"Digital Rights Management"

DRM e suas consequências

Tiago Serra
Março 2005
tserra [at] student.dei.uc.pt

Vivemos actualmente em guerra com editoras discográficas. Estas sentem-se ameaçadas por tecnologias que dão aos fans acesso a música de formas nunca antes por elas planeadas. Mas é tudo, no mínimo, paradoxal, porque as editoras sentem-se mais lesadas do que os próprios artistas. Se calhar porque são glutões capitalistas, que perdem, ou melhor, não ganham, os dólares que deviam ir para o criador. “We finally have the technology to share information. How could that not make the world a better place? Piracy may currently be illegal, but I have no question in my mind that is morally right.”, comentava alguém para a Wired deste mês. Pirataria no sentido de partilha, é este o adjectivo que os *media* gostam de usar.

Os direitos de autor existem para que o trabalho dos criadores seja rentabilizado e, dessa forma se sintam encorajados a serem mais produtivos. No entanto a obtenção destes direitos não é garantia de lucro.

No passado esta rentabilização era efectuada através do controlo da sua distribuição. Hoje em dia a distribuição pode ser conseguida de forma quase gratuita ou mesmo gratuita graças ao poder da Internet. Estamos tão tecnologicamente avancados que tal deixa de fazer sentido. No entanto, isso não quer dizer que os direitos de autor necessitem de ser alterados. Pelo contrário, os primeiros princípios destes direitos ainda permanecem intactos e, são a única forma de obter aprovação governamental do monopólio desse trabalho. Desprovidos destes direitos, o trabalho sería de domínio público. Assim, os criadores apenas terão de encontrar outra forma de rentabilização, e não de condenar aqueles que obtêm a música por outros meios.

O DRM ou "Digital Rights Management" é o termo usado para uma tecnologia que permite a uma entidade, que poderá ser o autor, vender um produto com direitos de autor e controlá-lo restringindo o seu uso. Por exemplo, um MP3 que só poderá ser ouvido no sistema do comprador.

Embora formas de controlo de software serem comuns desde os anos 80, o DRM tem sido usado cada vez mais em trabalhos artísticos. É este o contexto que pretendo aprofundar neste artigo.

Na verdade, o DRM tem muito pouco a ver com protecção de direitos de autor. Segundo a lei, o uso de obras para uso académico, noticioso, crítica ou comentário, pesquisa e ensino não é uma violação destes direitos. Admitidamente existem áreas cinzentas, mas no geral estas leis existem para impedir a cópia com a finalidade de venda. O DRM não impede às pessoas de cometerem acções proibidas pelas leis de direitos de autor, mas sim acções que são permitidas pelas leis de direitos de autor. Por ex-

emplo, existem e-books onde não existe qualquer lei de direitos de autor associada a essas obras, e, cujo DRM nos impede de o imprimir mais de 5 vezes por ano. Apesar de possuírmos todo o direito de imprimir quantas vezes as necessárias, isto força um direito que os publicadores neste caso não possuem e tiram-nos um direito que na realidade temos. É claro que a restrição deste publicador de imprimir o documento apenas 5 vezes podia ser diferente, ele podia antes simplesmente impedir a sua impressão. Esta escolha não é baseada em leis de direitos de autor, mas sim, na capacidade que o publicador possui graças ao poder do sistema DRM. O publicador é assim o determinante das restrições do produto. O produto neste caso poderá ser, por exemplo um ficheiro MP3, um e-book, etc. Sendo assim, a conclusão a que chego é que a existência do DRM tem motivos puramente económicos.

No mundo real o mercado rege-se através das leis de oferta e procura. Quando existe muita procura e pouca oferta os preços sobem. Ora, quando lidamos com o mundo real, oferta e procura funcionam relativamente bem, mas quando lidamos com o mundo digital, onde infinitas cópias podem ser realizadas com facilidade, este paradigma deixa de fazer sentido. O DRM tem, assim, como objectivo diminuir a oferta de forma a que publicadores possam exigir preços mais altos. É claro que, para produtos onde facilmente achamos alternativas desprovidas de DRM, os publicadores veem-se na obrigação de baixar o preço, mas nem sempre é assim. O mesmo acontece com muitos outros produtos com direitos de autor: não deixamos de comprar livros só porque os podemos requisitar numa biblioteca pública! O DRM elimina por completo bibliotecas; elimina por completo a ideia de "emprestar". Muitas pessoas não compram livros novos mas sim livros usados; o DRM elimina livros usados, elimina a revenda. Poderemos chamar piratas às pessoas que requisitam livros de uma biblioteca? Não me parece.

Além disso, as leis de direito de autor não restringem a revenda, por isso é perfeitamente legal vender, desde que este produto não seja uma cópia. Da mesma forma, alguns tipos de cópia são permitidos sob a lei de direitos de autor. Por isso, a tecnologia DRM, restringe ou impede, o comprador de exercer o seu direito a este respeito.

Cory Doctorow [1], jornalista, blogger, escritor de ficção cientifica e membro da EFF, deu o ano passado um discurso sobre DRM a um grupo de desenvolvimento da Microsoft nesta empresa [2]. Ele apresentou muitos pontos de vista. Um deles foi que o DRM não só não funciona como nunca funcionará. Na verdade o DRM pode funcionar. A afirmação de Doctorow é verdadeira, mas apenas no mundo do software, onde o sistema pode ser subvertido. Ao contrário do software, o hardware é vitima de um sem número de regulamentações. Como no mundo informático o hardware se torna obsoleto ao fim de poucos anos, se novos regulamen-

tos forem criados que incorporem DRM, a criação destes iria transformar toda a infraestrutura da Internet ao fim de poucos anos. Será assim tão difícil que leis como estas sejam aceites? Não me parece, pode acontecer, como no ultimo filme de Michael Moore (9/11), onde um membro da *U.S. House of Representatives* lhe diz: "Sit down my son, we don't read most of the bills we vote on".

Nos Estados Unidos existem leis propostas, já desde 2001, que tornarão o DRM obrigatório em todos os sistemas informáticos, e os produtores desse hardware, responsáveis por violações da lei que os utilizadores possam cometer. Até agora estas leis têm sido combatidas, mas não durará muito tempo até "que", e não "se", estas leis entrem em vigor e toda a indústria seja afectada.

Outra afirmação que Doctorow diz a respeito do DRM em software, diz respeito à sua inutilidade. Na sua pespectiva e na minha, é realmente descabido fazê-lo, isto porque, quando se expõe um sistema DRM em software, haverá alguém que seja suficientemente habil e/ou inteligente que o irá subverter. Posteriormente publicá-lo online, bem como software que permita extrair o DRM. Mas também me parece, que isto não torne o sistema inválido.

Um dos primeiros exemplos de um sistema DRM, foi o Content Scrambling System ou CSS, empregado pelo *Forum DVD* [3] nos DVDs. Foi originalmente desenvolvido no Japão pela Matsushita. Os dados num DVD encontram-se encriptados, de forma a que, só possam ser lidos usando uma chave criptográfica, que o *DVD Consortium* manteve em segredo. De forma a ter acesso a esta chave, um fabricante de um leitor de DVDs necessitaria de assinar um contrato de licenciamento, com o *DVD Consortium* e, os restringia de incluírem nos seus leitores algumas funcionalidades desejadas, como saída digital que podería ser usada para copiar um filme com alta qualidade. Visto o único hardware no mercado capaz de desencriptar os DVDs ser controlado pelo *DVD Consortium*, estes esperavam ser capazes de impor quaisquer restrições na leitura de filmes. O DIVX, por exemplo, era um sistema deste género, mais restritivo e comercialmente menos aceite que hoje em dia não existe, e cujo nome é usado em tributo irónico a este DRM para uma implementação de compressão de vídeo MPEG-4.

Mas, à uns anos atrás, um jovem chamado Jon Johanson escreveu um programa que permitia ler DVD's em sistemas Linux [4]. Ele subverteu o DRM dos DVD's de forma a que pudesse ler o DVD que era seu, num sistema que era também seu. Mas, como não possuia um leitor certificado pela *DVD Consortium*, a indústria e os *média*, habilmente se encarregaram de o etiquetar como pirata.

Na verdade, a maior parte das pessoas, apesar de o “hack” existir, preferem conformar-se com as restrições impostas pelos criadores do formato. Isto porque, é incómodo ter de ultrapassar esse obstáculo: fazer o download do código ou do programa e, esperar que funcione no seu sistema. Apesar disso, muitas pessoas são leigas e incapazes de o fazer.

Logo, a existência do “hack”, torna este sistema DRM mais frágil mas não menos útil. Na verdade, o DRM dos DVDs tem tido bastante sucesso do ponto de vista da indústria cinematográfica. Muitas pessoas, impossibilitadas de o copiar, preferem comprar outra cópia. Este sistema teve por isso bastante sucesso em diminuir a oferta de material com direitos de autor, apesar da existência deste “hack”.

Frágil, porque foi baseado em software e não complementado com um hardware que impingi-se as mesmas condições. O hardware é bastante mais difícil de subverter do que software. Não é de forma nenhuma impossível, mas também existem muito menos pessoas capazes de o fazer. Além disso, torna-se execuível tornar um “hack” incompatível com um sistema igual. Assim que o DRM chegar ao hardware, tornará tudo um pouco mais difícil.

Um dos grandes apoiantes do DRM tem sido a Microsoft. Não apenas esta empresa, mas ela e outras têm trabalhado em algo chamado "Trusted Computing". Este nome quase nos engana. Na verdade, "Trusted" ou confiável, significa que estas empresas podem confiar no seu computador para fazer ou não fazer algo. E quando fazer ou não fazer algo conflítua com o desejo do utilizador, o desejo da empresa sai vencedor. Claro que isto é exactamente o oposto do conceito de confiança que conheço, isto é, algo que controlo e no qual tenho uma confiança íntima de procedimento. O mesmo é dizer que, um sistema que foi penetrado é um sistema confiável. Claro que este sistema irá responder aos nossos pedidos mas, será também controlado por uma terceira entidade que poderá encarregar-se de o negar caso seja o seu objectivo.

A Microsoft chama ao seu sistema de "Trusted Computing" Palladium. Quando começou a ter muitas criticas na imprensa, alterou o seu nome para "Next Generation Secure Computing Base" ou NGSCB. Na verdade o seu nome não interessa, este sistema fará parte da proxima versão do seu Sistema Operativo Longhorn, e será também implementado em sistemas XP através de updates em forma de *Service Packs*.

Muitas empresas de hardware que fabricam BIOS e CPU’s encontram-se à espera do lançamento do Longhorn de forma a implementarem sistemas em hardware que, em parceria com o Sistema Operativo, desempenhem as suas funções avincadamente.

Sobre o Palladium, e funcionando com um cripto-processador embebido no PC, sistemas como este irão criar uma nova classe de aplicações que terão poderes especiais e protecções que funcionarão lado a lado com aplicações convencionais. O dito objectivo é corrigir os problemas actuais da insegurança informática, e criar novos tipos de aplicações distribuidas, onde cada componente pode saber e confiar noutras partes do sistema, mesmo quando estas se encontram em sistemas remotos.

É obvio que esta não é a forma de tornar os sistemas mais seguros, mas sim de controlar o mercado de hardware e software firmemente e extender o seu monopólio do *Windows*.

Quando estava a pesquisar para este artigo, deparei-me com um artigo da UK Metro [5], onde um “security expert” a trabalhar para a Microsoft, Simon Conant, dizia: "We need to go back to the drawing board with a brand new architecture for the PC". Referia-se ao facto do uso de DRM para acabar com os problemas de segurança. Ora:

1º - O SoBig.F apenas afecta/infecta sistemas operativos Microsoft, e, mesmo assim, apenas aqueles que usam o Outlook como o seu programa de e-mail. Qualquer programa de e-mail que não contenha uma linguagem de scripting inerentemente insegura, não será vítima deste tipo de virus. Usar um programa que não contenha estas falhas é uma defesa perfeitamente adequada para os virus de e-mail;

2º - Segundo os seus argumentos, uma das funcionalidades principais do NGSCB é proporcionar imunidade a programas "confiáveis" de outros programas, incluindo os vírus. Mas mesmo estes podem ser infectados, e vírus em forma de scripts que se executam de e-mails continuarão a ser executados;

3º - Mesmo que seja encontrada uma forma de impedir que scripts maliciosos se executem dentro de programas assinados pelo NGSCB, é demasiado moroso introduzir o NGSCB quando uma simples troca de sistema operativo e/ou de programa de e-mail seria suficiente, especialmente dado todas as outras desvantagens do NGSCB;

Consequências

- Monitores com DRM. Se desejarem ver uma imagem que não seja permitida, o próprio monitor encarregar-se-á de o impedir;

- Placas de som que impossibilitam a leitura de ficheiros de som, porque reconhecerão marcas de água inaudíveis, que o definem como material com direitos de autor e para o qual não terá autorização;

- Televisores e vídeos com DRM. Imaginem verem um programa televisivo, cuja emissora deseja que não seja reproduzido e o tentarem gravar: o video irá recusar-se a fazê-lo. Este video que lhe pertence, e que devia seguir as suas ordens, será confiável (”Trusted”); [6]

etc. ...

Na verdade, nem tudo é negro, o DRM foi usado por organizações como a British Library, no seu seguro serviço electrónico, de forma a permitir acesso mundial a um substancial número de raros (e em muitos casos únicos) documentos que, por razões legais, estavam apenas disponíveis a indivíduos autorizados que visitavam fisicamente o centro de documentos da biblioteca em Boston Spa - Inglaterra. Este é um raro caso onde o DRM na verdade aumentou o acesso público a um material restrito em vez de o diminuir.

Privacidade

Estas tecnologias têm também muitas implicações de privacidade que eu não aprofundei. Por exemplo, estas protecções podem assumir duas formas distintas: encriptação, onde a informação pode apenas ser lida por utilizadores autorizados, e marcação (”watermarking”), que não impede o uso ilicito, mas permite que estas cópias sejam identificadas posteriormente.

Nesta perpectiva, oportunidades comerciais e funcionalidades, tais como permitir que utilizadores autorizados possam fazer upgrade para uma versão mais completa de um programa informático tornam-se possiveis, mas também, capacidades de localização, identificando assim “*quem”* está a usar *o “quê”* e “*onde”*.

A localização pode também ser usada para criar perfis de utilizadores. Se, o conteúdo de um trabalho com direitos de autor poder contactar o autor através da Internet, todas as vezes que é usado ou transferido, não apenas poderá o autor verificar a autenticidade das cópias em circulacao, bem como criar uma imagem dos padrões de uso dos utilizadores, das suas localizações, etc. A Microsoft é um fervoroso apoiante de tecnologias de localização, algumas das quais estão implementadas no seu *Windows Media Player*, por exemplo.

Conclusão

Para muitos destes sistemas haverá “hacks” com certeza, mas a grande maioria dos utilizadores não os usará, porque, será dificil contorná-los preferindo assim conformar-se. Talvez países asiáticos façam concorrência ao mercado norte americano com hardware desprovido de DRM [7], mas, se não for este o caso, então precisaremos de mais pessoas como aquelas que tornaram possivel correr Linux numa Xbox ou ler DVDs em sistemas não autorizados. Serão estes que tornarão possivel subverter sistemas tão draconianos como o apresentado neste artigo. Mas estes possivelmente estarão a cometer uma ilegalidade graças a outras leis descabidas, protectoras de lobbies, tais como o DMCA[8].

Sou um optimista por natureza, e acredito que os consumidores em geral irão aperceber-se destas restrições e “fugir” de tais “tecnologias”. Mas se o futuro não for esse, então espero que *hackers* como os descritos anteriormente, detentores de antigas máquinas de turing, esperançosamente as retornarão para os sistemas não restritos que eram antigamente.

DRM - Alguns exemplos

- Serial copy management system (SCMS)

http://en.wikipedia.org/wiki/Serial_copy_management_system

- Macrovision

http://en.wikipedia.org/wiki/Macrovision

- Steam usada pela Valve Software para controlar jogos como o Half-Life 2

http://en.wikipedia.org/wiki/Steam_(content_delivery)

- iTunes (que incorpora o DRM FairPlay da Apple para download de conteudos atraves da loja de musica do iTunes)

http://en.wikipedia.org/wiki/Apple_iTunes

- Windows Media Player (usando o Windows Media Audio ou Windows Media Video, que ambos suportam DRM)

http://en.wikipedia.org/wiki/Windows_Media_Player

- OMA - Encontrado em alguns telemoveis

http://www.openmobilealliance.com/

- RealNetworks Music Store da RealNetworks tem um DRM tambem proprio -

http://en.wikipedia.org/w/index.php?title=RealNetworks_Music_Store&action=edit

- Sony anunciou a sua loja de musica chamada Connect usando um DRM chamdo OpenMG. O OpenMG suporta o formato de som da Sony chamado ATRAC

http://en.wikipedia.org/wiki/Sony

- MMK - Um numero de pequenas empresas como a MMK Secure stream oferecem DRM para as massas

http://www.mmksecurestream.com/

- Digital Transmission Content Protection (DTCP)

http://en.wikipedia.org/wiki/Digital_Transmission_Content_Protection

- Content Protection for Recordable Media (CPRM) -

http://en.wikipedia.org/wiki/Content_Protection_for_Recordable_Media

- High-Bandwidth Digital Content Protection (HDCP)

http://en.wikipedia.org/wiki/High-Bandwidth_Digital_Content_Protection

Referências

[1] http://en.wikipedia.org/wiki/Cory_Doctorow

[2] http://www.craphound.com/msftdrm.txt

[3] http://www.dvdforum.com/forum.shtml

[4] http://www.free-dvd.org.lu/

[5] http://archives.linuxfromscratch.org/mail-archives/lfs-chat/2003-August/016683.html

[6] http://www.eff.org/broadcastflag/

[7] http://news.xinhuanet.com/english/2005-02/25/content_2618207.htm

[8]

http://www.copyright.gov/legislation/dmca.pdf

http://anti-dmca.org/

http://www.eff.org/IP/DMCA/

Artigos

http://pfeifferreport.com/trends/ett_DRM.html

http://www.teleread.org/publishersdrm.htm

http://yro.slashdot.org/article.pl?sid=05/02/24/1847227&from=rss

http://www.fourmilab.ch/documents/digital-imprimatur/

http://www.gnu.org/philosophy/right-to-read.html

Estórias

http://journals.aol.com/garvis79/TriggersModerateOpinions/entries/204

http://bigpicture.typepad.com/comments/2004/06/industry_spinni.html

http://msl1.mit.edu/furdlog/index.php?p=2099

Fontes

http://en.wikipedia.org

http://www.drmwatch.com/