d.lgs. 159/2006, sulla protezione, integrità, autenticità e riservatezza dei documenti elettronici, nonché sui certificati digitali rilasciati dalle Certification Authorities e contenuti in apposite *smart-card* utilizzate come dispositivo per la firma digitale; si vedano ancora le disposizioni sulla gestione del protocollo informatico e sulla digitalizzazione del procedimento amministrativo; si veda ancora il protocollo d'intesa CNIPA-Adobe che riconosce Adobe PDF (Portable Document Format) quale formato valido per la firma digitale; si pensi poi alla produzione della CIE (Carta d'Identità Elettronica), della CNS (Carta Nazionale Servizi), al "passaporto elettronico" (*e-passport*) ecc.

Si ricordi che l'art. 69 CAD prevede per ciascuna pubblica amministrazione la possibilità di riutilizzare programmi realizzati anche da altre pubbliche amministrazioni, diverse da quella fruente, nonché di acquisire software *open source* (a codice sorgente aperto), oltre a quelli proprietari o soggetti a licenza d'uso (cosiddette EULA – *End User License Agrrement – Contratto di licenza con l'utente finale*).

acquistati venivano protetti dalla copia non autorizzata mediante la connessione, attraverso Internet, a un server al quale venivano fornite informazioni che identificavano il dispositivo e il file. Se l'utente aveva realmente acquistato il libro, la lettura poteva iniziare. In seguito tale tecnologia fu implementata in Windows XP e Office XP. In entrambi i casi l'utente, acquistando il software originale, riceve un codice alfanumerico di 25 caratteri, la cui validità viene inizialmente verificata dal software stesso tramite un algoritmo di *hashing*[18]. Entro un periodo stabilito (per es. 15 giorni) l'utente deve eseguire una verifica on-line o telefonica comunicando un codice numerico generato in base alla *Product Key* (numero di codice seriale del prodotto) e alla configurazione hardware del PC sul quale il software è installato. Se la verifica va a buon fine, il server (o l'operatore) risponde con un codice di conferma riconosciuto dal sistema, che sblocca tutte le sue funzionalità.

La tecnologia di attivazione è oggi adottata da tantissimi produttori di software, ma nella maggior parte dei casi può essere aggirata tramite *reverse engineering*.

Dopo la Microsoft, altre *software-house* e case di produzione e distribuzione discografica e cinematografica hanno sviluppato tecnologie DRMS per proteggere le opere coperte da copyright. Di seguito un elenco di alcuni tra i più noti DRMS, che comunque col passare degli anni sono divenuti obsoleti e ormai facilmente aggirabili o craccabili:

- Analog CPS (Macrovision 7.0): protezione anti-copia (solo video, non audio) per VHS, eluso da dispositivi presenti sul mercato a costi più che accessibili (Video Clarifier, Image Stabilizer, Color Corrector e CopyMaster);
- CSS (Content Scrambling System): protezione per DVD, sviluppata nel 1996 da Matsushita e Toshiba. Si basa sulla crittografia e su procedure di "autenticazione" tipiche della PKI (Public Key Infrastructure)[19]. Nell'ottobre del 1999, l'algoritmo CSS è stato violato e le chiavi furono pubblicate sul Web.

[18] Nel linguaggio scientifico, l'*hash* è una funzione univoca operante in un solo senso (ossia è irreversibile, non può essere invertita), idonea a trasformare un testo di lunghezza arbitraria (cioè non predefinita, variabile a seconda dei casi) in una stringa di lunghezza fissa, relativamente limitata. Tale stringa rappresenta una sorta di "impronta digitale" (identificativo univoco, universale e immodificabile del file generato) e viene detta *valore di hash* o *checksum* (riassunto) crittografico o *message digest*. Spesso il nome della funzione di *hash* include il numero di bit che questa genera (p. es. *SHA-256* genera una stringa di 256 bit). La funzione *hash* è molto utilizzata nella crittografia asimmetrica laddove è necessario apporre la firma digitale su documenti di testo particolarmente lunghi e corposi: grazie alla predetta funzione il file viene compresso. Per es. un file di migliaia di bit viene ridotto a una stringa di soli 128 bit e sarà quest'ultima ad essere firmata digitalmente, evitandosi così di firmare tutto il testo originale, operazione che potrebbe richiedere molto tempo e risorse.

[19] Infrastruttura a chiave pubblica, tipica della crittografia asimmetrica, usata sia per la *privacy* (riservatezza) che per l'autenticazione (garanzia di integrità, provenienza e non ripudio del documento elettronico formato con tale

– AACS (Advanced Access Content System): protezione per dischi ottici Blu Ray e HD DVD (High Density Digital Versatile Disc)[20], per controllarne l'accesso e la copia. Fu craccato il 18 dicembre 2006 dall'hacker Muslix64, che per prendere le chiavi di protezione non fece altro che sfruttare i *bug* di alcuni lettori multimediali che memorizzavano le chiavi nella RAM senza cifrarle. Slysoft[21] ha rilasciato il programma AnyDVD HD capace di sbloccare le nuove versioni delle protezione AACS per HD DVD. Da marzo 2007 è stata rilasciata la versione 6.1.2.9 del programma che è in grado di copiare su disco rigido anche i film Blu Ray e di rimuoverne il codice regionale.
– ARccOS: sistema di criptazione per la protezione anti-copia sviluppato dalla Sony e utilizzabile su alcuni DVD. Può essere usato insieme al CSS. Alcuni programmi come AnyDVD sono in grado di aggirare questa protezione. Sony ha cessato di usare il sistema ARccOS da febbraio 2006.
– HDCP (High-Bandwidth Digital Content Protection) per i file video digitali. Si basa su autenticazione (scambio di chiavi), crittografia e annullamento delle chiavi craccate (il codice utilizzato viene messo nella *black-list*).
– *Watermarking* (*tatouage numérique*): protezione per file audio, video, multimedia e anche per fotografie (.jpg, .gif ecc.). Mira a inserire in un flusso digitale una serie di informazioni di identificazione. Può essere visibile (per es. il logo di una emittente televisiva, addirittura gli

---

tecnologia). Il classico es. di PKI per l'auenticazione è offerto dal metodo o algoritmo di cifratura RSA (dalle iniziali dei cognomi di tre scienziati: Ron L. Rivest, Adi Shamir e Leonard Max Adleman). Il sistema si articola nel modo seguente:

- A crea un file e vuole che esso arrivi a B integro e autentico, cioè vuol esser certo che B sappia che il messaggio provenga da A e non sia stato contraffatto o alterato;
- per fare ciò, A firma il documento con la propria chiave privata (firma digitale), avente lo scopo di garantire integrità e certezza della provenienza del documento;
- il messaggio così firmato arriva a B, che dovrà verificarne integrità e paternità apponendo la chiave pubblica di A sul documento stesso;
- se il risultato dell'operazione andrà a buon fine, B sarà sicuro della veridicità e della provenienza del file da A.

In genere la firma digitale si appone non sul testo intero, ma solo sull'impronta digitale o *digest* creato dalla funzione *hash* usata per ridurne le dimensioni (v. nota 16), in modo da ridurre altresì i tempi di autenticazione e trasmissione del file medesimo.

[20] Formato ottico digitale sviluppato come standard per i DVD di nuova generazione adatti a contenuti ad alta definizione. Gli sviluppatori sono: Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Bros., IBM, Toshiba e Sony. Le specifiche furono rilasciate nell'aprile del 2005.

[21] «Slysoft Inc. è una società di software con sede a Saint John's, Antigua e Barbuda, specializzata in programmi di copia di CD e DVD. Taluni suoi programmi sono in grado di superare le protezioni anticopia punite dalla legge, ma non nello Stato dove risiede la società» (*SlySoft*, in: Wikipedia, http://it.wikipedia.org/wiki/Slysoft).

estremi identificativi dell'autore o della casa di distribuzione ecc.) o nascosto tramite steganografia[22] e in questo caso risulta più difficile da rimuovere. Serve a identificare la singola copia (ID univoco) o l'autore o anche il prodotto. Nel caso in cui venga trovata in rete una copia per es. di un film corrispondente al *watermark* assegnato in fase di acquisto e registrato su di un data-base o server, diventerebbe possibile identificare la fonte primaria della distribuzione illegale. Il sistema risulta rischioso in quanto non tutela l'acquirente di un CD o di un DVD in caso di furto o smarrimento: infatti il CD o DVD smarrito, se trovato da un malintenzionato, o comunque trafugato, potrebbe essere illecitamente usato (per es. per produrre copie illegali), ma l'ID univoco del *watermark* sarebbe sempre riferibile all'acquirente originale.

- BitLocker Drive Encryption: funzionalità di protezione dei dati integrata nel nuovo sistema operativo Microsoft Windows Vista che permette di crittografare e quindi di proteggere l'intera partizione del sistema operativo stesso. Per impostazione di *default*, cioè predefinita, viene usato l'algoritmo di crittografia AES (Advanced Encryption Standard)[23] con una chiave di 128 bit.
- Press Display: protezione per gli *e-book*. Consente il salvataggio del testo di singoli articoli di un giornale on-line, ma fa in modo che esso venga "gettato via" dopo un certo periodo, in

[22] Parola composta di origine greca (*steganós* = nascosto e *gráfein* = scrivere). Trattasi di una tecnica di scrittura che consente di inviare messaggi nascosti in altri messaggi di senso compiuto. Essa è dunque differente dalla crittografia, che desta maggior sospetto in quanto il messaggio crittografato è cifrato, codificato e incomprensibile (essendo costituito da una sequenza di numeri e/o lettere senza senso apparente) e potrà essere decriptato solo se il destinatario sia in possesso di una chiave in grado di palesarne il contenuto. In informatica la steganografia permette di inviare file occultati in altri file cc.dd. "di copertura" (es. foto .jpg, file multimediali ecc.), dal "peso", in termini di bit, alterato (proprio perché v'è un messaggio nascosto all'interno del file che appare), ma siffatta alterazione sfugge all'occhio umano e solo programmi sofisticati sono in grado di rivelare l'arcano. Sembra che la tecnica fosse nota già nell'antica Grecia. Lo storico Erodoto narra infatti del ribelle Istieo, che nascose un messaggio tatuandolo sul cranio rasato di un servo. Prima che il servo fosse inviato (con annesso messaggio) al destinatario, Istieo aspettò che ricrescessero i capelli; una volta ricresciuti, il servo partiva per la missione, con le istruzioni che, una volta giunto a destinazione, gli dovessero esser tagliati i capelli. Durante la Seconda Guerra Mondiale, si parla di tecniche fotografiche che avrebbero permesso all'esercito tedesco di nascondere una pagina di testo sul puntino della lettera "i".

Attorno al XVI sec. fu redatto il primo trattato di steganografia a opera dell'abate benedettino e alchimista Tritemio (Johann Heidenberg o Johannes Von Trittenheim, che egli latinizzò in Johannes Trithemius; visse dal 1462 al 1516). L'opera era intitolata *Steganographia, hoc est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa* (*Steganografia, cioè la tecnica di svelare, attraverso la scrittura nascosta, i desideri del proprio animo alle persone lontane*) e fu pubblicata postuma a Francoforte nel 1606.

[23] Trattasi di un algoritmo di cifratura simmetrica usato come standard dal governo americano e da molte altre organizzazioni e aziende. È in grado di assicurare un elevato livello di sicurezza (e quindi di riservatezza e integrità) ai dati e alle informazioni che con esso vengono criptate (viene infatti utilizzato, almeno nelle versioni più potenti con chiavi a 192 o 256 bit, per documenti classificati come i file *top secret*).

funzione del tipo di abbonamento stipulato, tramite trasferimento automatico nel cestino senza possibilità di ripristino. Il sistema rende impossibile l'inoltro a terzi non autorizzati. È abbastanza semplice da usare e contiene chiare informazioni su ciò che la protezione fa e non. È altresì possibile istallarlo e usarlo gratis per alcune volte (per es. per prova), ma con piena funzionalità, poi si paga un abbonamento (non troppo oneroso) e si rinnova in maniera semplice e veloce. Il DRM sembra basato su PDF criptati standard[24].

DRMS, libere utilizzazioni, opere di pubblico dominio e la cosiddetta "legge sull'accessibilità"

Fermo restando che l'arte debba essere "pagata" e il prezzo dell'opera ha comunque valore di remunerazione per la meritoria attività dell'autore nel contribuire alla crescita culturale e civile di una Nazione, purtuttavia non si può restare passivi e proni di fronte all'invasività dei DRMS. L'art. 41 Cost., nel garantire e riconoscere la libertà di iniziativa economica privata, al contempo fissa ad essa limiti invalicabili: infatti essa

> «non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana».

Giusta retribuzione dell'autore, ma anche diritto e libertà di fruizione, sia a seguito di legittimo acquisto dell'opera, sia quando l'opera stessa non sia più coperta da copyright in quanto ormai di pubblico dominio, sia quando si voglia fruire dell'opera per scopi puramente didattici o scientifici. E ci si chiede allora perché molti contenuti continuino a restare protetti pur decorso il settantesimo anno dalla morte dell'autore. Qui non si tratta più di tutelare un diritto (più che legittimo, lo si ripete) dell'autore, bensì si è di fronte a un "privilegio" che molte *majors* rivendicano: insomma siamo innanzi a un abuso, che blocca la crescita del mercato e lo sviluppo dell'arte e della cultura.
Lo stesso legislatore comunitario non è rimasto insensibile rispetto a siffatti rischi. Non a caso il considerando 31 della direttiva EUCD già di per sé aiuta a cogliere la *ratio* della necessità di stabilire taluni limiti ai diritti di carattere patrimoniale dei titolari, dacché deve essere garantito un giusto equilibrio e bilanciamento non solo tra i diritti e gli interessi delle varie categorie di titolari, ma anche «tra quelli dei vari titolari e quelli degli utenti dei materiali protetti», dovendosi altresì riesaminare le eccezioni e limitazioni alla protezione esistenti nelle legislazioni degli Stati membri «alla luce del nuovo ambiente elettronico». Per far ciò si potrebbero prevedere da parte degli Stati membri taluni casi di *fair use*, come per esempio nei considerando sottocitati:

[24] Per ulteriori approfondimenti, v. Marco Calamari, *Cassandra Crossing/Un DRM dal volto umano*, http://punto-informatico.it/p.aspx?i=2011295.

– l’utilizzo a scopo didattico e scientifico, per scopi d’informazione giornalistica, per citazioni, per l’uso da parte di disabili, per fini di sicurezza pubblica e in procedimenti amministrativi e giudiziari (34);
– l’utilizzo da parte di organismi pubblici che operano senza fini di lucro, quali le biblioteche accessibili al pubblico, gli istituti equivalenti e gli archivi (34 e 40);
– il diritto di riproduzione per taluni tipi di riproduzione di materiale sonoro, visivo e audiovisivo a uso privato (38).

Cionondimeno, per quanto qui interessa, aggiungasi la previsione del considerando 40, II periodo, che nel far salve le eccezioni e le limitazioni a favore degli enti pubblici senza scopi di lucro, come biblioteche e archivi, stabilisce che esse andrebbero comunque limitate a determinati casi specifici contemplati dal diritto di riproduzione e non dovrebbero comprendere l’utilizzo effettuato nel contesto della fornitura on-line di opere o altri materiali protetti. Ancora una volta dunque una “discriminazione” a scapito del *fair use* attuabile con tecnologie digitali, con conseguente possibilità di implementazione di mtp o, peggio, di sistemi DRM, almeno per la fornitura on-line. È netto il *vulnus* alla *e-democracy*, ai diritti del “*netizen*” (cittadino elettronico o della rete).

Per parte sua, il legislatore italiano, attraverso l’art. 71-quinquies, comma 1, della LDA, ha stabilito che

> «i titolari dei diritti sono tenuti ad adottare idonee soluzioni, anche mediante la stipula di appositi accordi con le associazioni di categoria rappresentative dei beneficiari, per consentire l’esercizio delle eccezioni di cui agli articoli 55, 68, commi 1 e 2, 69, comma 2, 70, comma 1, 71-bis e 71-quater, su espressa richiesta dei beneficiari ed a condizione che i beneficiari stessi abbiano acquisito il possesso legittimo degli esemplari dell’opera o del materiale protetto, o vi abbiano avuto accesso legittimo ai fini del loro utilizzo, nel rispetto e nei limiti delle disposizioni di cui ai citati articoli, ivi compresa la corresponsione dell’equo compenso, ove previsto»[25].

[25] Il comma 4 dell’art. 71-quinquies della LDA dispone che le associazioni di categoria dei titolari dei diritti e gli enti o le associazioni rappresentative dei beneficiari delle eccezioni possono svolgere trattative volte a consentire l’esercizio di dette eccezioni. In mancanza di accordo, ciascuna delle parti può rivolgersi al comitato consultivo permanente per il diritto di autore di cui all’art. 190 della LDA al fine dell’esperimento del tentativo di conciliazione, sorta di “alternative dispute resolution” o comunque di risoluzione della controversia in via stragiudiziale. Il tentativo di conciliazione è regolamentato dall’art. 194-bis della LDA. Per una breve, ma completa, analisi dell’istituto, v. Andrea Sirotti Gaudenzi, *Il tentativo di conciliazione obbligatorio e l’alternative dispute resolution nelle controversie legate alle “misure tecnologiche di protezione”*, http://www.notiziariogiuridico.it/sirotti_adr_copyright.html.

Orbene in merito a tali “eccezioni” e/o “limitazioni” all’uso di mtp e DRMS, occorre chiarire quanto segue:

- ai sensi dell’art. 69, comma 2, della LDA, per i servizi delle biblioteche, discoteche e cineteche dello Stato e degli enti pubblici è consentita la riproduzione, senza alcun vantaggio economico o commerciale diretto o indiretto, in un unico esemplare, dei fonogrammi e dei videogrammi contenenti opere cinematografiche o audiovisive o sequenze di immagini in movimento, siano esse sonore o meno, esistenti presso le medesime biblioteche, cineteche e discoteche dello Stato e degli enti pubblici;
- l’eccezione di cui all’art. 70, comma 1, della LDA è qui giustificata dall’esercizio di diritti costituzionalmente riconosciuti, garantiti e protetti: da una parte la libertà di critica e discussione, rientranti nella più ampia libertà di manifestazione del pensiero (art. 21 Cost.), dall’altra la libertà di insegnamento e di ricerca scientifica (art. 33 Cost.), in virtù dei quali sono liberi il riassunto, la citazione o la riproduzione di brani o di parti di opera e la loro comunicazione al pubblico;
- l’eccezione di cui all’art. 71-bis della LDA è per così dire un’eccezione “solidaristica”, a favore delle persone diversamente abili alle quali sono consentite, per uso personale, la riproduzione di opere e materiali protetti o l’utilizzazione della comunicazione al pubblico degli stessi, purché siano direttamente collegate alla loro specifico *status*, nei limiti di quanto è richiesto dal medesimo, e non abbiano carattere commerciale.

Ad integrazione di quanto sopra visto, si tengano presenti le seguenti considerazioni:

- l’art. 2 del ddl S1861 (*Disposizioni concernenti la Società italiana degli autori ed editori*), approvato definitivamente dal Senato il 21/12/2007 e ormai in vigore, per quel che concerne gli usi liberi didattici e scientifici, ha introdotto, dopo il comma 1 dell’articolo 70 della LDA, il comma 1-bis, che così recita:

> «È consentita la libera pubblicazione attraverso la rete internet, a titolo gratuito, di immagini e musiche a bassa risoluzione o degradate, per uso didattico o scientifico e solo nel caso in cui tale utilizzo non sia a scopo di lucro. Con decreto del Ministro per i beni e le attività culturali, sentiti il Ministro della pubblica istruzione e il Ministro dell’università e della ricerca, previo parere delle Commissioni parlamentari competenti, sono definiti i limiti all’uso didattico o scientifico di cui al presente comma».

Il riferimento alle immagini e musiche a bassa risoluzione o degradate fa certo pensare a formati audio, video, o audio-video cosiddetti "compressi", per es. le estensioni .mp3 o .avi, spesso presenti nelle piattaforme di *file-sharing* (es. eMule, eDonkey, Kazaa ecc.);

- quanto alle persone diversamente abili, in Italia esiste la l. 9 gennaio 2004, n. 4, cosiddetta *legge Stanca* (dal nome dell'allora Ministro per l'Innovazione e Tecnologie), recante *Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici*, accompagnata dal regolamento di attuazione contenuto nel d.p.r. 1 marzo 2005, n. 75[26]. E l'accessibilità dei più deboli può essere garantita solo eliminando o consentendo di eliminare le mtp e i sistemi DRM;
- per un altro aspetto, le modalità proprietarie (pagamento di determinati diritti o contributi, limiti d'uso o di tempo per la consultazione ecc.), adottate dalle pubbliche amministrazioni per la gestione di banche dati pubbliche, non convincono, in quanto la pubblica amministrazione è servente nei confronti dei cittadini, svolgendo funzioni e offrendo servizi nell'interesse pubblico generale. Allo stesso modo in cui preferibile sarebbe l'uso di programmi *open-source* o a codice sorgente aperto (v. lett. d) del comma 1 dell'art. 68 del CAD – Codice dell'amministrazione digitale[27]) rispetto a quello di programmi proprietari (lett. c) del comma 1 dell'art. 68 cit.). Sarebbe altresì consigliabile il cosiddetto riuso del software (v. lett. b) del comma 1 dell'art. cit.). Tutte soluzioni queste che garantirebbero quella interoperabilità invocata dal comma 2 dell'art. 68 cit.[28], ma che oggi stenta a decollare (si pensi al fatto che in circolazione ci sono troppe *smart-card*: CIE, CNS, tessera sanitaria ecc.), quando invece potrebbe bastarne una o al massimo due per erogare tutti i servizi richiesti dal cittadino alla pubblica amministrazione[29].

Pubblico dominio, usi didattici e scientifici, persone diversamente abili, documenti e contenuti di uso e interesse pubblico: tutte esigenze che si devono tradurre in diritti soggettivi pieni, inderogabili, incomprimibili da tecnologie cieche e sorde, fredde, inflessibili, restrittive come i DRMS, degne solo di un mondo orwelliano da *Big Brother* o del peggior *Panopticon* di Jeremy

[26] Si ricordi che il cons. 43 della direttiva EUCD stabilisce che «è in ogni caso importante che gli Stati membri adottino tutte le opportune misure per favorire l'accesso alle opere da parte dei portatori di un handicap che impedisca di fruirne, tenendo particolarmente conto dei formati accessibili».

[27] D.lgs 7/03/2005 n. 82 e successive modificazioni.

[28] Anche l'art. 69, comma 2, del CAD richiama l'importanza dell'interoperabilità, al fine di favorire il riuso dei programmi informatici di proprietà delle Pubbliche Amministrazioni, tant'è che nei capitolati o nelle specifiche di progetto deve essere previsto, ove possibile, che i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme.

[29] In tal senso, v. Diego Zanga, *Lettera aperta alla senatrice Magnolfi: proposte concrete per l'open source nella PA italiana*, http://www.computerlaw.it/entry.asp?ENTRY_ID=280.

Bentham, ove tutto è sperimentazione, analisi e controllo, ove la legge non è fatta e applicata più dall'uomo, ma da macchine, ove la cultura, la lingua, il pensiero stesso sono continuamente sorvegliati, limitati, confinati[30].

Per rendersi meglio conto di quanto detto, basti pensare ad alcuni casi clamorosi in cui a fronte della grandezza dell'ingegno umano e della sua creatività si pone la scarsa lungimiranza (meglio, miopia, se non addirittura cecità) della legge, quando essa si assoggetta ai desiderata di pochi.

Un primo caso fu quello che vide coinvolto nel 2000 l'esimio prof. Edward W. Felten dell'università di Princeton del New Jersey. La Secure Digital Music Initiative (SDMI) indisse una sorta di gara per testare la resistenza delle misure di protezione, da essa prodotte (nel caso di specie trattavasi si *digital watermarking*) e apposte a file musicali, e per verificare alfine se esse fossero davvero efficaci o se invece potevano essere forzate o *bypassate*. La sfida fu raccolta dal prof. Felten e vide coinvolti anche altri ricercatori e studiosi sia dell'università di Princeton sia della Rice University di Houston. Il team guidato da Felten riuscì a violare senza problemi ben quattro sistemi di protezione, ottenendo conferme anche all'interno della SDMI stessa. Ma quando giunse il momento di proclamare i risultati, la SDMI negò (per ovvie ragioni) che Felten fosse riuscito a vincere la sfida. Pertanto, egli annunciò sul proprio sito web di voler pubblicare la relazione che aveva steso in merito e di presentarla a Pittsburgh, nel corso di un seminario che si sarebbe dovuto tenere nell'aprile del 2001. Con tale relazione Felten voleva rendere noti i risultati delle sue ricerche e dimostrare la scarsa utilità e la facile eludibilità dei sistemi DRM. Tuttavia ciò gli fu impedito e ne nacque una controversia legale, che vide Felten imputato di aver violato il DCMA (si ricordi che egli aveva commesso quattro "violazioni" e per ognuna erano previsti fino a 5 anni di reclusione!). La SDMI, con l'appoggio della Recording Industry Association of America (RIAA)[31] trascinarono in tribunale Felten, appoggiato tra l'altro dalla Electronic Frontier Foundation (EFF). Felten e la EFF si appellarono alla libertà di ricerca scientifica (e più in generale alla libertà di manifestazione del pensiero riconosciuta, garantita e tutelata dal primo emendamento della Costituzione degli

[30] E poco importa se v'è una parte di dottrina che parla di "interoperabilità" dei DRMS (DRM in grado di funzionare su ogni piattaforma digitale e che dunque, se possono essere rimossi dall'una, possono esserlo anche dalle altre; una sorta di DRM "intelligenti"). Il risultato non cambia: sempre controllo, identificazione, profilazione. Un po' come dire, usando l'espressione di Auguste Kerckhoffs, che «la sicurezza di un crittosistema non deve dipendere dal tener celato il crittoalgoritmo. La sicurezza dipenderà solo dal tener celata la chiave» (cosiddetta *Legge di Kerckhoffs*, v. Auguste Kerckhoffs, *La Cryptographie Militare*, «Journal des sciences militaires», vol. IX, 1883, p. 5–38). Insomma, a parer di chi scrive, rendendo *open* i sorgenti dei DRM non si risolvano i problemi.

[31] Organizzazione americana dell'industria discografica, associazione americana dei produttori discografici, fondata nel 1952. Rappresenta l'industria discografica americana e cura la certificazione per gli albi d'oro e di platino. Ad essa sono legate anche le cosiddette BIG Five: BMG, EMI, Sony, Universal Music e Warner Bros.: ci si riferisce a una quota di mercato ammontante al 95% circa di tutti i CD a livello mondiale.

U.S.A.) che veniva grandemente limitata, se non impedita, da talune disposizioni del DMCA (*Digital Millennium Copyright Act*). È fin troppo chiaro che non è possibile paragonare un'opera di elevato rilievo culturale e scientifico con un volgare atto di pirateria! La *querelle* si trascinò stancamente per mesi e Felten restò sempre in bilico, anche se alla fine la SMDI e la RIAA tacitarono il tutto asserendo che si trattò di un "errore" (sic!). A dire il vero, comunque, le suddette organizzazioni avrebbero desistito solo quando il Dipartimento di Giustizia aveva affermato che Felten non intendeva commettere una violazione pura e semplice dei sistemi di sicurezza in questione, ma solo effettuare uno studio; inoltre il Dipartimento stabilì in via di "interpretazione autentica" che il *Digital Millennium Copyright Act* non poteva e non può applicarsi agli scienziati che effettuano ricerche. Ma Felten e la EFF, pur rinunciando a successive azioni legali, hanno promesso di non abbassare la guardia di fronte a provvedimenti che minacciano i diritti e le libertà fondamentali delle persone in nome di interessi economici di parte.

Altro caso controverso fu quello dello scienziato russo Dmitry Sklyarov arrestato dalla FBI su denunzia del colosso Adobe (padre del formato per file di testo .pdf). Sklyarov, che rischiò ben 25 anni di reclusione (5 per ogni violazione, più o meno come Felten, che ne rischiò 20), si trova oggi in patria da uomo libero. La sua colpa era stata quella di aver distribuito un programma in grado di leggere, condividere, stampare e fare copie di *backup* di *e-book* in modi non previsti dalle licenze e dalla clausole contrattuali, nonché dalle regole tecnologiche della casa produttrice (la Adobe per l'appunto). Tra l'altro l'opera di Sklyarov era tanto più meritoria in quanto, nel software da lui implementato, erano incluse funzionalità *text-to-speech* per consentire anche ai non vedenti, attraverso il loro PC, di leggere!

Senza contare poi i danni apportati ai sistemi informatici e lettori CD e DVD dal famigerato *rootkit* della Sony/BMG[32]!

Negli U.S.A. il caso Sony/BMG ha avuto conseguenze di non poco conto. Per es. il Tribunale federale di Manhattan (New York) ha omologato un accordo raggiunto tra la Sony e i rappresentanti dei consumatori in base al quale tutti coloro che avessero acquistato CD infetti avrebbero potuto restituirli al produttore e ottenere nuovi dischi privi del sistema anti-copia (la decisione ha validità soltanto nel territorio degli Stati Uniti e riguarda i CD venduti nel periodo compreso tra il 1° agosto 2003 e il 31 dicembre del 2007). La Sony/BMG, secondo i termini dell'accordo, ha poi deciso di fermare la distribuzione di qualsiasi CD contenente la tecnologia DRM incriminata e, per evitare

[32] A riguardo del caso Sony/BMG, si consiglia la lettura di un interessante articolo a firma di Corrado Giustozzi intitolato (ironicamente, ma emblematicamente) *Attenti all'hacker, si chiama Sony/BMG…*, http://www.interlex.it/copyright/corrado24.htm.

ulteriori inconvenienti, si è obbligata a sottoporre l'uso di eventuali altri DRM al parere di periti ed esperti prima di installarli sui CD destinati al mercato internazionale. Altro accordo è stato raggiunto al cospetto della Federal Trade Commission: la Sony/BMG in tal caso si è impegnata a sostituire il CD infetto con uno privo del software nocivo almeno sino al 31 giugno 2007, a realizzare software per la disistallazione del rootkit, a corrispondere 150 dollari di rimborso agli utenti infettati e a mantenere notizia della causa sul proprio sito web per due anni[33].

Inoltre il comportamento della Sony/BMG potrebbe avere, almeno in Italia, un certo qual rilievo anche per l'ordinamento penale, potendovisi ravvisare più di una fattipsecie delittuale. Difatti si può ipotizzare la commissione dei reati di esercizio arbitrario delle proprie ragioni (*ex* art 392 c.p.), di diffusione di programmi atti a danneggiare sistemi informatici e telematici (*ex* art 615-quinquies c.p.) e di danneggiamento informatico (*ex* art 635-bis c.p.), anche in concorso materiale fra loro (v. artt. da 71 a 80 c.p.)[34]. Ipotesi di reato del suddetto tipo sono state poste all'attenzione del Nucleo Antifrode della Guardia di

[33] Tuttavia la stessa Sony/BMG non è rimasta a guardare, tant'è che ha citato in giudizio la Amergence Group Inc., nuova denominazione dell'allora fornitore di sistemi DRM SunnComm. In una denuncia presentata presso il Tribunale dello stato di New York, la Sony ha sostenuto che la tecnologia sviluppata dalla SunnComm era difettosa e ha sottolineato come quei difetti siano costati all'azienda almeno 12 milioni di dollari (per lo più necessari per tacitare le denunce dei consumatori e rispondere alle inchieste governative a seguito dall'infezione di massa). Per ulteriori approfondimenti, v. *Sony BMG denuncia gli autori del (suo) rootkit*, http://punto-informatico.it/p.aspx?i=2038494.

[34] In effetti la possibilità che si configurino tutta una serie di reati è dovuta al fatto che il "*rootkit*" è un vero e proprio *malware* o software malizioso o codice maligno, al pari di *virus*, *worm*, *trojan*, *dialer*, *backdoor*, *spyware* etc. Esso in realtà, nel caso della Sony, si è rivelato tale nelle conseguenze, non certo nell'intenzione iniziale di chi l'aveva progettato, che era solo quella di realizzare un Drms da applicare ai CD musicali.

Ad ogni modo è opportuno chiarire cosa è un rootkit. In poche e semplici parole, trattasi di un programma in grado di nascondere all'amministratore di sistema o al legittimo utilizzatore della macchina eventuali *backdoor* o altri programmi installati da un hacker, cracker o virus writer, insomma da malintenzionati, siano essi "pirati" o "untori" informatici. Lo scopo di tale istallazione è semplice: ottenere il controllo di un computer, sia in locale come un virus, sia da remoto come un trojan o uno spyware. Pertanto il rootkit è in grado di mascherare intrusioni o tentativi di accesso non autorizzati (perciò abusivi) e di rendere i virus da essi occultati immuni alla scansione di antivirus (esiste infatti una tipologia di virus chiamata "*virus stealth*", lett. "*virus invisibile*", che utilizza largamente queste caratteristiche), in tal modo compromettendo la sicurezza di qualsiasi sistema. Si può dire dunque che i rootkit riescano ad agire in maniera completamente invisibile, in quanto non vengono rilevati né dall'utente, né dai programmi applicativi né dai software di controllo come antivirus e antispyware. In definitiva sono "*software-fantasma*" (*ghostware*) in grado di agire occultamente, senza che il proprietario o l'amministratore della macchina se ne possa rendere conto. Anche se, va detto, in realtà esistono anche rootkit "*buoni*" (si pensi a quello della Norton System Works usato per facilitare la possibilità di ripristinare i files dal cestino). Tuttavia gli usi illeciti sono più frequenti, tanto più se si pensa che un rootkit può nascondere un virus o uno spyware ovvero riesce a sovrascrivere o a modificare o ad alterare altri programmi. Oggi per es. vengono usati come strumento di ricatto a scopo di profitto in mano a "cyber-mafie" (nel qual caso potrebbe concretarsi il reato di estorsione ex art. 629 c.p., oltre agli eventuali altri crimini informatici concorrenti) o come valido mezzo di spionaggio industriale e di concorrenza sleale.

Finanza da parte di un pool di legali per conto dell'ALCEI (*Associazione per la Libertà nella Comunicazione Elettronica Interattiva*) con un esposto presentato a Milano il 4 novembre 2005[35].

[35] Il testo integrale è consultabile all'URL http://www.interlex.it/copyright/esposto.htm.