1 – INTRODUZIONE

- Definizione di sistema DRM secondo il NIST (*National Institute of Standards and Technology*) americano: "**sistema di componenti e servizi basati su tecnologie dell'informazione che unitamente alle corrispondenti leggi, politiche e modelli di business hanno lo scopo di distribuire e controllare la proprietà intellettuale e i diritti relativi.**"

- Esempi più diffusi: **FairPlay** e **PlaysForSure** (audio), **CSS** e **AACS** (video), **SecuROM** e **Starforce** (contenuti videoludici).

- I sistemi DRM sono una **sottoclasse delle cosiddette TPM** (*Technical Prevention Measures*) – componenti comunque destinate al controllo di accesso e fruizione di contenuti protetti da *copyright*.

2 – IL PANORAMA NORMATIVO

- **1996**: I trattati **WIPO** (*World Intellectual Property Organization*) WCT e WPPT sono posti in essere. I trattati sanzionano apertamente la violazione, la circonvenzione e l'aggiramento dei sistemi di *Digital Rights Management*, indipendentemente dagli scopi o dalle finalità di queste azioni.

- **Art. 11 del *WIPO Copyright Treaty***: “Le parti contraenti dovranno fornire una protezione legale adeguata e degli strumenti legislativi efficaci contro la circonvenzione delle misure tecnologiche efficienti che sono usate dagli autori in relazione all'esercizio dei loro diritti secondo il presente Trattato o la Convenzione di Berna e che impediscono azioni, riguardo alle loro opere, che non sono autorizzate dagli autori coinvolti o dalla legge.”

I trattati WIPO sono stati recepiti dagli **USA** con il *Digital Millennium Copyright Act* del 1998, e dall'**Unione Europea** con la Direttiva 2001/29/CE.
In quanto legati agli accordi TRIPs del **WTO**, WCT e WPPT devono inoltre essere adottati da ogni paese membro o aspirante tale, e sono già stati sottoscritti da tutti i paesi membri dell'**OCSE**.

3 – LO TSUNAMI P2P

I circuiti di scambio P2P nascono con **Napster** nel 2000, fornendo al pubblico una tecnica di trasmissione dati che ha poi sia generato nuove aziende (**Skype**) che fornito a tutti una nuova ed economica tecnica di distribuzione di contenuti. Successivamente le reti P2P di massa diventeranno sia del tutto decentralizzate che molto più performanti (**BitTorrent**).

Secondo gli autori del cosiddetto ***darknet paper*** (Biddle *et al.,* 2002) queste reti continueranno ad esistere fintanto che permarranno tre condizioni:

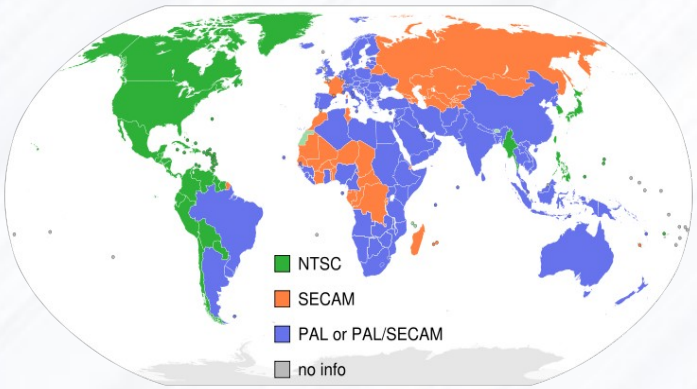
- ogni contenuto distribuito in massa sarà disponibile in un formato che ne permetta la copia ad una minoranza di utenti;
- gli utenti copieranno contenuti se sarà per loro possibile e vantaggioso farlo;
- gli utenti avranno a disposizione canali di comunicazione a banda larga.

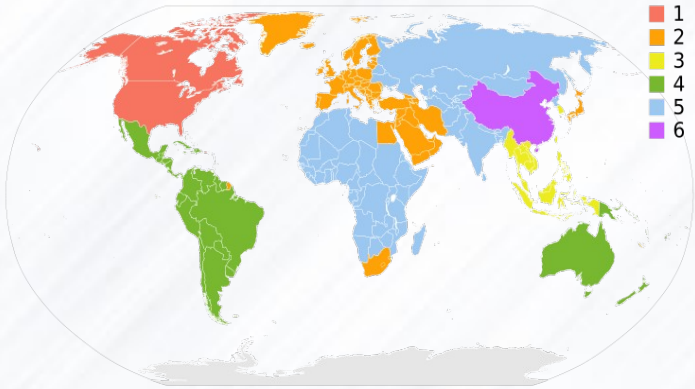
A meno di non voler sottoporre ad ispezione automatizzata **ogni trasmissione dati attraverso la rete**, questi circuiti di scambio (*darknet*) non potranno essere del tutto eliminati: questa la conclusione degli autori.

4 – *PRIVACY* E *COPYRIGHT*

La storia degli ultimi dieci anni indica che la *privacy* degli utenti e dei clienti non è certo stata una *issue*, anche solo periferica, per i molti consorzi che definiscono i termini di adozione di una nuova tecnologia.

- **1996**: in fase di definizione dello standard DVD come successore del VHS alcuni membri della **DVD-CCA** esaminarono il problema del come mantenere la codifica regionale – un problema da risolvere, secondo alcuni, tramite l'inserimento di un sistema GPS in ogni lettore venduto sul mercato.





"**Avete un'idea di quanto costassero allora i sistemi GPS?**" anonimo testimone della riunione in cui fu presentata la proposta (citato in Lasica, 2005; pp.23-24).

5 – CONTROMISURE

MPAA (*Motion Picture Association of America*), **RIAA** (*Recording Industry Association of America*) e **IFPI** (*International Federation of the Phonographic Industry*), si sono mosse su più fronti per combattere la pratica della condivisione illegale di contenuti protetti, e questo tramite

- uno **sviluppo sostenuto di sistemi DRM con funzioni e capacità sempre diverse**, in cerca di una soluzione che non arriva mai;

- l'**utilizzo di *contractors* privati**, dedicati all'inquinamento delle reti P2P e alla raccolta di indirizzi IP di utenti presumibilmente coinvolti nello scambio di contenuti protetti;

- **citazioni in giudizio**, dapprima contro sviluppatori di *software* dedicati alle reti P2P - in violazione della cosiddetta “dottrina Betamax” - e successivamente verso i singoli *filesharers*.

Ad oggi in America sono state intentate oltre 20.000 cause giudiziarie di questo tipo.

6 – *CASE STUDIES*

Due sistemi DRM, in particolare, danno credito a fin troppi possibili scenari negativi per quanto riguarda le interazioni tra questa traduzione teorica del copy*right* nel mondo digitale e la sicurezza operativa dei terminali di un numero notevole di persone.

2005: dopo il fallimento del sistema Copy Control, creato nel 2001 per cercare di impedire la pratica del *ripping*, Sony-BMG Music Entertainment incarica due società di creare dei nuovi DRM per sostituirlo:

- **SunnComm** (USA)
- **First 4 Internet** (Inghilterra)

(Entrambe, almeno fino ad allora, potevano tranquillamente essere definite come due sconosciute *start-ups* senza né arte né parte)

7 – SCOPI E FUNZIONI DI MEDIAMAX CD-3

- Il sistema di SunnComm generava il rischio di una ***privilege escalation*** su ogni terminale Windows in cui veniva installato - un processo che avveniva indipendentemente dall'assenso dell'utente e che si svolgeva in maniera del tutto invisibile;

- MediaMax CD-3 creava **forti vulnerabilità nei confronti di attacchi remoti**, oltre a installare un processo che era previsto inserirsi nel *kernel* ed eseguirsi indipendentemente dalla presenza o meno del contenuto protetto in questione;

- il sistema cercava di **bloccare il normale funzionamento del lettore ottico** per impedire la copia di ogni tipo di dati, quindi anche dati provenienti da supporti del tutto estranei al contenuto protetto;

- il sistema contattava regolarmente i *servers* di Sony BMG e SunnComm per **comunicare indirizzo IP e codice identificativo del CD**, anche in questo caso senza informarne l'utente medesimo.

8 – UN CURRICULUM ECLETTICO

Viste le caratteristiche del sistema MediaMax CD-3, è lecito chiedersi quali competenze e quali professionalità potesse vantare SunnComm. Ecco il loro *core business* fino al 2001:

Nel 2001, con la bolla delle *dotcom* in pieno svolgimento, SunnComm compra uno stabilimento per la produzione di supporti di stoccaggio portatili. Questi:

Poco dopo questa mossa di mercato, due impiegati - che avevano annunciato di volersi mettere in proprio per sviluppare sistemi DRM - furono assegnati alla conversione dell'azienda in questo senso, dando vita alla SunnComm responsabile di Mediamax CD-3.

9 – XCP-AURORA

Sviluppato dalla britannica **First 4 Internet** e rilasciato nelle copie di 52 titoli di catalogo del 2005. Qualche mese dopo il lancio delle copie sul mercato, Mark Russinovich diffuse i risultati delle sue analisi sui metodi e sulla struttura operativa del sistema.

"[XCP-Aurora] è **funzionalmente indistinguibile da un rootkit**." Mark Russinovich, Sysinternals, Ottobre 2005.

- **Installazione automatica ed invisibile del sistema**, non citata dalla EULA e non rifiutabile;
- **restrizioni indirette sull'uso**, non solo del CD in questione ma di ogni supporto ottico;
- **invisibilità garantita** ad ogni processo con l'iniziale sys, caratteristica molto presto notata - e sfruttata - da decine di altri sviluppatori di *malware*;
- **comunicazione continuata e indebita** (verso non meglio specificati lidi) dell'indirizzo IP dell'utente ad ogni fruizione del contenuto protetto.

10 – LE REAZIONI DEI MEDIA (E DI SONY)

In seguito alla scoperta di Russinovich ed allo studio approfondito dei sistemi DRM di SunnComm e First 4 Internet, la reazione dei media e del pubblico non si fece attendere.

- “Questo software è progettato per proteggere i nostri CD dalla copia non autorizzata e dal ripping, e la tecnologia rootkit è uno dei mezzi migliori per fare proprio questo. [...] **La maggior parte delle persone, penso, non sa nemmeno cos'è un rootkit, quindi cosa dovrebbe importargliene?**” (Thomas Hesse, direttore della produzione digitale mondiale di Sony-BMG, ai microfoni della radio di servizio pubblico americana NPR, 4 Novembre 2005)

- Dan Kaminsky, quantificò la propagazione dell'infezione in circa **568.000 reti private, pubbliche, militari e civili di tutto il mondo** tramite una serie di *queries* DNS.

- Persino il CERT, un'agenzia governativa americana appartenente all'onnipotente *Department of Homeland Security*, ha definito come *malware* il sistema XCP-Aurora per via delle vulnerabilità che ha creato all'interno dell'infrastruttura informatica americana, esortando i cittadini americani a non installare *software* “[...] **da fonti che non si ritiene debbano contenerlo, come un CD audio**”.

11 – ECCEZIONE O REGOLA?

Nonostante l'enorme danno di immagine di Sony-BMG e lo scandalo conseguente alle scoperte di Russinovich, molti altri sistemi DRM hanno dimostrato di poter rendere vulnerabili elaboratori privati e i dati personali in essi contenuti.

- **Starforce 3.0**: *privilege escalation* su terminali con diritti limitati.
- **SecuROM:** *privilege escalation* tramite il *driver* del sistema DRM.
- **Safedisc**: vulnerabilità ad accessi remoti con possibilità di esecuzione di codice esterno.

Tutti i sistemi DRM hanno in comune due caratteristiche: quella di considerare la propria utenza come disonesta a priori, e il loro naturale aggiramento nello spazio di qualche mese (problema ***trusted client***).

Paradossalmente, le copie disponibili tramite reti P2P di questi prodotti sono spesso paradossalmente più sicure di quelle originali. Inoltre i sistemi DRM ad autenticazione continua (come PlaysForSure) possono scadere, e quindi **negare un possesso completo dei prodotti acquistati**.

12 – TEORIE E PRATICHE

> “Non sapevamo nemmeno chi assumere. **Non saprei di certo riconoscere una persona con buone conoscenze tecnologiche** - qualunque persona con una buona stronzata da raccontare avrebbe passato il mio test personale”.
> Doug Morris, CEO di Universal Music Group, Dicembre 2007.

- **Audio**: i sistemi DRM per questi contenuti sono praticamente morti per volontà popolare, ma l'industria si sta rivolgendo a tecniche di *watermarking* dei dati personali degli acquirenti nelle copie digitali dei brani, o - come è già successo con Apple - inserendo in chiaro questi dati nelle *tags* dei file stessi.

- **Videogiochi**: un panorama in evoluzione, anche per via un mercato PC dal futuro incerto, ma con sistemi DRM ancora presenti in molti titoli oggi in commercio. Alcuni di questi sono stati trovati contattare i terminali della casa produttrice ad intervalli regolari.

- **Video**: con l'avvento del video in alta definizione, è indubbio che il nuovo campo di battaglia tra utenti e produttori di artefatti culturali di massa sarà la tutela del diritto di copia dei contenuti forniti in formato Blu-Ray - il settore dell'*home video* è infatti la fonte dei tre quarti circa degli introiti totali di Hollywood.

13 – LETTORI “INTELLIGENTI” (E INTOCCABILI)

Il sistema DRM dei DVD video, **CSS**, fu aggirato dall'ormai celeberrimo Jon Lech Johansen, e il suo successore, **AACS**, fu progettato per impedire il più possibile il ripetersi di questo evento. Ovviamente non funzionò.

Visto che AACS prevede un sistema di **revoca dei certificati**, l'eterno gioco di rimessa dei produttori di contenuti continua a svolgersi.

Lo standard Blu-Ray non solo contiene AACS, ma anche un sistema aggiuntivo di protezione, il BD+ - vale a dire una *virtual machine* progettata per eseguire ad intervalli regolari i seguenti compiti:

- **verifica dell'integrità** fisica e logica del lettore in questione;
- verifica dell'integrità delle **chiavi di decrittazione;**
- **decrittazione parziale** del contenuto video e audio;
- **esecuzione di codice**.

Queste caratteristiche, se sommate alla **presenza obbligatoria di una connessione Internet** all'interno del profilo più recente dello standard di Sony, tracciano i contorni di una situazione potenzialmente pericolosa.

14 – *A DAY IN THE LIFE*

Il pubblico è abituato ormai da più di vent'anni alla presenza di un riproduttore di contenuti video sotto al proprio televisore. Purtroppo il futuro dell'*home video* e dei diritti d'autore correlati dipinge un quadro in cui

- sarà proibito **modificare in ogni modo e per qualsivoglia scopo** i propri apparecchi, anche per scopi perfettamente legittimi;
- **ogni lettore farà capo ad un *database***, probabilmente condiviso tra più aziende;
- non vi è alcun modo di **sapere esattamente natura, numero e scopi** dei programmi fatti girare tramite *virtual machines* dal lettore ;
- i dati raccolti in questo modo sono sicuramente personali e altrettanto sicuramente utilizzabili **per scopi non corretti**.

15 – SOLI AL COMANDO

Produttori di apparecchi, venditori di supporti e lettori e produttori di contenuti spesso sono la stessa entità multinazionale.

- **Sony** ha comparti di produzione contenuti e di produzione di apparecchi, ed inoltre si sta allargando sul mercato della distribuzione digitale;
- **Amazon** ha da tempo avviato i propri servizi di vendita di contenuti in formato digitale (Amazon Unbox);
- **Netflix** (noleggio di supporti per via postale) sta stringendo accordi con parecchi produttori di apparecchi Blu-Ray;
- **Blockbuster** ha lanciato una OPA su Circuit City, una popolare catena statunitense di vendita di apparecchi e supporti.

Si va quindi verso una pericolosa verticalizzazione dell'offerta, con sempre più *walled gardens* a mantenere perpetua una clientela anche casuale.

In uno scenario del genere sono a rischio tanto la **libera competizione sul mercato** quanto la **tutela dei dati personali** di milioni di comuni cittadini.

16 – *WORST CASE SCENARIOS*

Volendo anche escludere possibili usi scorretti sul piano commerciale, è ragionevole accettare che questa raccolta di dati abbia luogo come conseguenza di un effetto non previsto della tutela accordata ai sistemi DRM dal WIPO?

- **Kerviel-Société Générale**: un 'quadro' medio-basso del gruppo bancario francese provoca un buco di qualche miliardo di Euro nei bilanci manipolando telematicamente gli investimenti del gruppo. Gli è stato sufficiente **avere l'accesso ai dati**.

- **Tavaroli-Telecom**: un *tiger team* con in mano le chiavi di accesso giuste, è capace di creare - su vasta scala ed illegalmente - profili di privati cittadini. È sufficiente **un database da qui attingere le giuste informazioni**.

- **Her Majesty's Revenue and Customs**: due dischi persi equivalgono alla messa in pericolo dei dati di due milioni di cittadini britannici.

1988: Robert Bork, candidato di simpatie repubblicane alla Corte suprema americana, subì un tentativo di gogna mediatica quando la sua lista di noleggi video fu rilasciata a mezzo stampa. Eventi come questo potrebbero ripetersi ad ogni fuga dei dati raccolti tramite piattaforme Blu-Ray, e su ogni tipo di scala.

17 – CONCLUSIONI

Il nascente mercato digitale sta dimostrando di essere, con tutta probabilità, il futuro prossimo venturo per i consumatori e i produttori di artefatti culturali di massa: un mercato, va sottolineato, impensato ed impensabile all'epoca dei trattati WIPO.

1996

In Italia il teatro La Fenice brucia. Deep Blue batte Kasparov. Windows 95 compie un anno. Yeltsin negozia un cessate il fuoco in Cecenia. Non esistono CD riscrivibili sul mercato. Nasce la pecora Dolly. La capacità di un disco fisso si misura spesso in MB. Ci sono le Olimpiadi estive ad Atlanta (e vanno forte gli Oasis). Apple compra NeXT. Esce Quake.

- È ragionevole continuare a fornire ai conglomerati dell'intrattenimento e alle tante piccole SunnComm del mondo carta bianca per quanto riguarda lo sviluppo dei loro sistemi DRM?

- Ed è ragionevole impedire ai consumatori di reagire in qualsiasi modo agli effetti negativi che queste tecnologie, del tutto in efficaci nei confronti dei "pirati", hanno invece su di loro?

"**Remember: a paranoid is simply someone in possession of all the facts**"
Warren Ellis, *Transmetropolitan*

18 – BIBLIOGRAFIA

ERCOLANI S. - *Il Diritto d'Autore e i Diritti Connessi*, Giappichelli, Torino 2004.

GOLDSMITH J., WU T. - *Who Controls The Internet?*, Oxford University Press, Oxford 2006.

LASICA J.D. - *Darknet*, Wiley & Sons, Hoboken 2005.

MASON M. - *The Pirate's Dilemma*, Free Press, New York 2008.

SCHNEIER B. - *Secrets & Lies* (2000), Wiley & Sons, Indianapolis 2004

.

BANERJEE A., FALOUTSOS M.,BHUYAN L.M. - P2P: Is Big Brother Watching You?, in *Technical Report UCR-CS-2006-06201*, Department of Computer Science and Engineering, University of California, Riverside, 2006.
[http://www1.cs.ucr.edu/store/techreports/UCR-CS-2006-06201.pdf]

BIDDLE P., ENGLAND P., PEINADO M., WILMMAN B. - The Darknet and The Future of Content Distribution, 2002.
[http://crypto.stanford.edu/DRM2002/darknet5.doc]

FELTEN E.W., HALDERMAN J.A. - Lessons from the Sony CD DRM Episode, in *Proceedings of 15th USENIX Security Symposium*, 1-3 Giugno 2006: 77-92.
[http://www.usenix.org/events/sec06/tech/full_papers/halderman/halderman.pdf]

FUGGETTA A. - The Net is Flat, in *CEFRIEL White Papers* n. 1, 2007.
[http://www.cefriel.it/index.php?option=com_content&task=view&id=44&Itemid=60&lang=it]

MULLIGAN D.K., PERZANOWSKI A.K. -The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident, in *Berkeley Technology Law Journal* vol.22/03, 2007.
[http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1072229_code698753.pdf?abstractid=1072229&mirid=5]

19 – RICONOSCIMENTO DIRITTI

IMMAGINI:

Slide 4 – Fig. 1: immagine “PAL-SECAM” rilasciata dall'autore nel pubblico dominio. Autore: Akomor1/Wikipedia.

Slide 4 – Fig. 2: immagine “Region Coding” tutelata sotto licenza GFDL. Autore: Monaneko/Wikipedia.

Slide 8 – Fig.1: immagine “Floppy” sotto tutela Creative Commons BY-SA 2.0. Autore: chrisjroos/Flickr.

Slide 8 – Fig.2: immagine “Elvis” sotto tutela Creative Commons BY-NC 2.0. Autore: rekkid/Flickr.