Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Curso de Ciência da Computação

THIAGO GONÇALVES DE MORAES

O Impacto das Tecnologias DRM no Direito do Consumidor

São Luís
2014

THIAGO GONÇALVES DE MORAES

O Impacto das Tecnologias DRM no Direito do Consumidor

Monografia apresentada ao Curso de Ciência da Computação da UFMA, como requisito parcial para a obtenção do grau de BACHAREL em Ciência da Computação.

Orientador: Maria Auxiliadora Freire

Profª. Msc. em Engenharia Civil

São Luís

2014

Moraes, Thiago Gonçalves

O Impacto das Tecnologias DRM no Direito do Consumidor / Thiago Gonçalves Moraes - 2014

64.p

1.Ciência da Computação 2.Computação e Sociedade 3.Direitos 4.DRM. I.Título.

THIAGO GONÇALVES DE MORAES

O Impacto das Tecnologias DRM no Direito do Consumidor

Monografia apresentada ao Curso de Ciência da Computação da UFMA, como requisito parcial para a obtenção do grau de BACHAREL em Ciência da Computação.

Aprovado em – 12/12/2014

BANCA EXAMINADORA

Maria Auxiliadora Freire

Profª. Msc. em Engenharia Civil

Samyr Beliche Vale

Prof Dr. em Informática

Carlos Eduardo Portela Serra de Castro

Prof Msc. em Informática

Dedico esta monografia a todos aqueles que me apoiaram e ajudaram a passar por essa etapa da minha vida. Colegas de curso, professores e em especial meus orientadores.

Agradecimentos

Aos meus professores pelo conhecimento que me foi passado... Aos meus orientadores, Francisco e Auxiliadora, pelo suporte dado para realizar este trabalho... Aos meus amigos pelo apoio... À minha família pela paciência e à minha namorada, Dannielle por tudo isso e ainda pelo incentivo, carinho e motivação.

Resumo

Este trabalho visa discorrer sobre a DRM e seus principais aspectos tecnológicos e impactos sociais, abordando desde seus componentes até o arcabouço legal desenvolvido para sustentar a tecnologia.

Palavras-chave: Gestão, Digital, Copyright, Consumidor, Direitos, Privacidade.

Abstract

This work aims to argue about DRM and its main technological aspects and social impacts, viewing from it's componentes to all the legal enforcement developed to sustain the technology.

Keywords: Management, Digital, Copyright, Consumer, Rights, Privacy.

A mente que se abre a uma nova idéia jamais voltará ao seu tamanho original.

(Albert Einstein)

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Siglas

AES Advanced Encryption Standard

CD Compact Disc

CSS Content Scrambling System

DES Data Encryption Standard

DMCA Digital Millennium Copyright Act

DOI Digital Object Identifier

DRM Digital Rights Management

DVD Digital Video Disc

ECAD Escritório Central de Arrecadação e Distribuição

FL FrontLine

IDPF International Digital Publishing Forum

IP Internet Protocol

ISAN International Standard Audivisual Number

ISBN International Standard Book Number

ISSN International Standard Serial Number

MPEG Moving Picture Experts Group

PC Personal Computer

P2P Peer-to-Peer

REL Rights Expression Language

SSL Secure Sockets Layer

TLS Transport Layer Security

XCP Extended Copy Protection

XML Extensible Markup Language

WIPO World Intellectual Property Organization

WMA Windows Media Audio

WMV Windows Media Video

1 Introdução

A DRM, ou Gestão de Direitos Digitais, pode ser definida como: " *(...) a classe de tecnologias utilizadas por fabricantes de hardware, editores, proprietários de Copyright e indivíduos com o objetivo de controlar o uso de conteúdo digital pós venda.*"[1]. Por possuir tais características acabou se tornando uma classe particularmente controversa, pois tem por intuito gerir a cópia, reprodução e alteração de conteúdos digitais.

Sendo assim, primeiro precisamos definir o que é Propriedade Intelectual, uma vez que o conceito de *Copyright* deriva deste, que segundo a WIPO é:

> "Propriedade Intelectual se refere as criações da mente, como invenções; obras literárias e outras artes; *designs*; e símbolos, nomes e imagens utilizadas em divulgação."[2]

E dentro do escopo da Propriedade Intelectual destacam-se 2 grupos [3].

- Propriedade Industrial: Inclui patentes para invenções, marcas registradas, nomes comerciais, designs industriais, proteção contra competição injusta e indicações geográficas.
- *Copyright*: Inclui obras literárias (novelas, poemas e peças), filmes, músicas, obras artísticas (desenhos, pinturas, fotografias e esculturas) e arquitetura. Direitos relacionados a *Copyright* também incluem aqueles de performances de artistas e produções musicais.

A propriedade intelectual está relacionada a informações ou conhecimentos, as quais podem ser incorporadas em objetos tangíveis ao mesmo tempo em ilimitadas cópias ao redor do globo. A propriedade não está nas cópias em si, mas no conhecimento refletido nas mesmas. A importância da propriedade intelectual foi reconhecida pela primeira vez na Convenção para Proteção da Propriedade Industrial em Paris, França (1883) e na Convenção para Proteção da Literatura e Obras Artísticas em Berna, Suiça (1886), ambos os tratados assinados nessas convenções são agora administrados pela WIPO.

De acordo com a WIPO, a definição de *Copyright* é:

> "*Copyright* é um termo legal utilizado para descrever os direitos que os criadores tem sobre suas obras. Obras abrangidas pelo Copyright vão de livros, músicas, pinturas, esculturas e filmes até programas de computador, banco de dados, propagandas, mapas e desenhos técnicos."[4]

Como é possível ver, o *Copyright* é um conceito muito abrangente. E ele também possui uma particularidade muito importante, é um direito normalmente concedido por um período finito de tempo e dá ao criador não só a permissão de fazer cópias como também de receber crédito pela utilização do material, de escolher quem pode adaptar seu trabalho, reproduzi-lo e até mesmo quem pode ser financeiramente beneficiado por ele. [4] Direito esse que está apresentado na Declaração Universal de Direitos Humanos, art 27. [5]

> "(1) Todos tem o direito de participar livremente da vida cultural de sua comunidade, de desfrutar das artes e compartilhar do conhecimento científico e seus benefícios.
> (2) Todos tem o direito a proteção de sua moral e aos proveitos decorrentes de produções científicas, literárias ou artísticas das quais ele mesmo seja o autor."

Outra definição de *Copyright* pode ser encontrada no Oxford Dictionary como: "*O exclusivo direito legal dado a um criador ou procurador de imprimir, publicar, representar, filmar ou gravar material literário, artístico ou musical, e de autorizar outros a fazer o mesmo*". E esse material passível de *Copyright* subsiste mais especificamente de obras de autorias originais em meios tangíveis de expressão, os quais possam ser reproduzidos ou de alguma forma comunicados, seja diretamente ou com a ajuda de algum dispositivo. Estão incluídas obras nas categorias a seguir, de acordo com a lei de *Copyright* dos EUA. [6]

- Obras Literárias;
- Obras Musicais, incluindo quaisquer letras que possam a acompanhar;
- Obras Teatrais, incluindo quaisquer músicas que possam a acompanhar;
- Pantomimas e obras coreográficas;
- Obras pictóricas, gráficas e esculturais;

- Filmes e outras obras audiovisuais;
- Gravações de áudio;
- Obras Arquitetônicas.

Incluem-se também compilações e obras derivadas, mas a proteção desse tipo de conteúdo faz necessário que o material preexistente utilizado não possua *Copyright* abrangendo toda e qualquer parte da obra.

O *Copyright* da compilação ou obra derivada se aplica somente ao material agregado pelo autor para a criação do mesmo e não implica em qualquer tipo de direito sobre o material preexistente. Os direitos de tal obra são independentes e não afetam ou expandem o escopo, duração ou propriedade dos direitos sobre o material preexistente. [6]

E é a partir desse *Copyright* que a DRM é formada. A análise tecnológica irá mostrar exatamente como se aplica esse controle dos direitos. Contudo é facil perceber a tênue linha entre a garantia dos direitos dos detentores do *Copyright* e a garantia do direito de uso do consumidor sobre o material adquirido, e é exatamente esse o grande desafio da DRM, garantir os direitos de *Copyright* sem afetar a experiência do consumidor, funcionando da forma mais transparente possível.

Neste contexto conceitual, observar-se que a DRM surgiu para controlar a cópia de materiais pelos usuários, limitando os consumidores nos usos dos conteúdos digitais. Esta capacidade, de interferir na maneira como o produto é consumido, que tornou a DRM uma tecnologia controversa, uma vez que ela tange desde a produção até o consumo do mesmo, podendo armazenar informações dos usuários, rastrear seus hábitos e disseminar estas informações para terceiros. Podendo assim, infringir alguns direitos dos consumidores e até impossibilitando atividades completamente legais, como realizar cópias de backup de CDs ou DVDs que possuam a tecnologia.

O principal objetivo da DRM é de preservar os interesses dos detentores do *Copyright*. Em seu início, a intenção era de somente controlar a cópia do material, mas em sua segunda geração a DRM controlava a visualização, cópia, impressão, alteração e até os dispositivos nos quais o conteúdo era utilizado. [7]

E levando em consideração a evolução da internet e dos dispositivos de mídia (CD/DVD), é fácil compreender a preocupação das grandes empresas e detentoras de

Copyrights em fazer valer seu direito num ambiente com cópia e distribuição tão facilitada, estas empresas se viram na necessidade de desenvolver uma tecnologia que pudesse impor as restrições de *Copyright* no ambiente digital. As mídias analógicas inevitavelmente perdiam qualidade com cada cópia gerada, no entanto as mídias digitais podem ser copiadas sem praticamente nenhuma perda de qualidade nas cópias. A evolução dos mecanismos digitais de cópia a tornou uma tecnologia disruptiva com forte impacto na indústria de entretenimento, principalmente para os mercados cinematográfico e fonográfico.

1.1 Objetivo Geral

Considerando os aspectos apresentados sobre a DRM e as consequências de seu uso para a sociedade, o presente trabalho visa discutir o embate entre os detentores de *Copyright* e os direitos dos consumidores, trabalhando com um contexto histórico, tecnológico e social.

1.2 Objetivos Específicos

- Abordar os conceitos necessários para a melhor compreensão da DRM;
- Analisar os requisitos necessários para a construção de uma tecnologia DRM;
- Compreender a arquitetura básica e os componentes necessários a DRM;
- Compreender como um sistema DRM funciona, entendendo seu fluxo de informação e quais técnicas são utilizadas para garantir sua eficiência;
- Analisar tecnologias específicas vendo inclusive seu impacto nos consumidores;
- Entender as necessidades dos consumidores e o impacto que as restrições da DRM podem causar;
- Discutir sobre a complexidade em garantir a eficiência da tecnologia sem afetar os direitos de uso do consumidor.
- Analisar a DRM no cenário brasileiro e discutir sobre as possíveis adequações necessárias para a evolução da tecnologia.

1.3 Organização do Texto

Capítulo 2: Análise Tecnológica. Demonstra o modelo da tecnologia DRM e seu fluxo de informação, assim como analisa algumas tecnologias mais específicas.

Capítulo 3: DRM e a Sociedade. Faz uma abordagem de um ponto de vista mais social, discutindo sobre o arcabouço legal necessário para que a tecnologia pudesse ser eficiente e principalmente sobre o impacto de seu uso na sociedade.

Capítulo 4: DRM dentro do âmbito do Brasil. Analisa o cenário brasileiro relacionado a DRM e aborda alguns pontos necessários para a adequação da tecnologia no país.

2 Análise Tecnológica

A DRM é um modelo de tecnologia que pode seguir diversas abordagens, podendo ser mais ou menos intrusiva e usando diversas arquiteturas diferentes. Mas, apesar de ter um modelo particularmente flexível, a tecnologia conta com alguns requisitos e componentes básicos para o seu funcionamento. [8] Atributos esses que serão explicitados a seguir.

2.1 Requisitos do DRM

Essa seção vem essencialmente detalhar os pré-requisitos desejáveis para os sistemas DRM, os quais podem ou não existir nas arquiteturas atuais.

2.1.1 Usabilidade(*User Friendly*)

A Usabilidade é um dos critérios de maior impacto, pois o provedor do serviço DRM deve garantir que seu sistema é de fácil uso para todos os grupos envolvidos no fluxo de distribuição. Qual seria o motivo para um consumidor alternar para um novo sistema se ele é confuso e problemático? Esse argumento é válido não somente para o consumidor final como também para outras entidades envolvidas no processo, como detentores de *Copyright* e distribuidores de conteúdo, já que o sistema precisa apresentar benefícios para todos os envolvidos até que seja devidamente adotado.

2.1.2 Confiabilidade

A confiabilidade trata do quanto os envolvidos precisam estar seguros de que o sistema irá se comportar da maneira que foi planejada. Em especial de como os detentores dos direitos irão estar certos que o conteúdo não será compartilhado para além das pessoas que adquiriram direitos sobre o mesmo. Já no outro lado têm-se o usuário final, que deseja ter seu acesso garantido ao conteúdo que ele adquiriu.

2.1.3 Segurança

A segurança é uma das características que também costuma estar entre as de maior preocupação quando se fala em DRM. Mesmo assim é muito difícil achar um sistema que seja 100% seguro, isso se dá, em boa parte, pelo fato de que o endurecimento da segurança traz consigo um custo bem alto, que é o de diminuição do conceito de Usabilidade. Mas apesar de não se ter a garantia de que os sistemas DRM realmente sejam capazes de alcançar 100% de segurança, outro ponto também é levado em consideração para justificar a segurança nem tão elevada assim, o custo, pois é completamente inviável proteger um conteúdo que possui valor X com um sistema de segurança que custa 2X. Sendo assim, o nível de segurança do DRM precisa se adequar a necessidade do conteúdo.

Outro aspecto associado a segurança é a robustez do sistema, que se trata da dificuldade em remover os dispositivos de segurança, permitindo que mesmo que um conteúdo tenha sua segurança quebrada, ele possa ser depois identificado como uma cópia ilícita. A marca d'agua digital [1] é uma das tecnologias utilizadas nos DRMs para conseguir atingir esse objetivo.

2.1.4 Flexibilidade

A distribuição online é um método relativamente novo de oferecer conteúdo ao consumidor, o que faz com que seja normal que esse método seja abordado por várias maneiras diferentes. Torna-se importante então que o DRM seja flexível o suficiente para conseguir trabalhar com essas novas ideias e conceitos sem que sejam necessários *upgrades* uma vez que as abordagens devem se tornar bem mais complexas do que os modelos mais antigos de assinatura e *pay-per-view*.

2.1.5 Implementabilidade

A implementabilidade é um item de especial interesse aos fabricantes de dispositivos, pois diz respeito aos recursos necessários para suportar um sistema DRM. Os algoritmos escolhidos para um DRM tendem a serem definidos de acordo com o tipo de

[1] É uma tecnologia de segurança que trabalha com a inserção de um pequeno ruído no conteúdo, para que se possa identificar a origem do conteúdo

dispositivo no qual o conteúdo pretende ser distribuído(um leitor de *e-books* por exemplo, será trabalhado com algoritmos que levem em consideração sua menor memória e poder de processamento em relação a um computador).

Sendo assim, as capacidades dos dispositivos podem servir como severos meios de restringir as capacidades técnicas do DRM. Itens a serem analisados incluem capacidade de memória, processador e até mesmo requisitos específicos de hardware ou software, como o sistema operacional.

A conectividade também por ser um problema. Se o sistema DRM necessitar de uma conexão permanente com o servidor a quantidade de dispositivos os quais esse sistema é aplicável torna-se bem restrito. Como, por exemplo, o uso desse sistema em um *Player* portátil de músicas.

2.1.6 Código aberto

Esse é um tópico que começa a ser discutido como forma de aumentar a atratividade da tecnologia e potencializar o seu uso. Assim como possui a vantagem de melhorar o acesso e a quantidade de desenvolvedores e sistemas, também deverá facilitar o acesso do código a pessoas que tenham como único objetivo o de criar mecanismos que possam contornar a DRM e acessar o conteúdo ilegalmente.

Uma maneira possível de aumentar a abertura do código é o de criar padrões que podem manter alguns componentes mais seguros e ainda assim garantir que a partir desse "núcleo"inicial possam ser desenvolvidos sistemas genéricos e capazes de trabalhar melhor com novos tipos de dispositivos e conteúdos.

2.1.7 Interoperabilidade

Bastante relacionado a Usabilidade e Abertura de Código é a Interoperabilidade, que lida com a capacidade dos sistemas DRM de lidarem com outros sistemas. Por exemplo, ao adquirir um *ebook* protegido por DRM o usuário precisa se preocupar se esse conteúdo será lido corretamente pelos leitores de *ebooks* que ele possui em seu PC e *tablet*. Será se alguma conversão será necessária? E se for, quão trabalhoso e custo será esse processo?

Dispositivos, serviços e conteúdos devem ser suficientemente interoperáveis

para que o conteúdo possa ser distribuído eficientemente, de forma que nenhum desses 3 sirvam de empecilho para a utilização do conteúdo. Embora várias tentativas de distribuir música protegida tenham sido feitas, os *players* capazes de reproduzir essas músicas eram relativamente restritos além de possuir um problema ainda mais grave, que era o de diferentes distribuidoras possuírem tecnologias DRM incompatíveis. Isso tornava impossível a reprodução de vários conteúdos diferentes pelo mesmo *player*, já que cada tecnologia podia estar associada a um software diferente. O resultado disso foi que a maioria das músicas distribuídas fossem aquelas sem proteção DRM. Pois como foi citado anteriormente, a usabilidade é uma das principais características a serem analisadas por um sistema DRM, pois foi exatamente ignorando essa característica que o DRM foi ineficiente para proteger o conteúdo mp3.

Existem alguns padrões para as interfaces DRM lidarem com interoperabilidade, a MPEG com seu MPEG-4, que buscava trazer um padrão para identificação e proteção de conteúdo. No entanto, sistemas DRM com interfaces e componentes abertos são coisas que os experts em segurança são veementemente contra, fato que se foi verificado na quebra do CSS, que era o padrão de protecão de conteúdo em mídias físicas (CDs, DVDs), mostrando que até mesmo um padrão completamente revisado tem suas fraquezas. [8]

Outro aspecto importante é referente aos *upgrades* dos sistemas. O sistema, quando atualizado, tem compatibilidade com a versão antiga? Se não for, então como atualizar o sistema de um conteúdo que o usuário já possui? Pois se tal atualização impactar, ou até mesmo impedir, o uso do conteúdo adquirido, que segurança os consumidores terão em adquirir algo com uma tecnologia que pode inutilizá-lo depois? O mesmo também é aplicável se a atualização for um processo muito complexo e custoso.

2.1.8 Custo

O custo também deve ser levado em consideração. Não só o custo para desenvolvimento e manutenção da tecnologia como principalmente o custo para embutir a proteção nos conteúdos. Pois se for exigido um processo muito custoso para proteger os conteúdos as distribuidoras do conteúdo não terão interesse em adquirir esse tipo de tecnologia, até porque esse se tornará um custo associado que será repassado a um consumidor que irá exigir vantagens por esse preço mais caro.

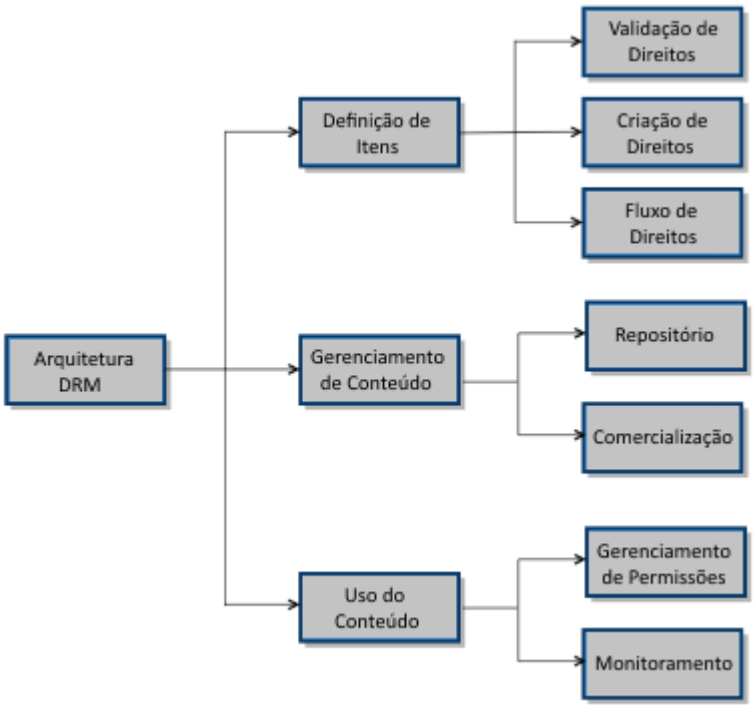

Figura 2.1: Arquitetura de um Sistema DRM Genérico [9]

2.2 Arquitetura Funcional

Não existe uma arquitetura padrão para o DRM, cada desenvolvedor pode criar a sua própria. No entanto, toda arquitetura segue modelos bem semelhantes, como mostrado no modelo genérico apresentado na figura 2.1.

O modelo apresentado na fig. 2.1 é definido em 3 partes: Definição de Itens, Gerenciamento de Conteúdo e Uso do Conteúdo.

2.2.1 Definição de Itens

Essa parte se refere ao processo de criar e gerenciar a propriedade intelectual de forma a simplificar sua comercialização. Esse módulo é dividido em:

- Validação de Direitos: Garante que conteúdo criado de algo já existente pode ser realmente feito.
- Criação de Direitos: Trata da alocação de direitos ao novo conteúdo especificando quais são os dos proprietários do conteúdo e quais as permissões de uso aceitáveis.

- Fluxo de Direitos: Permitir que o conteúdo possa passar por uma série de etapas para que os direitos e conteúdos possam ser aprovados e revisados.

2.2.2 Gerenciamento de Conteúdo

Trata do processo de gerenciar e permitir a comercialização de conteúdo. Os dados gerenciados aqui incluem metadados como utilização, pagamento, entre outros. Sendo divido em:

- Funções do Repositório: Permite o acesso de dados e metadados.
- Funções de Comercialização: Permite a emissão de licenças para aqueles que estão autorizados a acessar o conteúdo. Em alguns casos o conteúdo pode ter que passar por etapas de aprovação antes de ter a licença emitida. Como por exemplo, o conteúdo ter sido criptografado para o uso em um dipositivo específico.

2.2.3 Uso do Conteúdo

Esse módulo se refere a utilização do conteúdo depois dele ter sido comercializado. É composto basicamente de:

- Gerenciamento de Permissões: Permite a aplicação dos direitos associados especificamente a esse usuário e conteúdo. Por exemplo, o usuário tem o direito de leitura do arquivo mas não o de impressão.
- Monitoramento: Permite o monitoramento no uso do conteúdo, o qual deve estar indicado nas licenças de uso do material. Como por exemplo, um usuário que tem o direito de executar o conteúdo somente 5 vezes, ou o usuário que só pode fazer 2 cópias do conteúdo.

2.3 Componentes de um sistema DRM

Para entender melhor o funcionamento da DRM é necessário entender exatamente como funciona o fluxo da informação dentro desse sistema e depois entender os componentes pelos quais o fluxo passa. O Fluxo é essencialmente composto por 3

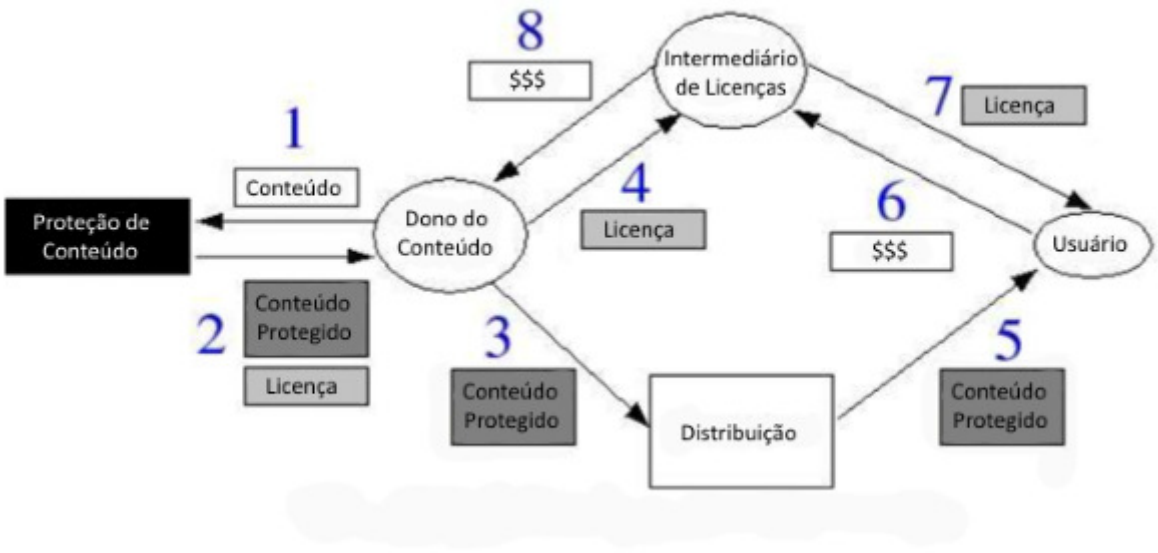

Figura 2.2: Fluxo do sistema DRM [10]

personagens apresentados na figura 2.2, Dono do Conteúdo, Intermediário de Licenças e Usuário.

O Dono do Conteúdo normalmente é aquele que possui os direitos sobre o conteúdo, podendo ser uma gravadora musical, uma empresa de jogos ou mesmo um artista solo. O Intermediário de Licenças é o responsável por todas as transações referentes ao conteúdo em questão e o usuário final, sendo o responsável por especificar o tipo de acesso concedido ao usuário final. O Usuário se refere a um hardware/software confiável que funciona como um proxy para o consumidor. É dito confiável por ser feito para coibir o acesso não autorizado ao conteúdo e é através desse recurso que se implicam as regras definidas pelo Intermediário de Licenças.

1. O Dono do Conteúdo vai adequar os dados para o a área de Proteção do Conteúdo. Como por exemplo o caso da Microsoft DRM, que exigia que a mídia estivesse em formato .WMA ou .WMV. Nesta etapa também há a possibilidade de se inserir uma marca d'agua digital, a fim de facilitar a verificação da autenticidade dessa midia. O Dono do Conteúdo então especifíca a regra ou conjuntos de regras aplicáveis a essa mídia, considerando o fato de que podem existir vários tipos de acessos diferentes disponíveis aos usuários finais, como por exemplo a distinção que algumas empresas utilizam, de usuário *Basic* com acesso relativamente restrito e usuário *Premium* com acesso superior.

2. O Sistema DRM então retorna 3 objetos, o Conteúdo Protegido, a Licença e a Chave.

O Conteúdo Protegido é o arquivo que será executado pelo usuário final. A Licença corresponde as regras as quais esse arquivo está configurado para esse usuário específico, ou seja, cada tupla Usuário, Conteúdo tem uma Licença específica. A Chave depende somente do Conteúdo e é necessária para descriptografar os dados requisitado.

3. O Dono do Conteúdo então faz a distribuição do Conteúdo Protegido, podendo esse ser de várias formas: CD/DVD, emails, compartilhamento P2P [2]. A distribuição feita online permite que os usuários compartilhem o material livremente, mas ainda garante o controle do Dono do Conteúdo uma vez que os usuários ainda precisam da Licença para ter acesso ao conteúdo.

4. O Dono do Conteúdo envia a Licença para o Intermediário de Licenças, sendo esse o responsável por lidar com todas as transações referentes ao acesso daquele conteúdo, podendo assim deixar o Dono do Conteúdo focado na melhoria e/ou desenvolvimento de novos conteúdos.

5. O Usuário recebe o Conteúdo Protegido e a partir da análise de seus metadados, identifica o Intermediário e as suas Licenças disponíveis para que possa ter acesso ao conteúdo.

6. Se o Usuário não possuir uma Licença, ou se a Licença que ele possui não for mais válida, ele solicita ao Intermediário de Licenças uma que esteja de acordo com o tipo de acesso que ele deseja, fazendo então o pagamento da mesma.

7. Após o pagamento, o Intermediário de Licenças envia a Licenças junto com a Chave, para que o usuário possa enfim descriptografar o conteúdo e ter o acesso especificado na License que ele acaba de adquirir.

8. O Intermediário de Licenças então repassa o pagamento ao Dono do Conteúdo, podendo também repassar algumas informações relevantes sobre os usuários.

Pode-se facilmente ver algumas diferenças impostas pelo uso da DRM. Primeiramente na geração do conteúdo, que em alguns modelos específicos, as vezes faz com que o conteúdo precise ser modificado antes que possa ser protegido. Um exemplo

[2] O P2P é uma arquitetura de compartilhamento descentralizada, no qual cada ponto da rede funciona tanto como cliente como servidor, eliminando a necessidade de um servidor central.

é o modelo da Microsoft DRM, que necessita que o conteúdo esteja em um formato específico, no caso .WMA ou .WMV, para que a segurança possa ser implementada nesses arquivos. Outra diferença causada pela DRM está na oportunidade de se realizar a distribuição por meio dos usuários, não mais dependendo de grande alocação de recursos dos desenvolvedores de conteúdo, pois o material agora exige uma Licença para que possa ser propriamente acessada pelos usuários finais.

Outra mudança importante se dá no modelo de negócio, pois agora o comércio não tem mais como foco o conteúdo, uma vez que esse já pode ser livremente compartilhado entre os usuários, agora toma-se como foco a licença de uso sobre esse conteúdo. [10]

2.4 Técnicas de Segurança

Muitas técnicas diferentes são utilizadas para prover proteção aos sistemas DRM, muitas vezes sendo inclusive utilizadas em conjunto para aumentar ainda mais a segurança. A seguir apresentam-se algumas das principais técnicas utilizadas e uma breve análise das mesmas.

2.4.1 Criptografia

A criptografia consiste de embaralhar o conteúdo ou uma chave necessária para abrir o mesmo, de forma que torne o conteúdo impossível de ser lido a não ser pelo recipiente que contém o código necessário para descriptografá-lo. Além de precisar de um algoritmo robusto e seguro para garantir a segurança da criptografia, outro aspecto muito importante é o gerenciamento das chaves de descriptografia para garantir que ela seja enviada para os usuário de forma segurança, impendido seu roubo e comprometendo assim a eficiência dessa técnica. A criptografia costuma ser utilizada sempre em conjunto com outras técnicas.

2.4.2 Certificados Digitais

Assim como uma pessoa precisa se identificar para conseguir realizar algumas atividades, os certificados digitais funcionam como a maneira de provar sua identidade no

meio digital. O certificado digital é o link entre a pessoa e sua identidade virtual, ela é criada associando a pessoa com sua chave criptografada. A assinatura digital é enviada por uma autoridade de certificação que visa garantir que a chave pertence a mesma pessoa indicada no certificado.

2.4.3 Marca D'água Digital

Marca D'água é o processo de incluir dados ocultos juntos do conteúdo. É uma maneira de digitalmente incluir uma espécie de selo de *Copyright* no conteúdo. A Marca D'água no entanto não pode alterar ou atrapalhar a usabilidade do conteúdo, devendo ser totalmente invisível para o usuário final.

2.4.4 Protocolos de Comunicação Segura

SSL e TLS são alguns dos protocolos criptografados que provêem uma comunicação segura pela Internet. Eles foram desenvolvidos de forma a garantir uma comunicação cliente/servidor de forma a impedir a captura, interceptação ou qualquer outra forma de acesso aos dados da comunicação.

Também têm-se o IP Security, que é um padrão de comunicação utilizado para criptografar todos os pacotes enviados pela rede e assim potencializar seu nível de segurança.

2.4.5 Impressão Digital

A Impressão Digital é outro mecanismo também utilizado para aumentar a segurança dos sistemas DRMs, só que ele é utilizado mais como forma de rastreamento do que necessariamente proteção contra cópia, como a maioria dos outros mecanismos.

A Impressão Digital eletrônica procura codificar cada cópia com os dados do usuário que está adquirindo o conteúdo, de forma a identificar cada cópia com um código exclusivo. Caso cópias ilegais sejam realizadas, os dados do primeiro usuário persistirão, sendo possível assim rastreá-lo e acusá-lo pela atividade ilegal.

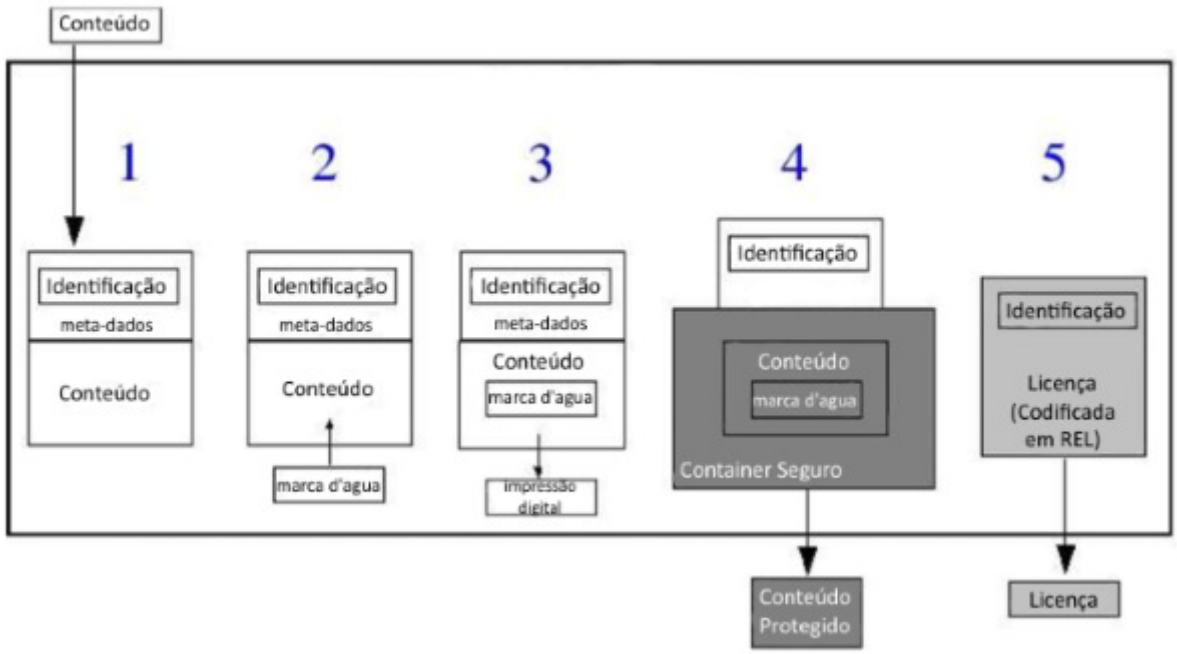

Figura 2.3: Processo de proteção de conteúdo [10]

2.4.6 Hash

Outro mecanismo de proteção contra cópias ilegais é a chamada "*one-way hash*". Que é um algoritmo que pega o conteúdo e a partir dele gera um código extremamente específico, de forma que qualquer pequena alteração no conteúdo, mesmo que seja imperceptível, irá gerar um código completamente diferente. Ao adquirir um conteúdo o consumidor pode utilizar esse mecanismo para verificar o código do conteúdo adquirido é igual ao de um original, caso sejam iguais o consumidor pode ter a certeza que possui uma cópia original.

2.5 Proteção de Conteúdo

Para analisar o componente de segurança de um modelo genérico de DRM, apresenta-se a figura 2.3, que é a representação da parte interna do item Proteção de Conteúdo indicado na figura 2.2.

1. O conteúdo é marcado com um identificador único e são inseridos metadados que ajudam a identificá-lo.

   Identificador: Além de precisar ser necessariamente único, o identificador tem

que ser persistente, isso significa que mesmo que o proprietário do conteúdo seja modificado, a identificação deve permanecer sempre a mesma. Mas além de ser utilizado para tornar o conteúdo único, o identificador também pode ser utilizado para procurar conteúdo relacionado ou até mesmo versões similares do mesmo conteúdo pois o Identificador é gerado seguindo padrões internacionais como o ISBN, ISSN, ISAN e DOI.

Metadados: Os metadados complementam o uso do Identificador, pois por si só, ele não faz muito sentido. Em geral são os metadados que descrevem o conteúdo e como eles devem ser acessados, podendo inclusive definir também as regras de uso do conteúdo.

2. Uma marca d'água (*watermark*) digital é inserida no conteúdo para indicar o material como original.

Marca D'água Digital: É uma tecnologia desenvolvida para controle de cópia, identificação de conteúdo e rastreamento. A maioria das técnicas de marca d'agua trabalham com a inserção de um pseudo ruído de pequena amplitude diretamente no conteúdo ou em sua frequência (dependendo do tipo de conteúdo em que está se inserindo a marca d'agua). Essa marca depois pode ser detectada utilizando um conjunto de métodos e geralmente uma chave oculta, para garantir que a marca d'agua só possa ser detectada e/ou alterada por pessoas autorizadas.

Os sistemas DRM são particularmente vulneráveis de ataques do lado do usuário, seja por captura do conteúdo durante sua renderização (audio ou video) ou tendo seu Container Seguro (item 4 da fig. 2.3) removido ou inutilizado por meio de ataques diretos. No primeiro caso pode-se detectar que o conteúdo é ilegal pois não é possível capturar a marca d'água por meio de softwares de captura de audio/video, uma vez que o ruído é visível somente a nivel de código. No segundo caso a detecção é possível uma vez que ao fazer a validação e encontrar a marca d'água, se irá também procurar o Container Seguro associado a essa marca, não encontrado-o percebe-se então o conteúdo como ilegal.

Sendo assim, a marca d'água Digital funciona sobre 3 requisitos: Imperceptibilidade, a marca não pode afetar a qualidade visível do conteúdo.

Segurança, a marca não pode ser acessada por pessoas não autorizadas. Robustez, a marca deve ser persistente e resiliente a ataques.

Entretanto a marca d'agua Digital pode ter efeitos colaterais que a tornem inviável, como visto em [11]. O efeito da Marca D'agua em imagens de satélite acabou gerando classificações incorretas, assim podemos perceber que um conteúdo que precisa passar por análises muito minuciosas, ou conteúdos muito sensíveis, pode ser prejudicado pelo uso desta técnica, uma vez que ela modifica ligeiramente o conteúdo.

3. Aplica-se outra técnica de segurança, a impressão digital. Nesta etapa ela é gerada e então salva no banco de dados. Ela é útil para a identificação automática de conteúdo.

   A impressão digital é uma técnica de Identificação Baseada no Conteúdo, pois ela funciona como uma caracterização da representação (sinais ou funcionalidades) do conteúdo. Ela funciona de uma maneira bem diferente da Marca D'água Digital, mas apesar disso ainda existe uma certa confusão entre os termos. A principal diferença entre as duas é que a impressão digital é uma saída gerada a partir do conteúdo ao invés de ser embutida dentro do conteúdo. A tabela 2.1 mostra uma comparação que pode exemplificar melhor a diferença entre essas duas técnicas.

   O processo de impressão digital se divide basicamente em 2 etapas, o treinamento, onde as características do conteúdo são extraídas e armazenadas em um banco de dados, e o reconhecimento, que é basicamente o reconhecimento dos padrões do conteúdo de forma a comparar com os arquivos do treinamento que se encontram no banco de dados.

   Algumas características essenciais da impressão digital são a robustez e a compactação. As técnicas mais robustas são capazes inclusives de detectar variações (como versões diferentes) do conteúdo original. A compactação é essencial para realizar uma extração, identificação e comparação veloz.

4. O conteúdo é então protegido por um container de segurança, o qual vai efetivamente impedir o acesso não autorizado.

Tabela 2.1: Principais Diferenças entre Marca D'água e Impressão Digital [10]

Marca D'água	**Impressão Digital**
Embute um sinal no conteúdo, alterando sua codificação	Não embute sinal, não alterando assim seu código
Não é uma função do conteúdo	Uma função do conteúdo
Deve ser invisível, para evitar detecção	Não possui tal preocupação. Não intrusivo.
Requer acesso prévio ao conteúdo	Não requer acesso prévio. Pode ser usado em "conteúdo legado"
Pode proteger cópias de forma individualmente personalizadamente	Não possui essa capacidade
Precisa reprocessar todo o conteúdo em caso de troca de tecnologia.	Não precisa reprocessar conteúdo
Não precisa realizar tratamento adicional para novas cópias	Precisa armazenar a "digital"do novo conteúdo no banco de dados

Os containers são geralmente implementados usando criptografias do tipo DES [3] e AES [4] . Também é comum utilizar-se de ofuscação de código [5] para aumentar o nível de segurança, isso junto com a utilização de assinaturas digitais e certificados torna o container mais confiável.

É importante perceber que é o Container de Segurança o responsável pela alteração no modelo de negócio de venda de conteúdo online. Onde antes tanto o conteúdo quanto sua chave eram enviados juntos, agora eles estão separados. A proteção do conteúdo é feita offline e a chave de segurança é obtida posteriormente. Isso permite uma distribuição menos restrita e muito mais veloz do conteúdo, mas tem como principal desvantagem o fato de possuir uma mesma chave de segurança para todas as cópias do conteúdo.

[3] o DES foi o método de criptografia definido como o Padrão para o Processamento de Informação nos EUA por muitos anos.

[4] O AES é o atual método Padrão para o Processamento de Informação dos EUA sendo hoje utilizado no mundo todo.

[5] Ofuscação de código é uma técnica de programação que visa ocultar o funcionamento real do código por meio da adição de linhas de código irrelevantes, a fim de confundir e dificultar técnicas como a engenharia reversa

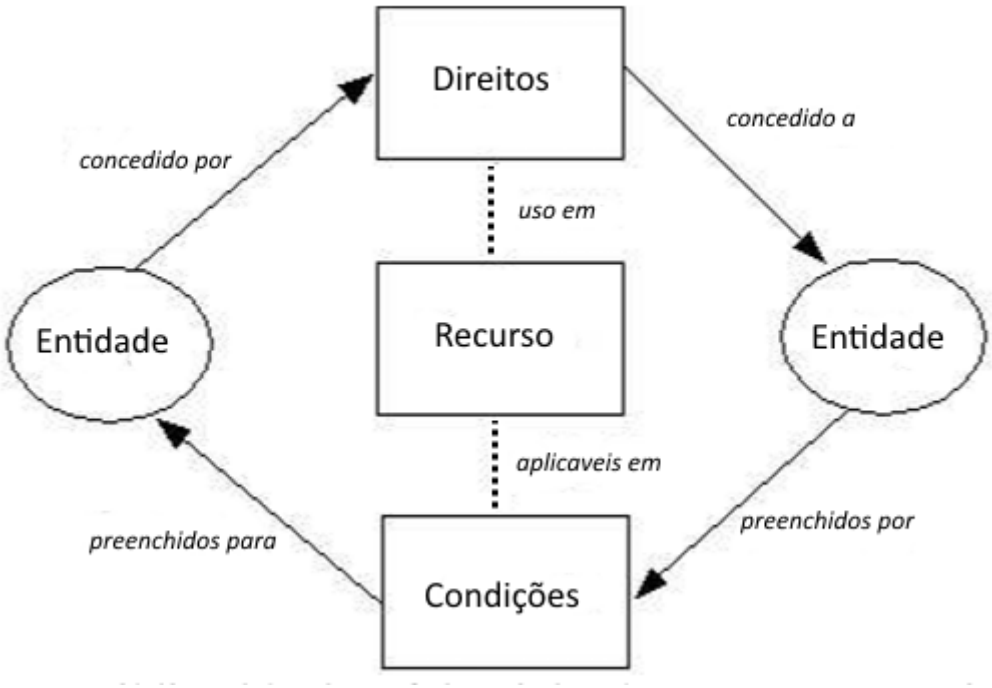

Figura 2.4: Conceito dos blocos de uma REL [10]

5. Uma licença que explicita os direitos e condições de uso do conteúdo é descrita em uma linguagem específica conhecida como REL.

   A REL é uma linguagem em XML e seu principal objetivo é de definir licenças e descrever essas licenças em termos de quais permissões e restrições os usuários terão sobre aquele conteúdo, pode-se ver o relacionamento desses blocos na figura 2.4. Em geral, os blocos necessários para a construção do código REL são os seguintes:

   Direitos: As permissões sobre o uso do conteúdo, aqui é onde se incluem restrições como quantidade limitada de vezes que o material pode ser reproduzido.

   Condições: Os pré-requisitos que precisam ser atendidos antes de ter acesso aos direitos.

   Recurso: O conteúdo em questão, que deve possuir uma identificação única.

   Entidade: Os envolvidos na transação.

   É também importante lembrar, que para garantir a segurança das licenças, elas só podem ser construídas e/ou modificadas por pessoas autorizadas e também que uma licença não pode ter informação suficiente para que se possa gerar

outra licença a partir dela. A validade e integridade da licença sempre deve ser verificada antes de habilitar o conteúdo.

2.6 DRM e Jogos Eletrônicos

No campo dos jogos eletrônicos, após um recorde de vendas em 2013, alcançando mais de 93 bilhões de dólares, existe um crescimento esperado para mais de 100 bilhões em 2014 [12]. Vendo esse enorme crescimento, as empresas da área tiveram a necessidade de adaptar e até mesmo retirar as DRM's de forma a facilitar o crescimento do mercado.

O principal foco do DRM nos jogos é impedir a cópia do conteúdo dos CDs e em alguns casos limitar a quantidade de instalações dos jogos. Ressaltando que esse último gerou muitas críticas dos consumidores e até mesmo da própria indústria, pois algumas vezes deixavam um jogo impossível de ser jogado depois de um certo tempo de ser adquirido e além disso muitos usuários consideravam o sistema muito intrusivo e diziam afetar suas experiências com o jogo.

Ao longo dos anos várias tecnologias foram utilizadas, cada uma com sua abordagem específica, algumas perduraram (geralmente as menos intrusivas) e outras fracassaram, a seguir serão apresentados alguns DRMs utilizados ao longo dos anos na indústria de jogos.

2.6.1 SecuRom

É uma tecnologia proprietária desenvolvida pela Sony que tem como objetivo impedir a cópia dos softwares em CDs assim como a engenharia reversa dos mesmos.

De acordo com a própria Sony, esse tecnologia tem duas formas de proteção de conteúdo. A primeira é alcançada através de softwares com uma robusta criptografia, a segunda tem um processo bem mais complexo e é alcançada pelo hardware. Durante o processo de produção dos CDs uma assinatura é incluída em cada disco. No momento da inicialização uma rotina de validação verifica a assinatura para garantir que o CD é original, se a validação falhar o usuário irá receber uma mensagem informando que o conteúdo não será executado.

A SecuRom também oferece um serviço de ativação online, o qual é similar com a verificação via hardware. Nesse método uma licença é obtida online e então salva no computador, sempre que o conteúdo for executado essa licença será verificada, se ela não existir ou não for mais válida o usuário receberá uma mensagem de erro.

Muitas controvérsias surgiram em torno dessa tecnologia, entretanto, boa parte delas foram em jogos que utilizavam uma versão alterada do SecuROM e que continham componentes que ficavam ocultos e agiam de forma muito mais intrusiva que o SecuROM padrão. O jogo The Sims 2 era protegida pelo SecuROM e possuía severos problemas quanto a erros de execução, falhas no driver de leitura de CDs, interferia com programas antivírus e até mesmo falhas completas do sistema operacional. BioShock, que também foi distribuído com o SecuROM incluía uma ativação personalizada e um número limitado de instalações. A repercusão dos consumidores acabou sendo bem negativa, levando a desenvolvedora do jogo a retirar essas restrições cerca de 1 ano depois do seu lançamento. [13]

2.6.2 Steam

A Steam é uma plataforma de distribuição digital, *multiplayer* e de comunicação lançada em Setembro de 2012 pela Valve. A Steam gerencia a DRM dos jogos distribuídos por ela, depois de comprados e baixados, os jogos devem ser lançados pela própria plataforma a qual pode inclusive gerenciar jogos adquiridos por outros meios que não a loja online da Steam, mas nesse caso ela não interfere no DRM já existente no jogo. Para rodar os jogos é gerado um executável personalizado que é único para aquele usuário/jogo e que é autenticado por uma cópia local das credenciais daquela pessoa.

Portanto, possui a possibilidade de abrir e rodar jogos sem necessitar de uma conexão com a internet, sendo necessário somente que já se tenha o jogo instalado e atualizado até sua versão mais recente. Algumas funcionalidades se tornam indisponíveis no modo offline, mas ainda assim é uma opção muito útil para quando se tem problemas na conexão ou nos servidores Steam. Outra interessante funcionalidade é a de realizar os backups dos jogos de forma bastante simples, sendo facilmente restaurados em caso de formatação ou troca de máquina.

Quando lançada a Steam possuia apenas jogos da sua desenvolvedora, a Valve, mas ao passar dos anos outras companhias de jogos foram sendo incluídas no portfolio da

Steam, trazendo não só jogos recém lançados como alguns jogos antigos também. Essas características tornaram a Steam uma das plataformas DRMs de mais sucesso do mundo, sendo responsável por 75 % de todos os downloads para jogos para PC em outubro de 2013. [14]

2.6.3 StarForce

StarForce é um software de proteção contra cópias com o objetivo de coibir a pirataria. É um software especialmente conhecido no mundo dos jogos por possuir técnicas muito invasivas, as quais podem causar problemas como falhas nos leitores ópticos dos PCs. Existem várias variações do software e cada uma foi desenvolvida para proteção num nível diferente.

O nível mais básico de proteção oferecido pelo StarForce é o FL *Disc*, que inclui funções como proteção contra cópia e emulação ilegais. Existem ainda níveis dentro do próprio FL Disc, sendo os mais altos desenvolvidos para dissuadir até mesmo os mais habilidosos hackers. o FL Disc pode proteger tanto CDs como DVDs. [14]

O próximo nível do StarForce é o FL Universal, que oferece muitas da funcionalidades já existentes no FL Disc e ainda traz a possibilidade de proteger conteúdo que não é distribuído por mídias físicas. Isso é alcançado pela verificação online do código de série. Outras funcionalidades são, controlar a quantidade de vezes que o jogo é ativado e quanto tempo é necessário até que uma reativação seja exigida.

Como parte do FL Disc e FL Universal, tem-se a tecnologia DiscFree, que provê mais algumas funcionalidades que podem ser customizadas para a desenvolvedora do game, como por exemplo permitir que o usuário jogue sem precisar do CD original, sendo necessário somente na instalação e primeira vez que o jogo é executado. Permitindo assim mais comodidade e reduzindo o stress do leitor óptico.

2.7 DRM e a Música

A passagem da DRM pela indústria da música também não foi muito diferente da ocorrida na indústria de jogos, muitas das tentativas de aumentar a segurança das mídias físicas ou digitais se provaram ou extremamente intrusivas e em alguns casos até

mesmo danosas aos dispositivos dos clientes, ou fracas e ineficientes. Um dos casos mais famosos da DRM em mídias físicas é o da Sony XCP que eram não somente fracas, pois ainda permitiam que o seu conteúdo fosse gravado e reproduzido como também instalava um programa na máquina dos usuários sem que eles tivessem conhecimento e que podia inclusive deixar o driver de CD dos computadores inoperantes. A Sony sofreu um processo público e consequentemente abandou a tecnologia. [14]

Hoje em dia existem lojas de música online que oferecem material com proteção DRM, entretanto, devido a característica analógica do audio, a proteção acaba se tornando frágil e é facilmente quebrada. Com isso muitas companhias optaram por oferecer material livre de DRM. A seguir apresenta-se algumas das tecnologias DRM usadas na indústria musical, a Sony XCP e a Apple FairPlay.

2.7.1 Sony XCP

Com a popularização da venda de música em CDs, as companhias fonográficas começaram a procurar maneiras de impor o *Copyright* e coibir a pirataria. As primeiras tentativas de proteção eram falhas e simples de serem evitadas. Ao perceber isso e com a esperança de proteger sua lucratividade e seus direitos, a Sony então licenciou comercialmente o produto de duas empresas especializadas em DRM. A First 4 Internet e a SunnComm desenvolveram, respectivamente, o XCP e o MediaMax CD-3.

Em junho de 2004 a Sony começou a comercializar CDs com as nova tecnologias, 52 álbuns foram distribuídos com a XCP e 50 com MediaMax. Ambas as tecnologias foram desenvolvidas para instalar softwares ocultos que tinha por objetivo monitorar e impedir acessos não autorizados como mais de 3 cópias do CD ou conversão para MP3. Ambos foram depois classificados como *malwares* (softwares maliciosos), por alterar o funcionamento normal dos PCs sem qualquer autorização. Além disso, um efeito colateral não esperado foi o de abrir brechas que permitiam os acessos de outros programas maliciosos como vírus, cavalos de tróia. [14]

Depois de mais de um ano, em Outubro de 2005, a falha foi descoberta e o software foi considerado malicioso, a Sony então trabalhou para prover um desinstalador que pudesse remover esses softwares. Entretanto, o desinstalador também era falho, o que ocasionou um desastre ainda maior, estima-se que mais de 500 mil computadores foram infectados. Ainda em dezembro de 2005 a Sony liberou um desinstalador funcional e os

softwares foram enfim removidos.

2.7.2 Apple FairPlay (iTunes)

O iTunes é uma software que permite que os usuários baixem, organizem e reproduzam vários tipos de arquivos digitais como músicas, vídeos, séries e filmes. O iTunes foi criado em Janeiro de 2001, exclusivamente para Macs, e precedeu o lançamento de um de seu player portátil, iPod, em Outubro de 2001. Em 2003 a loja digital do iTunes é lançada já com sua própria tecnologia DRM embutida.

FairPlay foi a tecnologia desenvolvida pela Apple especialmente para o conteúdo do iTunes. A tecnologia usa criptografia AES juntamente com hashes MD5 para gerenciamento das chaves, ela possuir uma chave mestra para descriptografar e uma chave de usuário que descriptografa a chave mestra, ambas ficam armazenadas junto com os dados do conteúdo.

Devido ao fato das chaves estarem junto com o arquivo, elas ficam particularmente vulneráveis a ataques como engenharia reversa ou então explorando o processo de autenticação tentando se passar pelo software legítimo para conseguir destravar as chaves escondidas. Por esses motivos a Apple acabou abandonando a tecnologia e anunciou conteúdo livre de DRM em 2009. [13]

2.8 DRM e os E-books

Em se tratando dos E-books, o debate sobre sua eficiência e retorno financeiro é ainda mais forte. Alguns argumentam que o DRM em E-books torna a publicação trabalhosa e complexa, enquanto outros acreditam que elimininando ou pelo menos diminuindo as restrições que a DRM impõe seja melhor financeiramente devido a facilidade de se publicar e de adquirir os livros. Assim aumentam-se as compras legais e o efeito da pirataria é diminuido.

Nesse contexto, o grande desafio da DRM é o de conseguir desenvolver tecnologias robustas o suficiente para suportar a rápida evolução e variedade dos dispositivos capazes de ler E-books. Como resultado disso as tecnologias acabam se tornando obsoletas pouco tempo depois de serem adotadas. Duas tecnlogias utilizadas

nesse meio serão apresentadas a seguir, a Mobipocket e Topaz e a Microsoft Reader.

2.8.1 Mobipocket e Topaz

A Amazon desenvolveu sua versão de DRM para o Kindle, inclusives para as aplicações para PC (K4PC) e iPhone/iPod, a criptografia era feita a partir de uma chave por dispositivo que era válida para todo o conteúdo restringido, o algoritmo de criptografia foi desenvolvido pela própria Amazon. A versão para PC ainda se utilizava de uma chave por livro que era usada na descriptografia. A grande diferença e o que garantia um alto nível de segurança dessa tecnologia era a complexidade do algoritmo que era utilizado para ocultar essas chaves. [13]

2.8.2 Microsoft Reader

Microsoft Reader é o aplicativo para leitura de E-books da Microsoft, ele lê somente arquivos no formato lit. O controle é feito em 3 níveis, cada um com um crescente nível de restrição. O primeiro nível é chamado de "*sealed*" e não possui restrições, somente impede a alteração no texto do documento. O segundo nível é chamado de "*inscribed*" e possui um identificador digital que reconhece o proprietário do documento, dificultando assim o compartilhamento do arquivo. O terceiro e último nível é chamado de "*owner exclusive*" e tem o arquivo criptografado e associado a conta do usuário, além disso, o único dispositivo capaz de visualizar o documento é aquele que fez seu *download*. [13]

3 DRM e a Sociedade

A DRM é uma tecnologia que lida diretamente com os conceitos de privacidade e *Copyright*, então é difícil abordar a tecnologia sem analisar todos os pontos associados a ela. Por trabalhar com um conceito legal, como é o do *Copyright*, a DRM teve a necessidade de também se inserir no campo legal. As relações da DRM com esses outros itens serão analisadas a seguir.

3.1 Legalização da DRM

Para ter respaldo legal e para garantir que seu objetivo principal, que é o de proteger os interesses dos detentores de *Copyright*, seja alcançado várias leis relacionadas a DRM foram desenvolvidas. Essas leis definiam o escopo da DRM e inclusive garantiam que a quebra desse mecanismo de segurança fosse vista como uma infração legal.

Primeiramente temos a lei do *Copyright*, (*Copyright Act*), a qual enumera as atividades legais aquele que é o proprietário da obra, pois ela não da o controle total da obra aos proprietários dos direitos, na seção 106 da lei [6] são enumeradas as atividades definidas como "Direitos Exclusivos", as quais são garantidas aquele que tem posse da obra. São elas:

> "(1) direito de reproduzir obra protegida em cópias ou registros fonográficos;
> (2) direito de preparar obras derivadas baseadas na cópia protegida;
> (3) direito de distribuir cópias ou registros fonográficos da obra protegida para o público por meio de venda ou outra transferência de posso, ou por aluguel, arrendamento, ou empréstimo;
> (4) no caso de obras literárias, musicais, teatrais e coreográficas, pantomimas, e filmes ou outras obras audiovisuais, o direito de apresentar esse material protegido publicamente;
> (5) no caso de obras literárias, musicais, teatrais e coreográficas, pantomimas, e graficamente ilustrado, ou esculpido, incluindo as imagens individuais de um filme ou outra obra audiovisual, o direito de exibir esse material protegido

publicamente; e

(6) no caso de gravações de som, o direito de apresentar esse material protegido publicamente por meios de transmissões digitais."

3.1.1 DMCA

Para garantir a eficácia da DRM, os financiadores da mesma precisavam de suporte legal para sua tecnologia. Em 1998 foi conseguido que o governo dos Estados Unidos aprovasse a DMCA, a qual criminalizava a produção e disseminação de tecnologias, serviços ou dispositivos com a intenção de quebrar o DRM impostos pelos detentores de *Copyright* e inclusive criminalizava quebrar o DRM mesmo que o material não fosse protegido por *Copyright* [15]. Essa lei blindava o DRM de forma que as grandes organizações poderiam ter seu respaldo legal que qualquer tentativa de remover seu mecanismo de segurança seria completamente ilegal. Segue parte do texto da DMCA. [16]

"(...) cria-se duas novas proibições no artigo 17 do Código dos E.U.A, um sobre o contorno das medidas tecnológicas utilizadas para proteger os detentores de direitos autorais e suas obras e um sobre a adulteração das informações de gestão dos direitos de *Copyright*. E adiciona reparação civil e sanções penais por violar essas proibições."

Contudo, esse foi só o primeiro passo da DRM no âmbito legal. Em 22 de maio de 2001 foi aprovado pelo Parlamento Europeu, o decreto 2001/29/EC [17] "*on the harmonisation of certain aspects of copyright and related rights in the information society*" que instituía um conjunto de regras muito semelhante ao da DMCA para os EUA, conforme descrito no artigo 6, capítulo 3 desse decreto.

"(...) 2. Membros do Estado devem prover adequada proteção legal contra fabricação, importação, distribuição, venda, aluguel, propaganda para venda ou aluguel, ou posse para motivos comerciais de dispositivos, produtos ou componentes ou a provisão de serviços que:

(a) são fomentados, divulgados ou comercializados com o objetivo de contornar, ou

(b) tem uma restrita finalidade comercial de uso para outros objetivos além de contornar, ou

(c) são especialmente concebidos, produzidos, adaptados ou utilizados para o objetivo de permitir ou facilitar o contorno de, qualquer medida tecnológica efetiva."[17]

E a partir da blindagem adquirida com essa lei e do amplo controle da DRM sobre o material em que ela era inserida, que se criou uma grande controvérsia e debate sobre o seu uso, pois a DRM impossibilitou atividades plenamente legais, como fazer cópias de backup de CDs ou DVDs, emprestar materiais por meio de uma biblioteca, acessar obras de domínio público ou usar materiais protegidos por copyright para pesquisa e educação de acordo com as leis de uso aceitável (*Fair Use Doctrine*).

3.1.2 DMCA e o Fair Use

A doutrina de uso aceitável é definido pela Iowa State University como:

"permite ao tribunais evitar aplicações rígidas das leis de *Copyright* quando, na ocasião de, reprimir a criatividade o qual a lei foi desenvolvida para nutrir."[18]

Ela foi originada nos Estados Unidos com o objetivo de garantir que os direitos dos detentores de Copyright não interferissem no compartilhamento de conhecimento científico ou do aprendizado, pois a partir dela é possível o compartilhamento de material protegido por *Copyright* sem ter necessariamente autorização do proprietário do conteúdo. Ela entrou como um adendo a lei geral de *Copyright* dos EUA, sendo encontrada na seção 107 da lei [6] e sendo aplicável de acordo com uma análise dos itens a seguir:

"(1) para o objetivo ou caráter de uso, incluindo se tal uso é de natureza comercial ou para propósitos educacionais sem fins lucrativos;

(2) a natureza da obra protegida por Copyright;

(3) a quantidade e substancialidade da porção usada em relação ao material protegido como um todo; e

(4) o efeito do uso sobre o mercado em potencial ou o valor da obra protegida"

Graças a uma certa dificuldade em avaliar os itens definidos pela lei, ela deve ser analisada caso a caso pois funciona como uma exceção a lei de *Copyright* e não deve

ser utilizada com o objetivo de violação. Alguns exemplos do uso aceitável incluem comentários, críticas, reportagens, pesquisas, uso como material de ensino e acervo de bibliotecas.

Com a DMCA, o material protegido por DRM acaba tornando-se fora do alcance do uso aceitável, uma vez que o modelo de negócio mudou de foco do conteúdo para foco na licença e a tentativa de contornar a tecnologia se tornou um crime. A doutrina permitia aos consumidores "infringir"o *Copyright* sem medo de retaliação, contudo, a evolução da tecnologia e o advento da DRM, sustentada legalmente pela DMCA, frustrou as expectativas dos consumidores.

A lei de uso aceitável foi criada não somente como uma "válvula de segurança"da livre expressão, mas também como um mediador entre as tensões do *Copyright* e as novas tecnologias. Funcionava como uma lei análoga a da livre competição, existiam usos aceitáveis, como uma análise que um autor poderia fazer da obra de outro autor, e usos inaceitáveis, como plágio. Mas existia também um outro tipo de uso, o "uso comum", sem objetivo competitivo, que é aquele que se faz ao obter um produto como um CD ou livro, o consumidor obtém uma cópia e tem o direito de fazer o uso, sem objetivos financeiros, dessa obra.

No entanto esses conceitos não são fáceis de serem implementados em um sistema digital, uma vez que são limites tênues e até mesmo flexíveis. Criar um sistema que consiga promover o direito ao uso aceitável assim como assegurar os direitos autorais aos seus donos de maneira que um não prejudique o outro é um desafio que ainda não consegue ser respondido pelas tecnologias existentes. [19]

3.1.3 Legalizando a Privacidade Intelectual

Articular os princípios legais necessários para proteger a privacidade afetada pela DRM é um exercício extremamente complicado. Desenvolver tal controle legal requer um elevado grau de esforço, uma vez que nenhum ramo legal consegue abordar todos os elementos necessários para a efetiva proteção da privacidade intelectual, uma vez que precisaria sintetizar elementos extremamente complexos de se definir. Seria necessário não só criar conceitos tangíveis para a privacidade intelectual como também para a quebra da mesma.

Um dos ramos legais que tem certo potencial para conseguir trabalhar os problemas causados pela DRM são os da Lei de Delitos da Privacidade. Com sua ênfase no controle sobre os espaços pessoais, fatos particulares e comercialização de imagem, ela tem capacidade de ser remodelada para uma abordagem voltada a era digital. Além disso, pelo fato da informação também ser uma mercadoria do consumidor, uma abordagem mais explícita sobre a DRM, baseada nos princípios da Lei de Proteção ao Consumidor pode aumentar significativamente o nível de segurança da privacidade intelectual.

1. Lei de Delitos da Privacidade

A lei de delitos da privacidade se baseia inicialmente num antigo e relativamente flexível conceito desenvolvido por Warren e Brandeis como: "o direito de ser deixado em paz"[20]. O problema acaba recaindo exatamente sobre esse aspecto geral e vago, sem um maior aprofundamento desse conceito, praticamente qualquer tipo de incômodo pessoal poderia ser considerado uma infração. Em meados do século XX essa lei foi repartida em 4 diferentes delitos, 3 deles potencialmente aplicáveis ao escopo da DRM, são, invasão da vida privada, apropriação de nome ou imagem e divulgação pública de fatos particulares. Apesar de ainda não serem aplicadas num cenário digital, tais abordagem podem ser flexibilizadas para atender os impactos da DRM.

Aplicações atuais da lei de delitos da privacidade não englobam os efeitos causados pela DRM. A invasão da vida privada comentada anteriormente, por exemplo, tem sido usada para abordar somente invasões físicas ou audiovisuais. Mas poderia ser considerada nos casos das inserções feitas pelos dispositivos DRM, como a utilização de sensores que reportam as atividades do consumidor para outras máquinas ao invés de pessoas, ou tecnologias que restrinjam fortemente sem necessariamente informar sobre sua utilização para outros.

Não diferentemente, o delito de apropriação de nome ou imagem também não é utilizada no contexto da DRM, sendo usado principalmente na área de propaganda. O delito que aborda a divulgação pública de fatos particulares tem sido geralmente utilizada em casos de constrangimento envolvendo material sexual ou informações financeiras, mas não contemplando a venda de dados relacionados ao consumo ou preferência intelectual.

Apoio conceitual para a aplicação mais abrangente desses delitos pode ser encontrada em 2 ramos da lei mais associados com a privacidade intelectual: privacidade constitucional e a lei do *Copyright*. Comparada a lei comum de privacidade a lei da

constitucionalidade aborda com muito mais importância assuntos tangentes a privacidade intelectual. Enquanto isso, a lei do *Copyright* já trabalha outro lado, tentando criar um espaço de anonimato para que as pessoas possam consumir conteúdo intelectual livremente.

2. Lei de proteção ao consumidor

Apesar da lei de proteção ao consumidor não ser vista como um item de muita importância no âmbito legal, viver em uma era de distribuição em massa de informação está começando alterar a percepção da justiça sobre essas leis. As conexões entre a proteção do consumidor e as políticas de informação não podem mais ser ignoradas. A reformulação dos delitos referentes a privacidade da informação pode controlar os piores excessos da DRM e as leis de proteção ao consumidor poderão então definir padrões mínimos de segurança da informação os quais a tecnologia deverá seguir.

Se tal reformulação irá se converter em uma significativa mudança para a proteção dos direitos do consumidor é algo que deverá ser analisado, mas tais mudanças começam a se tornar cada vez mais necessárias, uma vez que a tecnologia evolui e se torna cada vez mais intrusiva. O poder de decisão do consumidor é cada vez mais restringido e junto com essa limitação a vigilância também se torna cada vez mais poderosa.

Essa evolução na tecnologia tem tipo impacto direto na forma como o *Copyright* é percebido, pois agora chega a induzir a maneira como ela funciona. Muitos dos recursos da regulamentação atual foram ditados pelo poder tecnológico. As leis como a DCMA são um grande exemplo disso, pois ela depende fortemente do nível de segurança que a tecnologia é ou não capaz de oferecer.

3.2 DRM x Privacidade

Analisando mais profundamente as relações entre a imposição do *Copyright* e a privacidade, pode-se perceber questões ainda mais profundas, como a natureza da privacidade e o que conta, ou deveria contar, como invasão de privacidade na era digital.

Pois é na tentativa de controlar o crescimento da distribuição de cópias não autorizadas, e de maximizar os lucros sobre produtos disponibilizados digitalmente, que é criada a DRM. No entanto, a mesma capacidade que permite o controle do conteúdo também implica na conversão das informações e interesses dos usuários em mercadoria,

pois cria-se um vasto potencial de coleta de informações dos hábitos e preferências particulares dos usuários. Portanto, essa tecnologia afeta a experiência de privacidade que os usuários estão acostumados a experimentar ao realizar suas atividades intelectuais.

3.2.1 Privacidade e o Consumo Intelectual

As tecnologias DRM funcionam na intersecção de 2 complexos campos da privacidade. Elas tem como alvo um conjunto de ações que são definidas em [21] como "Consumo Intelectual". Ela também afirma que essas ações compõem uma atividade, a exploração intelectual, a qual é essencialmente particular. E a ligação entre os campos da exploração intelectual e do espaço físico particular é um fator muito importante na análise da privacidade intelectual, visto que tanto o aspecto físico quanto o informacional são relevantes ao que tange a privacidade intelectual de um individuo. Em sua essência, a relevância caracteriza o "espaço livre", tanto metafórico quanto físico, necessário para exercer o consumo intelectual. A DRM ameaça esse "espaço livre"por coletar informações sobre esse consumo ou mesmo por impor restrições a essas atividades.

A privacidade intelectual deriva especialmente dos interesses na autonomia pessoal e são primariamente informacionais. Nas sociedades ocidentais, um dos princípios centrais do pensamento pós-Iluminista é a inviolabilidade dos direitos de cada indivíduo sobre si mesmo. Direitos esses que incluem não somente aqueles sobre sua integridade física como também sobre seus pensamentos e personalidade. [22]

Partindo desse pressuposto, Julie Cohen afirma em DRM and Privacy [21] que:

> "Vigilância e divulgações forçadas de informação sobre o consumo intelectual ameaçam os direitos sobre a integridade pessoal e personalidade de maneiras sutis porém poderosas. Apesar do indivíduo não ser impedido de pensar como quiser, essa leve, porém persistente, observação começa a redefinir comportamento, expressão e até mesmo a própria identidade do indivíduo."

E é a partir disso que é possível perceber a importância do direito a privacidade no consumo intelectual, de forma a garantir o espaço livre, metafórico, para exploração e construção do pensamento, além do próprio crescimento pessoal.

3.2.2 Privacidade Intelectual

A DRM é desenvolvida para afetar especialmente o campo da privacidade intelectual. Por restringir diretamente comportamentos relacionados ao consumo intelectual e por permitir a criação de registros detalhados e permanentes desse consumo. Isso da um potencial de mudar drasticamente a maneira como as pessoas consumem tais materiais, de forma que se torna importante questionar se essa mudança não se dará de forma a prejudicar a influenciar negativamente na maneira como esses materiais são consumidos. [23]

Saber se a DRM irá mudar o cenário de maneira a prejudicar os campos da privacidade intelectual torna-se uma questão muito importante. Mas para responder a isso é necessário primeiro analisar algumas das principais características da DRM.

1. Restrição

O CSS(*Content Scrambling System*) é um sistema com o objetivo de impedir a cópia de CDs/DVDs e inclusive restringir os dispositivos capazes de reproduzir seu conteúdo, pois tem um sistema capaz de garantir que CDs/DVDs desenvolvidos para equipamentos de uma região específica não possam ser reproduzidos em outros vendidos em diferentes regiões, por ter essas características o CSS atinge ambos os campos da privacidade intelectual.

No entanto, a privacidade intelectual consiste, em parte, na habilidade de exercer um nível razoável de controle sobre as circunstâncias físicas e temporais do consumo intelectual. Como pode-se ver na citação em [24].

> "A relação entre privacidade física e a atividade intelectual é essa: nós geralmente precisamo de espaços(físicos, sociais, etc...) para nos permitir pensar livremente e sem interferência."

Portanto, a privacidade física garante a liberdade necessária para o pensamento livre e outros processos da formação da crença, dando a eles um contexto no qual eles possam funcionar de forma mais eficaz. Um estudioso desse campo foi o Dr. Samuel Johnson, que escreveu em 1750 que a "reclusão"das agitações e demandas do dia-a-dia eram essenciais para as mentes poderem se engrandecer com o conhecimento. Esse argumento é importante para perceber a importância da capacidade de se afastar a um

lugar particular, isolado, com certo controle sobre a fronteira entre si mesmo e a sociedade para poder refletir naquilo que é importante para si mesmo.

2. Monitoramento

Outras tecnologias DRM tem como objetivo reportar informações sobre as atividades de cada usuário. Podem funcionar coletando e monitorando o uso do conteúdo de forma a tentar identificar preferências do usuário sobre conteúdos específicos ou também pode funcionar para tentar determinar informações sobre conteúdo armazenado naquele dispositivo, como identificar a presença de arquivos MP3 não protegidos contra cópia ou outros programas específicos que o usuário possa estar rodando. Criam-se assim não somente registros sobre o consumo intelectual como também sobre a exploração do mesmo, que é ainda mais pessoal e particular.

Muito dessa coleta de registro é feita automaticamente, sem o envolvimento direto de seres humanos, mas isso não diminui o risco aos interesses dos usuários, pois caso essas informações sejam armazenadas de forma a serem identificados e potencialmente acessíveis a outros, elas irão comprometer a privacidade dos usuários.

A privacidade permite que os indivíduos fujam de certos aspectos sociais indesejáveis, promovendo assim tolerância e pluralidade. Onde os contornos legais se tornam imprecisos ou as aplicações de certas regras podem ser contestadas, a privacidade protege os indivíduos para que eles possam realizar certas atividades. Tecnologias DRM altamente restritivas não permitem a realização de algumas dessas atividades, funcionando assim como uma espécie de novo modelo de distribuição de autoritarismo descentralizado, sendo exatamente a privacidade o escudo que protege a liberdade da interferência desses mecanismos.

4 DRM dentro do âmbito do Brasil

Considerando a falta de regulamentação sobre o conteúdo digital no Brasil, esse capítulo segue como uma análise para a regulamentação de dispositivos como o DRM dentro do âmbito legal brasileiro. A ideia é de analisar e discutir sobre uma proposta que possa incorporar melhor o novo modelo de negócio imposto pela internet através do amplo compartilhamento de conteúdo, de forma a garantir a privacidade dos consumidores sem negar os direitos garantidos aos criadores de conteúdo intelectual através da lei de direitos autorais.

4.1 Nova DRM

É preciso inicialmente definir o escopo da DRM, para que não ocorram problemas como o ocasionado pela DMCA nos EUA. Pois o grande conflito gerado pela lei foi por transformar em crime o contorno de uma tecnologia que controlava o uso dos consumidores de forma tão incisiva que chegava a lhes tirar a privacidade que eles usualmente adquiriam ao adquirir aquele material.

No entanto, o grande problema da DRM está em como garantir que o plano ideal possa ser implementado. Por exemplo, garantindo o direito dos consumidores de fazerem cópias de backup dos seus produtos mas ao mesmo tempo tentando impedir que essas cópias sejam revendidas ou utilizadas por outras pessoas que não aquelas que compraram e adquiriram legalmente o direito de reprodução desses materiais.

A DRM ainda não é capaz de fazer tal distinção. O que pode levar a pergunta, será se estamos prontos para implementar tal tecnologia? Como garantir os direitos de uns, detentores de *Copyright*, sem invadir os de outros, consumidores?

Um artigo da *International Digital Publishing Forum* descreve uma nova abordagem da tecnologia para o mercado de ebooks, denominada DRM de restrições leve [25]. Três pontos inter relacionados são descritos como essenciais para a definição de um modelo como leve ou pesado:

1. Implementação: DRMs leves são mais baratas de serem implementadas, o que gera um menor custo por cliente. Alguns fatores que contribuem para isso são:

   a. Uso de memória e processador.

   b. Requerimentos de segurança ou robustez de software. Alguns exemplos são técnicas de ofuscação de chaves que requerem um grande poder de processamento.

   c. Complexidade da interação cliente-servidor.

2. Experiência do usuário: DRMs leves são mais fáceis de usar e causam menos confusão ao consumidor. Elementos que colaboram para um bom uso são:

   a. Não atrapalham a interação do usuário com o conteúdo.

   b. Funcionam perfeitamente mesmo na ausência de uma conexão à internet. Não sendo afetado inclusive caso a tecnologia seja abandonada.

3. Intrusão: DRMs leves devem ser minimamente intrusiva aos usuários. As principais categorias consideradas são:

   a. Impor restrições de modo a impedir atividades do consumidor que sejam permitidas por lei.

   b. Invadir a privacidade através de relatórios sobre o uso dos consumidores sem realizar qualquer tipo de notificação sobre essa ação ou sem permitir a opção de se negar a fornecer tais dados.

   c. Por em risco a segurança dos dispositivos nos quais os usuários acessam o conteúdo.

Os pontos indicados pela *IDPF* são extremamente importantes para o desenvolvimento de modelos que possam garantir os direitos dos consumidores e até mesmo popularizar o uso da DRM. Especialmente o que considera a experiência do usuário, uma vez que a aceitação dos consumidores é essencial para o sucesso do modelo. A própria história mostra que os modelos excessivamente intrusivos foram rapidamente rechaçados e consequentemente abandonados.

Isso é percebido em alguns casos do uso da tecnologia SecuRom, como por exemplo no jogo Spore, em 2008. O qual levou a EA Games a ser processada por não informar sobre o uso dessa DRM e também pela tecnologia ser considerada maliciosa, uma vez que não podia ser desinstalada mesmo que o jogo fosse desinstalado, sendo removível

somente através da formatação dos PCs. Depois de amenizar as restrições impostas pela DRM, a EA Games se viu forçada a distribuir o jogo sem DRM, pois graças ao resultado negativo, Spore se tornou o jogo mais pirateado do ano de 2008.

Outro famoso caso é o da Sony em 2005 envolvendo a DRM MediaMax. Era também extremamente restritivo, permitindo que cada CD fosse copiado somente 3 vezes antes de ser travado, além disso os CDs só podiam ser reproduzidos através do player proprietário da Sony, forçando os consumidores a baixar o software. Essas informações não eram declaradas no momento da compra dos CDs, o consumidor só descobria as restrições ao tentar reproduzir seu conteúdo. Mais grave ainda era o fato dessa DRM se instalar sem solicitar permissão ao usuário e se inserir no kernel do sistema operacional de forma a ficar oculto.

Mais tarde foi descoberto que a tecnologia possuía uma séria falha de segurança, que permitia que hackers invadissem e tomassem controle completo das máquinas. A reação dos consumidores foi pesada, a Sony foi alvo de inúmeros processos de usuários insatisfeitos. Até a Comissão Federal de Comércio dos EUA entrou com uma ação contra a Sony pelos problemas gerados pelo MediaMax. [26]

É fácil perceber que essas tecnologias não se encaixam no modelo de DRM leve indicado pela *IDPF*. Comprometendo extremamente a experiência do usuário através da excessiva intrusão. Fica visível assim a necessidade de preocupação com a qualidade da interação que a tecnologia oferece aos consumidores, pois do contrário existe uma grande possibilidade da tecnologia ser mal recebida e ocasionar o efeito exatamente oposto ao que foi proposta, aumentando a pirataria.

4.2 Arquitetura

Uma proposta de arquitetura segura e com baixo nível de intrusão é apresentado em [27] como criptografia homomórfica, que basicamente se trata de realizar operações corretamente em dados criptografados sem necessariamente ficar ciente de seu conteúdo. Essa flexibilidade resolve os problemas de segurança garantindo o anonimato das informações trabalhadas, o que permite aos provedores de conteúdo terceirizar o gerenciamento da DRM sem precisar expor os dados criptografados.

O modelo dessa arquitetura consiste de 4 fases. Conteúdo conforme fig 4.1.

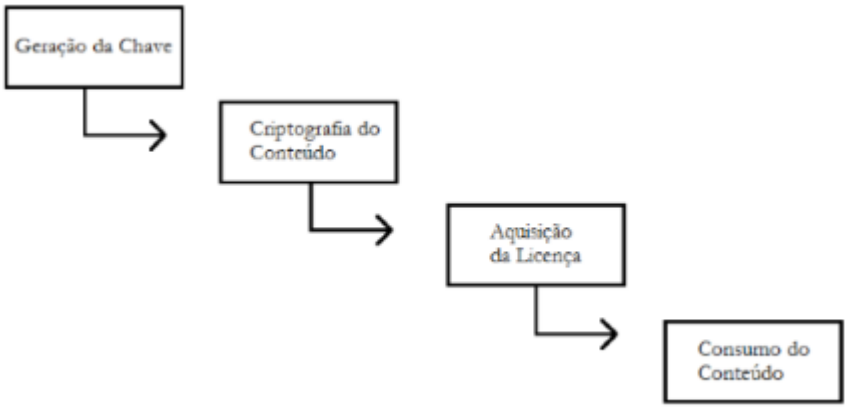

Figura 4.1: Modelo de Arquitetura de Baixa Intrusão

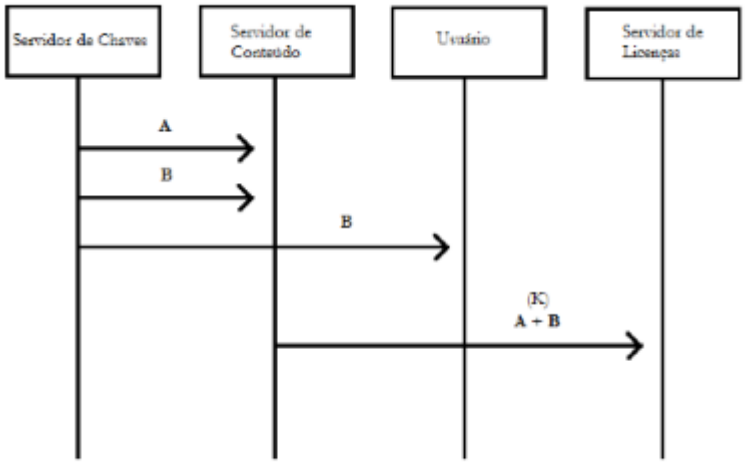

Figura 4.2: Geração de chaves [27]

1. Geração da Chave: O servidor de chaves gera o par de chaves pública e privada para o provedor de conteúdo e para o usuário. Conteúdo, conforme fig 4.2.

   Essa fase é composta por 3 etapas.

   Etapa 1: O servidor de chaves cria uma chave para o provedor de conteúdo e a envia para ele.

   Etapa 2: O servidor de chaves cria uma chave para o usuário anônimo e a envia para ele. O servidor não pode ser capaz de coletar informações pessoais do usuário.

   Etapa 3: O provedor de conteúdo gera uma chave adicional com base nas 2 chaves criadas anteriormente e a envia para o servidor de licenças.

2. Criptografia do Conteúdo: O provedor de conteúdo recriptografa a informação

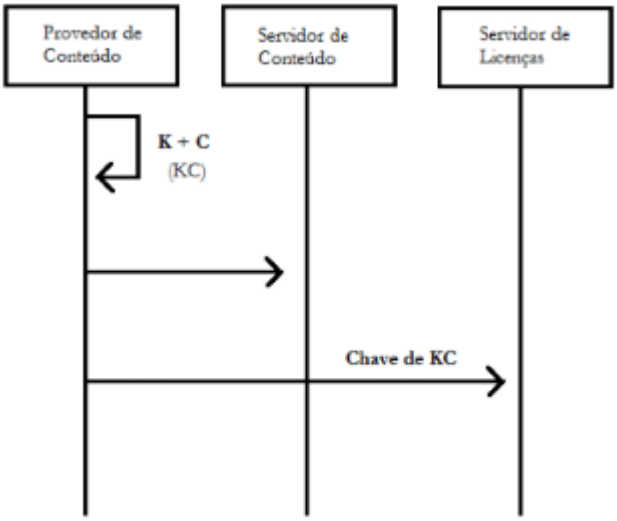

Figura 4.3: Criptografia do Conteúdo [27]

adicionando outra chave e então envia esse conteúdo para o servidor de conteúdo. Conteúdo, conforme fig 4.3.

Etapa 1: O provedor de conteúdo envia os dados protegidos ao servidor de conteúdo.

Etapa 2: O provedor de conteúdo envia a chave associada ao servidor de licenças.

3. Aquisição de Licença: O servidor de conteúdo requisita a licença ao servidor de licenças com base nas informações do usuário, que depois de gerada é enviada através do próprio servidor de conteúdo. Conteúdo, conforme fig 4.4.

   Etapa 1: O usuário requisita anonimamente a informação do provedor de conteúdo.

   Etapa 2: O provedor de serviço solicita uma licença ao servidor de licenças de acordo com as informações coletadas do usuário.

   Etapa 3: O servidor de licenças checa os dados do usuário e então solicita a chave ao servidor de chaves.

   Etapa 4: Após aquisição da chave, o servidor de licenças gera a licença que contém a identificação do conteúdo, a chave necessária para descriptografá-lo e os direitos de uso sobre esses dados.

   Etapa 5: O servidor de licenças envia o pacote de informações através do provedor de serviço.

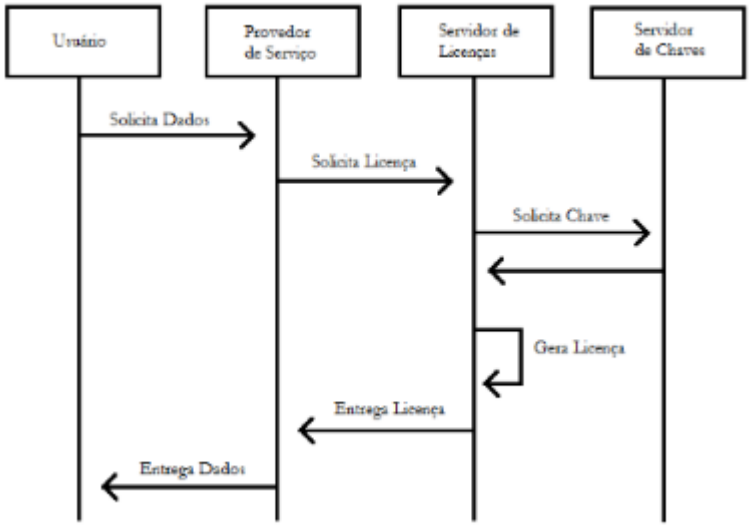

Figura 4.4: Aquisição de Licença [27]

4. Consumo do Conteúdo: O consumidor checa a licença e descriptografa o conteúdo com a mesma. Podendo então consumir o a informação protegida de acordo com as regras estabelecidas na licença. Aqui o DRM instalado no dispositivo do consumidor é o responsável por manipular a chave embutida na licença para a descriptografia do conteúdo.

   O usuário se comunica diretamente com o servidor de chaves e o provedor de conteúdo, outras entidades não entram em contato com ele. Na fase de criação das chaves, o usuário se registra anonimamente no servidor de chaves, de modo a garantir sua privacidade. Durante a aquisição da licença o mesmo procedimento é realizado, adquirindo assim o conteúdo e licença associada sem revelar suas informações pessoais.

4.3 Legalização no Brasil

O embasamento legal também é uma necessidade real, o cenário brasileiro não possui leis que abordem a DRM, mas para que a tecnologia possa funcionar de forma eficiente a proteção legal é essencial. A DMCA desenvolvida nos EUA é um suporte essencial, um similar teria que ser criado para proteger legalmente a DRM de possíveis ataques.

Em geral, se tratando tanto da lei de direitos autorais como das leis voltadas

ao ambiente digital o Brasil tem regulamentações bastante atrasadas, estando inclusive a lei de direitos autorais brasileira entre as 5 piores do mundo [28], sendo considerada extremamente restritiva. A lei não permite nem mesmo que sejam feitas cópias para uso privado, levando ao pé da letra, ela não permite sequer que uma música seja copiada de seu computador para seu smartphone.

Uma atualização da lei de direitos autorais foi decretada no dia 14 de agosto de 2013, mas em tal atualização não foi contemplada a necessidade de legalização digital. Sendo a maior parte das modificações referentes a arrecadação dos pagamentos sobre direitos autorais e na forma como o ECAD (Escritório Central de Arrecadação e Distribuição), que é uma instituição privada e sem fins lucrativos com o objetivo de centralizar a arrecadação e distribuição dos direitos autorais de execução pública musical.

No entanto o Brasil realizou recentemente um grande passo para a legalização do ambiente digital, instaurando o Marco Civil da internet, tornando-se inclusive referência mundial no assunto. O marco abrangeu pontos vitais ao ambiente digital, como:

1. Neutralidade da Rede:

   O princípio da neutralidade estabelece que a rede deve ser igual para todos, de modo que os responsáveis pela infraestrutura da rede e seus serviços não possam discriminar os conteúdos que nela circulam ou aplicar filtros que discriminem parâmetros como a identificação do usuário, conteúdo dos dados ou origem e destino da comunicação. Em outras palavras, todo o conteúdo trafegado pela rede deve ser tratado com isonomia pela rede, mantendo o usuário livre de interferência.

2. Guarda de Registros:

   O Marco também obriga os provedores de acesso a guardarem os registros de conexão dos seus usuários por um período de 1 ano, sob total sigilo e segurança. Essas informações dizem respeito somente a identificação da máquina (IP) a qual o acesso está sendo feito e data e hora do inicio e fim da conexão.

   A lei também obriga que o armazenamento de tais informações deve ser feito de forma completamente anônima, ou seja, os provedores devem armazenar o IP mas nunca informações específicas do usuário. E tal informação só poderá ser disponibilizada mediante ordem judicial.

Além disso, é fixado que os dados fornecidos pelos usuários aos provedores não podem ser utilizados para quaisquer fins diferentes daqueles que foram fornecidas. Impondo assim um maior controle sobre a venda de informações dos usuários.

3. Retirada de Conteúdo e Responsabilidades:

   Outro importante ponto é o que estabelece que um conteúdo só pode ser retirado do ar por meio de uma ordem judicial, e que o provedor não pode ser responsabilizado por conteúdo ofensivo publicado pelos usuários de seu serviço. O texto, porém, prevê algumas exceções. Um conteúdo pode ser retirado do ar sem ordem judicial caso infrinja alguma matéria penal, como racismo, pedofilia ou violência.

   O objetivo desse ponto é o de evitar a censura na internet, pois para se provar que um conteúdo é realmente ofensivo o caso deverá agora passar pela Justiça. E ao mesmo tempo criando exceções para garantir que os trâmites legais não prejudiquem casos notoriamente danosos, como os citados anteriormente.

5 Conclusão

Percebe-se a complexidade em analisar o escopo de uma tecnologia tão abrangente e que está extremamente inserida em direitos tão intrísecos a sociedade, como a privacidade e o direito ao uso. A DRM se depara com o desafio de definir exatamente uma fronteira que é difícil de indicar mesmo a nível conceitual. A questão principal é, como garantir que todas as entidades envolvidas nessa relação saiam satisfeitas, garantir que os autores de conteúdo, os detentores dos *Copyright*, os distribuidores de conteúdo e os usuários, tenham seus direitos garantidos sem ignorar ou invadir os dos outros.

O problema é que nessa relação, os distribuidores e detentores de *Copyright* tem uma posição privilegiada, pois a tecnologia foi desenvolvida a partir de uma necessidade deles mesmos, ao ver que seu material era pirateado e seu lucro não era devidamente recolhido. A DRM surge para garantir que todo material distribuído seja adquirido legalmente e que o lucro não seja perdido pela distribuição ilegal do material.

Mas a tecnologia acaba sendo, na maioria das vezes, muito rígida, e os consumidores começam a sentir seus direitos sendo invadidos, criando assim a maioria dos duelos legais entre a sociedade e as empresas distribuidoras de conteúdo protegido pela DRM. As empresas passam a não só restringir os direitos dos usuários como a invadir sua privacidade, pois usam a nova tecnologia como um meio para coletar informações sobre os hábitos e costumes dos usuários.

Boa parte dos modelos DRM desenvolvidos acabam sendo abandonados por pressão dos consumidores pelo alto nível de intrusão do modelo, ou até mesmo por não conseguirem proteger devidamente o conteúdo. Acaba se percebendo a dificuldade em desenvolver sólidos modelos, além de se perceber a necessidade em garantir que os usuários estejam satisfeitos com esses modelos. As tecnologias começam a se tornar mais flexíveis e passam a ser melhor recebidas, como no caso da plataforma de games Steam, no qual a DRM é oferecida em uma troca que é feita com o consumidor, lhe fornecendo um ambiente seguro, de fácil uso e acesso e se tornando assim a maior plataforma de jogos online do mundo.

Percebe-se que a melhor maneira de trabalhar a tecnologia é aceitar que precisa

ser feita uma troca com o consumidor, pois a DRM lida com um direito muito particular do mesmo. O poder de alterar a maneira como consumimos material digital precisa ser aplicado de forma moderada e ao mesmo tempo garantindo que irá se dar de uma maneira que o consumidor tenha algum benefício em abrir mão de algumas liberdades que ele possuía em materiais do mesmo tipo adquirido por outras fontes.

Referências Bibliográficas

[1] Anderson, Ross. *Security Engineering*, 2008, Wiley.

[2] *What is Intellectual Property?*, World Intellectual Property Organization, Publication n450.

[3] *WIPO Intellectual Property Handbook*, 2004, World Intellectual Property Organization, Publication n489.

[4] *Understanding Copyright and Related Rights*, World Intellectual Property Organization, Publication n909.

[5] Humphrey, John Peters & Cassin, René & Change, P. C. & Malik, Charles & Mehta, Hansa & Roosevelt, Eleanor. *Universal Declarations of Human Rights*, 1948, Paris, Palais de Chaillot.

[6] U.S. Copyright Office *Subject Matter and Scope of Copyright.*

[7] Office of The Privacy Comissioner of Canada *The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of PIPEDA*, 2006.

[8] Becker, Eberhard & Buhse, Willms & Günnewig, Dirk & Rump, Niels. *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, 2003, Springer.

[9] Arsenova, Emilija. *Technical aspects of Digital Rights Management*, 2006, MI, RWTH-Aachen.

[10] Ku, William & Chi, Chi-Hung. *Survey on the Technological Aspects of Digital Rights Management*, 2004, School of Computing, National University of Singapore.

[11] Heileman, Gregory L. & Yang, Yunlong. *The effects of invisible watermarking on satellite image classification*, 2003, University of New Mexico, Albuquergue.

[12] Stamford, Conn. *Gartner Says Worldwide Video Game Market to Total $93 Billion in 2013*, 2013, http://www.gartner.com/newsroom/id/2614915.

[13] Zhang, Xiao. *A Survey of Digital Rights Management Technologies*, 2011, http://www.cse.wustl.edu/ jain/cse571-11/ftp/drm/index.html.

[14] Anderson, Ben F. & Renzulli, Eric J. *MODERN DIGITAL RIGHTS MANAGEMENT METHODS*, 2009, Worcester Polytechnic Institute.

[15] Kumar, Nithin V. *Digital Rights Management and Intellectual Property Protection*, 2012, Nalsar University of Law, Hyderabad.

[16] U.S. Copyright Office. *The Digital Millennium Copyright Act of 1998*, 1998, U.S. Copyright Office Summary.

[17] European Parliament & Council. *Directive 2001/29/EC*, 2001, European Parliament.

[18] Iowa State University Research Foundation. *Copyrights*, http://www.techtransfer.iastate.edu/en/for_iowa_state/educational_resources/copyrights.cfm#Fair_Use.

[19] Hazarika, Shruti Sarma. *Digital Rights Management: A Restrictive Rather than a Defensive Mechanism and the Survival of the 'Fair Use' Doctrine*, 2012, Guru Gobind Singh Indraprastha University, Amity Law School.

[20] Warren, Samuel D. & Brandeis, Louis D. *The Right to Privacy*, 1890, Harvard Law Review.

[21] Cohen, Julie E. *DRM and Privacy*, 2003, Gerorgetown University Law Center.

[22] Hegel, Georg Wilhelm Friedrich *Elements of The Philosophy of Right*, (T.M. Knox trans., 1942).

[23] Ahmad, Tabrez & Chanda, Rudi. *FAIR USE AND DIGITAL RIGHTS MANAGEMENT IN THE LIGHT OF U.S. LAWS*, 2011, KIIT University, KIIT Law School.

[24] Richards, Neil M. *Intellectual Privacy*, 2008, Washington University in St.Louis School of Law.

[25] Bill, Rosenblatt. *EPUB Lightweight Content Protection: Use Cases & Requirements*, 2012, International Digital Publishing Forum.

[26] Mulligan, Deirdre K. & Perzanowski, Aaron. *The Magnificente of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 2010, Berkley Technology Law Journal.

[27] Huand, Qin-long & Ma, Zhao-feng & Yang, Yi-xian & Fu, Jing-Yi & Niu, Xin-xin. *Secure and privacy-preserving DRM scheme using homomorphic encryption in cloud computing*, 2013, The Journal of China Universities of Posts and Telecommunications.

[28] Consumers International. *IP WatchList 2012*, 2012, Consumers International. http://a2knetwork.org/sites/default/files/IPWatchlist-2012-ENG.pdf

[29] Abie, Habtamu. *Fronties of DRM Knowledge and Technology*, 2007, Norwegian Computing Center.

[30] Dolata, Ulrich. *The Music Industry and the Internet*. A Decade of Disruptive and Uncontrolled Sectoral Change, 2011, University Stuttgart, Institute of Social Sciences.

[31] Parchomovsky, Gideon & Weiser, Philip J. *Beyond Fair use*, 2009, University of Pennsylvania Law School.

[32] Dusollier, Séverine. *DRM at the intersection of copyright law and technology: a case study of regulation*, 2012, Belgium University of Namur.

[33] Ahmad, Tabrez. *Intellectual Property Law in Internet*, 2009, University of Petroleum and Energy Studies.