Digital Rights Management para TV Digital Fechada

Rodrigo Fontes Souto Marcelo A F Gomes Paulo Gondim
Instituto Nokia de Tecnologia

RESUMO

A legislação brasileira já proibiu esquemas de proteção de conteúdo dos canais abertos nos conversores de televisão digital. Entretanto, considerando-se um cenário de convergência de tecnologias, a proteção de conteúdo ainda é permitida para outros modelos de negócio, e.g., serviços de internet e telefonia e canais fechados de televisão. Mas as soluções encontradas no mercado são proprietárias, ou seja, deve-se pagar os devidos royalties para seus fabricantes. Desta forma, os sistemas de proteção de propriedade intelectual também geram custos aos criadores de conteúdo. No entanto, estes custos podem ser repassados conforme uma cadeia de valor. Neste trabalho, apresentamos as implicações na cadeia de valores da TV Digital em um cenário com proteção de direitos autorais, mostrando seus atores e papéis. Também são abordados alguns dos aspectos técnicos e legais, e apresentadas as principais entidades responsáveis pela definição técnica, legislação e tratamento da obrigatoriedade de uso de tecnologias de DRM (Digital Rights Management). Finalmente, são apresentadas ainda as possibilidades futuras do DRM e como pode ou deve ser tratado o assunto, na visão de diferentes entidades envolvidas.

Palavras-Chave: DRM, Proteção de Propriedade Intelectual, TV Digital.

1. INTRODUÇÃO

Desde que a humanidade começou a ter o poder de reproduzir produções culturais e de explorá-las comercialmente, existe a preocupação, tanto por parte de seus autores quanto de seus distribuidores e demais partes interessadas, em proteger tais produções contra cópias e, mais recentemente, contra usos indevidos.

O avanço tecnológico vivido nas últimas décadas tornou esta preocupação ainda maior, enquanto fez com que a discussão sobre o que deve ou não ser considerado indevido se tornasse mais acalorada. Tal avanço torna cada vez mais difícil obtermos consenso sobre aspectos básicos, tais como as definições de cópia e de uso válido.

Neste contexto, surgiu a tecnologia DRM. Descrita por GROSSMAN (2007) [1] na revista Time como "uma camada invisível de *software* que atua como um guarda-costas de um arquivo de computador e limita o que você pode ou não pode fazer com ele", esta tecnologia é definida de forma mais precisa na seção 2.

Apesar de a sigla DRM ter sido cunhada para significar *Digital Rights Management* (gerência de direitos digitais), alguns de seus críticos (por exemplo, The Free Software Foundation [2]) a utilizam como *Digital Restrictions Management* (gerência de restrições digitais), numa alusão ao fato de que as implementações existentes de DRM restringem as formas possíveis de uso de conteúdo digital, sem acrescentar qualquer vantagem a seu usuário final.

Apesar de não oferecer vantagens diretas a seus usuários, os criadores e distribuidores de conteúdo têm grande interesse nesta tecnologia. Prova disso é o número de patentes relacionadas ao assunto. Uma busca recente no *site* do Instituto Nacional da Propriedade Industrial (INPI) [3] mostrou 14 processos de patentes lá registrados contendo a sigla DRM em seu resumo. No *site* do escritório de patentes dos Estados Unidos (USPTO) [4], encontramos 202 patentes contendo a sigla DRM e a expressão "*rights management*".

O estudo de DRM tem despertado também grande interesse no meio acadêmico, por meio da publicação de diversos artigos para diferentes aplicações, tais como NISHIMOTO (2006) [5], onde é proposto um sistema DRM para *broadcast* digital, tanto em tempo real quanto para conteúdo armazenado, baseado em servidores domésticos; HARTUNG (2000) [6], em que é discutida a relação entre DRM e *m-commerce*, bem como seu impacto no modelo de negócios; TRIMECHE (2004) [7], que sugere a adição de marcas d'água para melhorar a segurança de propriedade intelectual em aplicações DRM voltadas a conteúdo visual para terminais móveis; ZHANG (2004) [8], onde é proposta uma arquitetura DRM baseada em autenticação biométrica, i.e., o sistemas utiliza características físicas do usuário a fim de autenticá-lo, e.g., impressão digital, face e íris; LAN (2006) [9], em que se apresenta uma solução DRM utilizando RFID para proteção de áudio; e GEER (2004) [10], que trata de tópicos sobre a interoperabilidade de diferentes sistemas DRM proprietários e é sugerido o desenvolvimento de um *software* de gerenciamento de sistemas DRM capaz de converter os vários sistemas DRM, ao mesmo tempo em que se reconhece a complexidade envolvida na produção de tal *software*, dado o aumento constante de sistemas DRM e de formatos de arquivos.

No presente trabalho, apresentamos uma breve introdução ao conceito de DRM na seção 2. Na seção 3, são apresentadas algumas técnicas de proteção utilizadas por sistemas DRM para proteção do conteúdo. Na seção 4 são apresentadas possíveis arquiteturas para TV digital com DRM e suas respectivas cadeias de valores. Na seção 5 são apresentados os principais organismos de normatização e defesa de interesse de diversas classes diretamente interessadas na TV digital. Por fim, apresentamos as conclusões pertinentes na seção 6.

2. DIGITAL RIGTHS MANAGEMENT (DRM)

Definir DRM não é uma tarefa fácil. Um comitê formado por membros interessados da comunidade, indústria e governos da União Européia tentou, mas não obteve consenso, mesmo na versão final de seu relatório sobre DRM, publicada em CEN (2003) [11], que continha diversas definições distintas, elaboradas por diferentes entidades proponentes.

Como não há uma definição formal amplamente aceita, a definição de DRM utilizada neste trabalho será: um conjunto políticas para regular o acesso e a fruição de produtos de propriedade intelectual, medidas tecnológicas para impor sua observação, bem como leis e medidas processuais para evitar que tais medidas e leis sejam burladas; concebido para proteger contra cópias e/ou formas de uso não autorizadas os produtos aos quais se destina sua aplicação.

De maneira geral, os sistemas DRM são projetados para permitir a troca segura de conteúdo protegido por direitos de propriedade intelectual, e.g., música, texto, imagens e vídeos por meio de CD, DVD, Internet e comunicações sem fio, como aparelhos celulares e de televisão. Sistemas DRM permitem ao dono do conteúdo distribuí-lo seguramente para consumidores, bem como controlar toda sua cadeia de distribuição. Um sistema DRM é composto pelos seguintes subsistemas:

Controle de Acesso: responsável pela decisão de permitir ou negar o acesso a um dado conteúdo para um dado usuário numa dada situação. Aqui, o termo *usuário* tanto pode se referir a um ser humano quanto a qualquer entidade, dispositivo ou canal de comunicação integrante da cadeia de valores pré-definida. Este subsistema deve ser flexível em relação às regras de uso. As regras de uso devem adaptar-se de acordo com o modelo de negócios. O controle de acesso pode restringir, por exemplo, usuários específicos, o tempo de uso e/ou o número de acessos. Um modelo de amostra grátis também seria possível, isto é, o primeiro acesso ao conteúdo seria gratuito e os demais seriam pagos. Outros modelos ainda podem vincular propagandas ao conteúdo.

Encriptação/Decriptação: subsistema opcional para prevenir o acesso não-autorizado ao conteúdo ou parte dele. Num sistema DRM ideal, apenas usuários autorizados pelo subsistema de controle de acesso poderão decriptar e assim conseguir acesso ao conteúdo.

Interface com sistemas de cobrança: como a maioria das transações de mídia envolve transações financeiras, os sistemas DRM devem ser capazes de lidar com estas questões.

Identificação e rastreamento do conteúdo: uma vez que surjam cópias não autorizadas, seria interessante saber sua fonte, e assim impedir a continuidade do processo de criação de novas cópias não autorizadas. Esta é a função deste subsistema. Além disso, Por melhor que seja, qualquer sistema DRM baseado puramente em tecnologia tem ao menos um "furo", conhecido como o *furo analógico*, ou "*analog hole*", descrito em EFF [12]: usuários autorizados normalmente possuem, pelo menos, acesso à versão analógica do conteúdo, como a imagem mostrada no monitor e o som proveniente das caixas acústicas, uma vez que nossos sentidos são analógicos. Desta forma, é possível a produção de cópias digitais a partir das saídas analógicas e estas dificilmente podem ser evitadas. Portanto, seria interessante também poder identificar e rastrear tais cópias, além de cópias digitais diretas. Uma possível proteção contra o *furo analógico* será mostrada mais adiante.

Controle/Prevenção de cópias: depende das regras de negócio. Pode-se permitir um número ilimitado de cópias, poucas cópias, uma cópia ou até mesmo nenhuma cópia do conteúdo. Também se pode definir quais regras serão aplicadas às cópias das cópias, seguindo o mesmo princípio. O controle de cópias é mais difícil de ser alcançado e necessita de tecnologia sofisticada, tal como o acréscimo de marcas d'água. Além de tecnologia, pode ser necessária a utilização de dispositivos legais, como veremos no caso do *furo analógico*, mais adiante.

A figura 1 ilustra as partes que podem compor um sistema DRM.

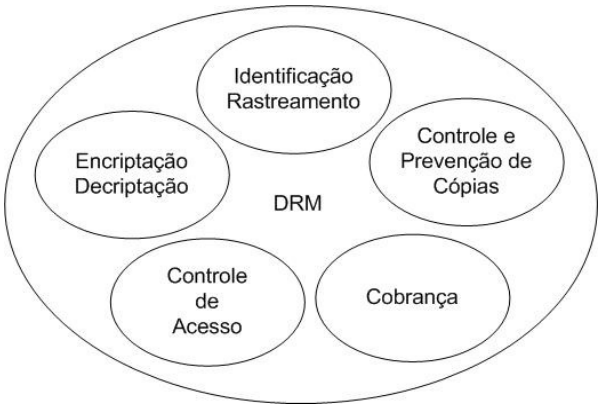

Figura 1 – Subsistemas de sistemas DRM.

As figuras 2 e 3 foram adaptadas de GIOVANI (2006). A figura 2 ilustra as formas possíveis de gerenciar a distribuição de conteúdo. No primeiro caso, junto ao conteúdo é adicionada uma mensagem DRM somente proibindo a distribuição do conteúdo. Na entrega combinada, segundo caso, junto ao conteúdo são adicionados os direitos de uso daquele conteúdo, bem como suas regras de distribuição. Na entrega separada, terceiro caso, os direitos de uso são entregues separados do conteúdo, e.g., um *hardware* dedicado pode possuir as regras de utilização em seu *firmware*.

A figura 3 ilustra um modelo de proteção baseado no controle de acesso ao conteúdo. As informações dos clientes autorizados a acessar os conteúdos ficam em um banco de dados, que é parte de um CAS (*Conditional Access System*). O receptor deve então se autenticar no sistema e estar autorizado a utilizar o conteúdo.

Figura 2 – Gerenciamento da distribuição de conteúdo.

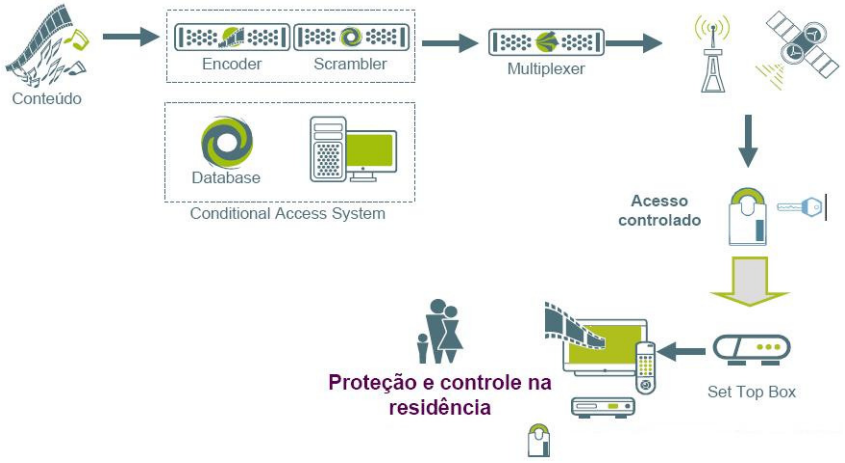

Figura 3 – Modelo de proteção por meio do controle de acesso.

3. TÉCNICAS DE PROTEÇÃO

Tipicamente, duas abordagens são as mais utilizadas para o controle de conteúdo digital. A primeira delas é a encriptação. A encriptação utiliza modelos matemáticos para misturar os dados de forma que sejam ilegíveis para alguém que não possua a chave correta para decriptá-los. Este processo é bastante utilizado em DVD's e na Internet. Entretanto, o processo de encriptar/decriptar é complexo e exige maior capacidade de processamento, encarecendo, e por vezes chegando a inviabilizar, sua aplicação em tempo real para sistemas por difusão (*broadcast*), como o da TV digital.

A segunda abordagem também é conhecida como "marcação". Trata-se de se

adicionar uma "marca" ao conteúdo digital. Tal marca pode ser utilizada simplesmente para indicar um direito autoral, mas também pode conter as regras de utilização daquele conteúdo, e.g., permitir um número ilimitado de cópias ou restringi-las. De acordo com GODWIN [13], há, principalmente, três formas de se adicionar uma marca ao conteúdo:

Adicionando um cabeçalho ao conteúdo.

Acrescentando uma marca d'água, de forma que bits de controle são escondidos no conteúdo

Adicionando uma "impressão digital", i.e., um identificar único obtido a partir do conteúdo.

Há três fatores que favorecem a utilização de marcas d'água. O primeiro é quando a encriptação não é viável. Outra vantagem é detectar cópias digitais. Desta forma, por exemplo, a marcação poderia ser utilizada por um sistema de busca pela Internet para identificá-la e classificá-la como uma cópia autorizada. Marcações mais complexas podem, inclusive, identificar a partir de qual original a cópia fora feita. Por fim, a marcação também pode ser empregada para combater os *Furos Analógicos*.

Há também uma terceira técnica de proteção, ainda mais simples que as duas primeiras, que consiste em se embaralhar as linhas de vídeo e/ou trechos do áudio antes de sua transmissão, desembaralhando-as no receptor. É claro que deve haver um mecanismo para a transmissão da ordem correta de desembaralhamento, juntamente com o restante do sinal.

A sugestão dada em BASTOS (2004) [14] é aproveitar o tempo de apagamento vertical do sinal de vídeo e inserir a informação necessária codificada ali, com um insersor de VITS (*Vertical Interval Test Signal*).

Com esta técnica, o transmissor pode trocar a ordem de embaralhamento de forma aleatória, e em intervalos de tempo igualmente aleatórios, tornando a recuperação do sinal original praticamente impossível para quem não conhece o formato da codificação inserida no apagamento vertical.

No entanto, seu ponto fraco é exatamente este. Esta técnica não é muito utilizada pois sua segurança está no sigilo do formato de codificação. Caso este formato torne-se público, será possível a qualquer pessoa com conhecimentos técnicos suficientes decodificar o sinal que deveria ser seguro. Ou até fabricar em série um decodificador *pirata* com o intuito de obter lucro ilícito a partir de sua venda.

3.1. BROADCAST FLAG

O *broadcast flag* consiste em um esquema para prover proteção de direitos autorais em transmissões de TV digital. Uma versão deste esquema fora adotado pela Federal Communications Commission (FCC) em 2003. Seu objetivo é evitar a recepção não autorizada de conteúdo e, caso ocorra esta recepção, sua reprodução e/ou distribuição devem ser limitadas.

O *broadcast flag* funciona da seguinte forma: pacotes em seqüência são transmitidos em *broadcast* para receptores de TV digital, e.g., *set-top boxes*. Cada pacote é composto por um cabeçalho e o conteúdo propriamente dito, i.e., um *frame* do vídeo a ser transmitido. No cabeçalho há informações da posição do pacote na seqüência de vídeo. Entretanto, em tais cabeçalhos também podem constar bits que indicam que o conteúdo possui um dono e/ou as restrições daquele conteúdo. Quando o de-modulador, *set-top box*, receber o conteúdo, deve

verificar a existência dos bits de proteção e, caso existam, o decodificador pode impedir o envio do conteúdo para outros dispositivos, tais como televisões, *DVD players* e computadores.

O *broadcast flag* é, portanto, uma marcação simples, ou seja, trata-se apenas de informações que acompanham o conteúdo. A principal vantagem desta abordagem é que a marca pode ser localizada e interpretada rapidamente, além de poder ser utilizada em diversos tipos de conteúdos. Por outro lado, sua simplicidade permite que seu cabeçalho seja removido e/ou modificado facilmente. A figura 4 ilustra um conteúdo marcado com o broadcast flag.

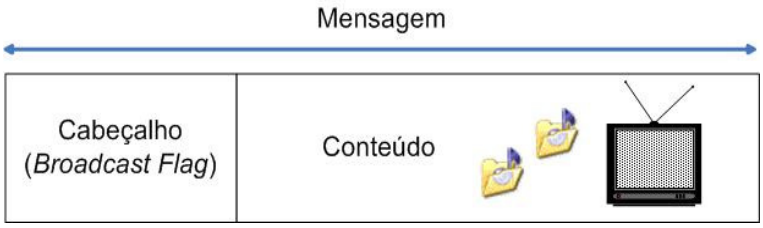

Figura 4 – Conteúdo marcado com broadcast flag.

3.2. PROTEÇÃO CONTRA O FURO ANALÓGICO

Conforme já mencionado, o *furo analógico*, ou *analog hole*, é um dos principais problemas para se implementar o DRM de forma consistente. Como precisamos do conteúdo em seu formato analógico para sua fruição, permite-se a gravação de uma cópia não autorizada a partir desta forma analógica. Hoje, há três métodos sendo estudados para combater o *furo analógico*, sendo que dois deles são de propriedade da Microsoft.

A primeira técnica tratra da utilização de marcas d'água. Parte-se do princípio de que algumas marcas ainda estariam presentes no conteúdo mesmo após sua gravação a partir de seu conteúdo na forma analógica. Desta maneira, após a digitalização do vídeo, as marcas permaneceriam e elas poderiam ser identificadas e classificadas.

Com o acréscimo de mecanismos legais obrigando os fabricantes de dispositivos capazes de executar as gravações a também identificar e honrar tais marcas, poderia-se efetivamente eliminar a possibilidade de exploração do *furo analógico* desta forma.

Outra solução, mostrada em EFF (2005) [15], de propriedade da Microsoft, é conhecida por *Protected Media Path* (PMP), e pode ser empregada tanto em computadores quanto em *set-top boxes*, PDAs, celulares ou dispositivos similares. Sua principal característica é desabilitar determinadas placas de vídeo ou alguns de seus sinais de saída. Assim, evita-se que placas antigas possam ser utilizadas para a gravação de cópias. Fabricantes sem a implementação do PMP não serão certificados. Eventualmente, o PMP poderá prover autenticação com dispositivos de saída por meio de uma comunicação segura. Desta forma, *drivers* de diferentes fabricantes seriam assinados digitalmente e autorizados a reproduzir o conteúdo protegido.

Outra técnica da Microsoft surgiu a partir do padrão *Copy Generation Management System for Analog* (CGMS-A) EFF (2005) [16]. O CGMS-A é um padrão da indústria para fabricação de filmes com meta-dados sobre os donos dos direitos autorais e/ou com informações dos provedores de quando e como aquele conteúdo pode ser copiado.

A implementação do CGMS-A da Microsoft chama-se *Protected Broadcast Driver Architecture* (PBDA). A PBDA oferece controle DRM tanto para sistemas de *broadcast* como

para dispositivos de entradas analógicas de vídeo. Seu funcionamento é bastante flexível, permitindo a negociação das restrições requeridas por todo produtor de conteúdo. No caso de se seguir o CGMS-A, a PBDA irá encriptar cada *frame* de vídeo obtida da placa de captura, se houverem restrições em relação ao conteúdo. No caso da proibição da geração de cópia do conteúdo, a PBDA impede o sistema operacional de realizá-la.

Entretanto, o uso da PBDA exige que os fabricantes de *hardware* sigam algumas orientações técnicas, e.g., fornecer ao sistema operacional sinais de vídeo apropriados para que o PBDA possa procurar as *flags* contendo as restrições daquele conteúdo. Outra desvantagem está no fato de que os *drivers* de captura de vídeo podem funcionar perfeitamente ignorando o CGMS-A descrito em MICROSOFT (2005) [17]. Alguns fabricantes têm se esforçado para evitar esta conduta por outros fabricantes EFF (2005) [16].

Atualmente, a interface *Broadcast Driver Architecture* (BDA) é utlizada para a transferência de conteúdo de vídeo em claro para a aplicação de gravação. A PBDA é uma extensão desta interface que permite serviços *broadcast* dinamicamente para o *Microsoft Windows Media digital rights management* (WMDRM). O WMDRM é responsável por gerenciar e proteger as chaves de segurança, além de liberar os conteúdos para cópias e/ou reprodução, quando for o caso. Ressalta-se a importância de não degradar o desempenho dos aplicativos que utilizam o conteúdo e atender aos requisitos estabelecidos pela indústria.

Seu funcionamento consiste no estabelecimento de um canal seguro entre os aplicativos e o WMDRM. Tanto os dispositivos PBDA como o WMDRM devem prover e requerer autenticação entre si, garantindo que não estão entregando conteúdo para um dispositivo não autorizado. Os dispositivos devem empregar protocolos padrão de criptografia, notadamente o RSA de chaves pública/privada no início da comunicação e o AES simétrico durante o tempo de execução do conteúdo. O fabricante oferece um manual com maiores detalhes sobre a implementação do PBDA em MICROSOFT (2005) [17].

4. ARQUITETURA DRM COM CONTROLE DE ACESSO E CADEIA DE VALORES

Uma caracterização da cadeia de valor do sistema brasileiro de televisão permite identificar a distribuição e o fluxo das receitas ao longo do processo. Devido à sua importância, este assunto é tratado com detalhes em CPQD (2004) [18]. Nesta mesma referência também é sugerida uma cadeia de valores em um cenário de TV Digital, conforme mostrado na Figura 5. Os detalhes de cada ator e seus papéis podem ser encontrados em CPQD (2004) [18].

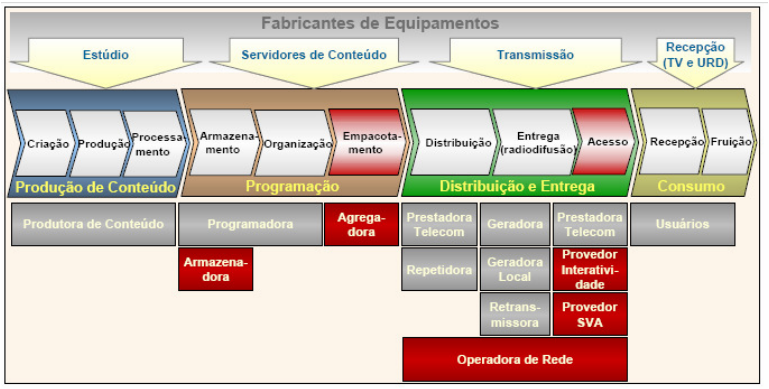

Figura 5 – Novos papéis sugeridos para a TV Digital terrestre.

Entretanto, com o desenvolvimento da TV Digital também surge um importante ator capaz de gerar valor agregado diversas vezes ao longo da cadeia. Trata-se do gerenciador dos direitos autorais ou DRM. Em PAGANI [38] é sugerida uma cadeia de valor com este novo ator, conforme Figura 6.

Figura 6 – Novos papéis sugeridos para a TV Digital terrestre.

Entretanto, este modelo não contempla o subsistema de identificação e rastreamento de cópias ilegais. Em um cenário de convergência dos papéis, este papel será executado pelo gerenciador de direitos autorais. Outro aspecto importante a explicitar é que os atores responsáveis pelos papéis de "Gerenciamento de Direitos e Contratos", "Armazenamento de Informações de Direitos" e "Gerenciamento de Licenças" também podem ser responsáveis pelo controle de acesso (CAS). Na Figura 7, contempla-se os dois casos mencionados. No papel de proteção de conteúdo, utiliza-se, entre outros, os métodos do *Broadcast Flag* e da Marca d'água. No caso de conteúdo reservado, as saídas do DRM incluem uma resposta ao pedido de acesso ao conteúdo (gerada pelo CAS) e, quando cabível, o conteúdo protegido. Percebe-se ainda o vínculo das saídas do DRM com o papel de cobrança. Neste papel, é possível obter informações sobre, por exemplo, pendências financeiras do ator que está requerendo o conteúdo. Desta maneira, mesmo que o ator possua um contrato validando a operação, a liberação do conteúdo está também sujeita à aprovação do papel de cobrança.

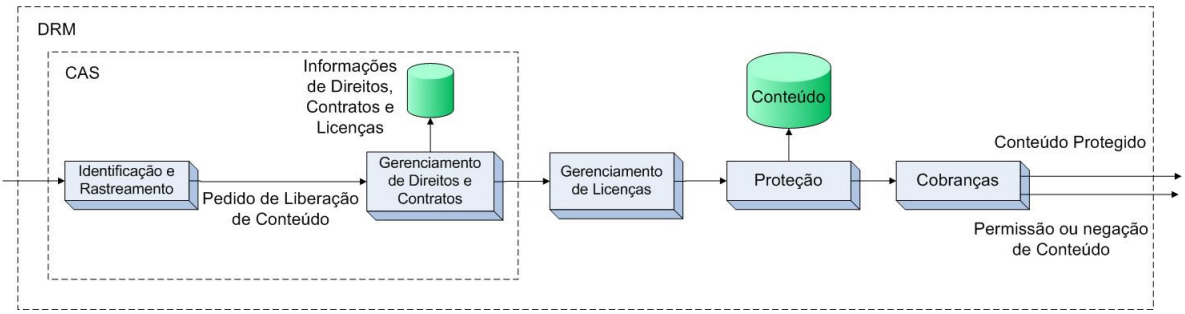

Figura 7 – Identificação, rastreamento e CAS sugeridos para a TV Digital.

A Figura 8 ilustra uma arquitetura para o sistema de TV Digital com proteção DRM e CAS. A Figura também apresenta os papéis dos atores nesta topologia, bem como o fluxo de valor agregado. As paredes indicam uma proteção, ou seja, conteúdos não autorizados não trafegam por estes canais, somente conteúdos liberados. Os cadeados indicam um canal seguro, i.e., exige-se a autenticação dos dois nós de comunicação.

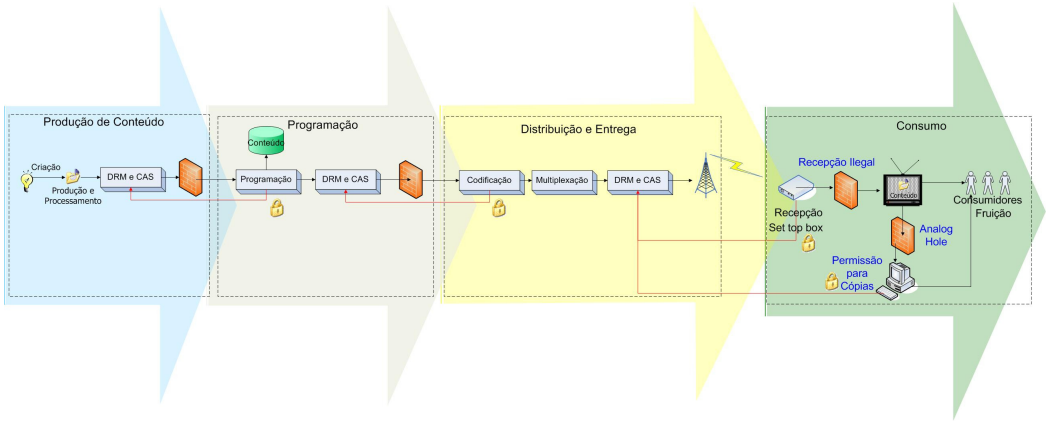

Figura 8 – Arquitetura para TV Digital com proteção DRM e CAS.

Na cadeia de valores da figura 8, nota-se que os gerenciadores de proteção de conteúdo podem agregar valor diversas vezes ao longo da cadeia. Tais gerenciadores atuam notadamente da seguinte maneira:

- Proibindo e/ou limitando sua reprodução
- Proibindo e/ou limitando a sua distribuição.

O gerenciamento da reprodução controla o número permitido de cópias do conteúdo para o consumo do próprio usuário. O gerenciamento da distribuição é responsável por, uma vez criadas as cópias do conteúdo, controlar a interação destas cópias com outros usuários.

Em um cenário de convergência de tecnologias, o mesmo ator poderá executar o papel de proteção de conteúdo para os demais atores. Em um cenário sem convergência, seriam necessários diferentes atores de DRM e CAS para cada etapa da cadeia de valor. Observa-se que a inclusão destes atores implica em uma re-alimentação na cadeia de valores, isto é, mesmo após a entrega do conteúdo ainda é possível agregar valor ao conteúdo, como, por exemplo, por meio do gerenciamento de sua distribuição.

Os atores de produção de conteúdo são responsáveis por desenvolver conteúdos originais. Eles agregam valor ao transformar uma idéia em conteúdo. Este conteúdo, por sua vez, deve estar protegido na interação com os atores de programação.

Os atores de programação adicionam valor agregado ao conteúdo, alterando seu formato, e.g., por meio de propagandas, indicação de horário e faixa etária, entre outros. A relação entre os atores de produção de conteúdo e os de programação ocorre por meio de um sistema DRM, ou seja, um mesmo produtor de conteúdo terá controle sobre a reprodução e a distribuição de conteúdo para diferentes atores de programação por meio do sistema DRM ilustrado na figura 7.

Os atores de distribuição são os responsáveis por fornecer o conteúdo dos atores de programação aos usuários finais. A aquisição de conteúdo a partir dos atores de programação também é realizada por meio de um ator de gerenciamento DRM.

Por fim, nos atores de consumo, além da recepção e fruição, nota-se a adição de uma camada que agrega valor ao conteúdo. Uma das funções desta camada é evitar a recepção ilegal de vídeo por meio de uma comunicação segura entre a *set top box* e os atores de distribuição. Esta comunicação é feita por meio do canal de retorno da *set top box*. Outra função é evitar o problema do *furo analógico*. Após fazer uma gravação ilegal do conteúdo, o

usuário irá transferi-lá para um computador. Por meio de uma comunicação com o ator de DRM, o computador será capaz de impedir a reprodução deste conteúdo, evitando assim sua cópia e distribuição ilegais.

5. ENTIDADES ENVOLVIDAS

Por ser a tecnologia DRM aplicável a qualquer conteúdo armazenado ou a ser copiado para algum meio digital, e como todos nós somos consumidores de conteúdo, a princípio, qualquer pessoa é, ou deveria ser, interessada nesta tecnologia e na forma como ela deve ou não ser implantada.

No entanto, serão citadas aqui apenas as entidades diretamente envolvidas na definição, padronização, implantação, legislação e defesa de direitos, tanto no Brasil quanto no exterior.

A tecnologia DRM em si é elaborada e implantada por diversas empresas, para ser vendida como um produto para grandes criadores ou distribuidores de conteúdo, tais como artistas, estúdios de Hollywood, gravadoras, ou distribuidoras.

Os criadores desta tecnologia normalmente desejam proteger sua criação, mantendo assim seu valor de mercado, e registram patentes. No Brasil, este registro é feito junto ao INPI – Instituto Nacional da Propriedade Industrial [3].

Esta tecnologia, no entanto, tem de ser compatível com outras tecnologias, tais como as utilizadas em rádio, televisão e computadores, e para isto deve obedecer aos padrões existentes. No Brasil, a ABNT – Associação Brasileira de Normas Técnicas e a Anatel – Agência Nacional de Telecomunicações são responsáveis, respectivamente, pela normatização de padrões, e pela regulamentação destes padrões e de seu uso na área de telecomunicações.

No exterior, os principais órgãos normatizadores são a ANSI – American National Standards Institute, a ISO – International Standards Organization e o ETSI – European Telecommunications Standards Institute. O órgão americano equivalente à Anatel, a FCC – Federal Communications Commision, atua no processo de regular o uso de DRM nas telecomunicações nos Estados Unidos.

Há ainda as organizações representantes de interesses de mercado. Por exemplo, o Broadcast Protection Discussion Group (BPDG) [19] é o subgrupo voltado para TV digital do Copy Protection Technical Working Group, este último formado por diversas entidades possivelmente interessadas na implantação compulsória do DRM, incluindo Aiwa, Broadcom, CableLabs, Hitachi, IBM, Intel, MPAA, Matsushita, Microsoft, NEC, Panasonic, Philips, Pioneer, Sony, Toshiba, Viacom e Warner Bros, entre outras.

Do lado dos consumidores, defendendo o banimento de qualquer tecnologia DRM, há a Free Software Foundation (FSF) [20], Electronic Frontier Foundation (EFF) [21], Creative Commons [22], entre outras.

No Brasil, há a ABERT (Associação Brasileira de Emissoras de Rádio e Televisão) [35] do lado das emissoras, e a ProTeste [36] do lado dos consumidores. Já os engenheiros e fabricantes defendem seus interesses através da Sociedade Brasileira de Engenharia de Televisão – SET [37].

Outros participantes óbvios são as casas legislativas, tanto brasileiras quanto estrangeiras. Assim, temos a Câmara e o Senado Federal, a Câmara Distrital e as Assembléias

Legislativas estaduais e Câmaras municipais também atuando, em maior ou menor grau, direta ou indiretamente, no processo de definição da TV digital no Brasil.

6. CONCLUSÕES

Este trabalho apresentou a aplicação de DRM voltada para a TV digital. Este é um tópico de bastante interesse e tem suscitado várias discussões no mundo todo. Foram apresentados os subsistemas DRM, opções de gerenciamento de distribuição de conteúdo, bem como um modelo de DRM baseado em controle de acesso. Outras técnicas de proteção de conteúdo também foram apresentadas.

Mostrou-se que um dos grandes desafios da indústria consiste em controlar a gravação não permitida de conteúdos protegidos a partir de sua forma analógica. Vários métodos foram apresentados, com destaque para o PBDA.

Por ser um assunto de interesse mundial, também foram apresentados os principais players internacionais deste mercado. No Brasil, apresentaram-se as entidades envolvidas com a implementação do DRM no país.

No Brasil, em especial, a TV digital ainda não está em operação, mas a legislação prevê o início de sua operação para o próximo ano FOLHANEWS (2007) [39]. Daí o interesse em se definir as regras de proteção dos direitos autorais desde já, pois uma vez definidas, *hardware* e *software* já seriam produzidos de acordo com a legislação, evitando futuros gastos com trocas ou atualizações de aparelhos fora das especificações.

7. REFERÊNCIAS

[1] GROSSMAN, Lev. “The Battle Over Music Piracy”. Disponível em <http://www.time. com/time/magazine/article/ 0,9171,1625209,00.html?iid=feed-biz_ad>. Acessado em 30 de maio de 2007.

[2] The Free Software Foundation, disponível em <http:// www.fsf.org/campaigns/drm.html>, acessado em 27 de maio de 2007.

[3] INPI, disponível em <http://www.inpi.gov.br/>, acessado em 30 de maio de 2007.

[4] United States Patent and Trademark Office, disponível em <http://www.uspto.gov/>, acessado em 30 de maio de 2007.

[5] NISHIMOTO, Y., BABA, A., KURIOKA, T. e NAMBA, S., “A Digital Rights Management System for Digital Broadcasting Based on Home Servers”, IEEE Transactions on Broadcasting, 2006, pp. 167 – 172.

[6] HARTUNG, F. e RAMME, F., “Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications“, IEEE Communications Magazine, 2000, pp. 78-84.

[7] TRIMECHE, M., CHEBIL, F., “Digital Rights Management for Visual Content in Mobile Applications”, IEEE First International Symposium on Control, Communications and Signal Processing, 2004, pp. 95 – 98.

[8] ZHANG, G. e ZHANG, C. "A Biometric-Based Framework for Digital Rights Protection", IEEE ICSP Proceedings, 2004, pp. 2314 – 2317.

[9] LAN, B. e TAN, T., "A DRM System Implementing RFID To Protect AV Content", 2006

[10] GEER, D., "Digital Rights Technology Sparks Interoperability Concerns", IEEE Computer Society Magazine, 2004, Vol. 37, Issue 12, pp. 20 – 22.

[11] CEN – Comité Européen de Normalisation (Comitê Europeu de Normatização), <http://www.cen.eu/cenorm/businessdomains/businessdomains/isss/activity/cenisssdrmreportfinal30october2003.zip>, acessado em 30 de maio de 2007.

[12] Eletronic Frontier Foundation. "Hollywood Versus the Analog Hole". Disponível em <http://www.eff.org/IP/analog hole/>. Acessado em 27/05/2007.

[13] GODWIN, M.. "What Every Citizen Should Know About DRM." Public Knowledge New America Foundation, Washington.

[14] BASTOS, A. & FERNANDES, S., Televisão Digital, Antenna Edições Técnicas, Rio de Janeiro / RJ, 2004.

[15] Eletronic Frontier Foundation. "Protected Media Path, Component Revocation, Windows Driver Lockdown", de 25 de julho de 2005. Disponível em <http://www.eff.org/deeplinks/archives/003806.php>. Acessado em 29/05/2007.

[16] Eletronic Frontier Foundation. "Microsoft Sells Out the Public on CGMS-A", de 27 de julho de 2005. Disponível em <http://www.eff.org/deeplinks/archives/003807.php>. Acessado em 29/05/2007.

[17] Microsoft. "Protected Broadcast Driver Architecture", de 25 de abril de 2005. <http://www.microsoft.com/whdc/device/stream/BDA_protect.mspx>. Acessado em 29/05/2007.

[18] CPqD / FUNTTEL. "Cadeia de Valor – Projeto Sistema Brasileiro de Televisão Digital – Modelo de Implantação – OS 40539". Disponível em <http://www.fndc.org.br/arquivos/MapeamentoCadeiadeValor-CPQD.pdf>. Acessado em 15/06/2007.

[19] Broadcast Protection Discussion Group, subgrupo do Copy Protection Technical Working Group, <http://www.cptwg.org/html/Bpdg_home_page.htm>, acessado em 30 de maio de 2007.

[20] Free Software Foundation. <http://www.fsf.org/>, acessado em 30 de maio de 2007.

[21] Electronic Frontier Foundation. <http://www.eff.org/>, acessado em 30 de maio de 2007.

[22] Creative Commons <http://creativecommons.org/>, acessado em 30 de maio de 2007.

[23] Electronic Frontier Foundation, <http://www.eff.org/IP/ broadcastflag/>, acessado em 30

de maio de 2007.

[24] Casa Civil da Presidência da República, Decreto nº 4.901, de 26/11/2003. <http://www.planalto.gov.br/ccivil/ decreto/2003/D4901.htm>, acessado em 30 de maio de 2007.

[25] Casa Civil da Presidência da República, Decreto nº 5.820, de 29/06/2006. <http://www.planalto.gov.br/ CCIVIL_03/_Ato2004-2006/2006/Decreto/D5820.htm>, acessado em 30 de maio de 2007.

[26] Senado Federal, Decreto nº 52.795, de 31/10/1963. <http://www6.senado.gov.br/legislacao/ListaPublicacoes.action?id=114597>, acessado em 30 de maio de 2007.

[27] Casa Civil da Presidência da República, Medida Provisória nº 352, de 22/01/2007. <http://www.planalto. gov.br/CCIVIL/_Ato2007-2010/2007/Mpv/352.htm>, acessado em 30 de maio de 2007.

[28] Casa Civil da Presidência da República, Lei nº 9.472, de 16/07/1997. <http://www.planalto.gov.br/ccivil/leis/L9472. htm>, acessado em 30 de maio de 2007.

[29] Casa Civil da Presidência da República, Lei nº 4117, de 27/08/1962. <http://www.planalto.gov.br/ccivil/Leis/L4117. htm>, acessado em 30 de maio de 2007.

[30] World Intellectual Property Organization, "Proposal for the establishment of a developpment agenda for WIPO". <http://www.wipo.int/documents/en/document/govbody/wo_gb_ga/pdf/wo_ga_31_11.pdf>, acessado em 30 de maio de 2007.

[31] United States Congress, "Digital Millennium Copyright Act". <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi? dbname=105_cong_public_laws&docid=f:publ304.105.pdf>, acessado em 30 de maio de 2007.

[32] FreeCulture.org, "University DMCA Policies". <http://freeculture.org/blog/2007/05/17/university-dmca-policies/>, acessado em 30 de maio de 2007.

[33] União Européia, "Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society" <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML>, acessado em 30 de maio de 2007.

[34] GIOVANI, H. "Proteção do Conteúdo Audiovisual na Televisão Digital", Disponível em <www.senado.gov.br/sf/atividade/Conselho/CCS/Documentos/CCS20060605-GiovaniHenrique.pdf>. Acessado em 31/05/2007>.

[35] ABERT <http://www.abert.org.br>, acessado em 31/05/2007.

[36] ProTeste <http://www.proteste.org.br>, acessado em 31/05/2007.

[37] SET <http://www.set.com.br>, acessado em 21/06/2007.

[38] PAGANI, M. “Multimedia and Interactive Digital TV: Managing the Opportunities Created by Digital Convergence”. IRM Press, 2003.

[39] Correio Braziliense, citando FolhaNews, “TV digital chega ao Brasil em dezembro, mas sem interatividade”. <http://noticias.correioweb.com.br/materias.php?id=2708734&sub=Economia>, acessado em 29 de maio de 2007.