

مدیریت حقوق دیجیتال: فرصت‌ها و چالش‌ها

مرضیه سیامک^۱

چکیده

با توجه به نقش اطلاعات به عنوان کالای با ارزش و لازمه حفاظت از آن در تجارت امروز، طراحی سیستمی برای مدیریت امنیت اطلاعات است، تا از این طریق بتوان از سرمایه‌های اطلاعاتی خود حفاظت کرد. برای دستیابی به این هدف، مدیریت حقوق دیجیتال مطرح شده است. این مقاله مدیریت حقوق دیجیتال را براساس آخرین تغییرات شرح می‌دهد. کاربرد مدیریت دیجیتال، روند تکامل، جنبه‌های مختلف آن، مؤلفه‌های مطرح در مدیریت حقوق دیجیتال، معماری اصلی، زبان‌های مهم و مسائلی از این قبیل را شرح می‌دهد. در پایان چالش‌های مطرح درباره آن را بیان می‌نماید.

کلیدواژه‌ها

مدیریت حقوق دیجیتال، محتویات دیجیتالی، تجارت الکترونیکی.

مقدمه

یکی از بخش‌های سودآور و در حال رشد اقتصاد امروز، صنعت اطلاعات است. صنعت اطلاعات در مدت کوتاهی فرصت‌های شغلی جدیدی با تولیدات اطلاعاتی دیجیتال ایجاد کرده است.

در حال حاضر، تکنولوژی‌های جدیدی مانند ارتباطات از راه دور، اینترنت و غیره، الگوهای شغلی جدیدی مثل تجارت

الکترونیکی را ممکن می‌سازند. این مسئله در حوزه تجارت دیجیتالی، موجب رواج اطلاعات می‌شود و کانال‌های توزیعی تازه‌ای فراهم می‌کند که در نهایت موجب کاهش هزینه‌ها و موانع می‌گردد. اما سالیان سال دستیابی به تجارت بی‌نقص محتویات دیجیتالی رؤیای دیرینه ناشران و توزیع‌کنندگان بوده است. توزیع اطلاعات در قالب‌های دیجیتالی، به‌ویژه در اینترنت، مفاهیم قانونی

۱. کارشناسی ارشد کتابداری و اطلاع‌رسانی msiamakm@gmail.com

زیادی را مطرح می‌کند.

اینترنت از ابتدا براساس معماری باز^۲ طراحی شده است که این مسئله فرصت‌های شغلی جدید زیادی را ممکن می‌سازد، اما در هنگام استفاده غیرقانونی از اطلاعات آسیب‌پذیر است. برای تهیه‌کنندگان اطلاعات، کنترل این‌که دیگران با اطلاعات چه کار می‌کنند، مشکل است. به عنوان مثال یک مشکل بزرگ ناشران، انتشار و نسخه‌برداری غیرقانونی از آثار آنهاست. چرا که تکثیر اطلاعات دیجیتال بسیار آسان و به خوبی کیفیت همان متن اصلی است (۱۲).

برخلاف مواد آنالوگ، همه کپی‌های مواد دیجیتال، اصل هستند. فن‌آوری جداسازی و نسخه‌برداری مواد دیجیتال به حدی ارزان است که در ذهن نیز نمی‌گنجد (۵). به‌طوری‌که دیگر نمی‌شود میان اثر اصلی و نمونه‌های کپی‌برداری شده کوچک‌ترین تفاوتی دید. پس طرفداران موسیقی و دیگر

محتویات دیجیتالی می‌توانند آثار موردنظر خود را برای صدها تن از دوستان ارسال کنند، بی‌آنکه لازم باشد کوچک‌ترین هزینه‌ای بابت این مسئله پردازند (۳).

این مسئله منجر به کاهش معنی‌دار نویسندگان، ناشران و کاربران مجاز گذشته است. چرا که تولیدکنندگان محتویات دیجیتال زیادی با کپی‌برداری غیرقانونی از محتویات اطلاعاتی، موسیقی، فیلم، نرم‌افزار، بازی و غیره، بلیون‌ها دلار خسارت دیده‌اند (۱۴: ۱۱۰-۱۱۱). اکنون صنعت نیاز فوری به مکانیسم کارآمدی برای حمایت از تجارت الکترونیکی دارد (۱۲). با توجه به نقش اطلاعات به عنوان کالای با ارزش لزوم حفاظت از آن در تجارت امروز ضروری به نظر می‌رسد. برای دستیابی به این هدف نیاز به طراحی سیستمی برای مدیریت امنیت اطلاعات است تا از این طریق بتوان از سرمایه‌های اطلاعاتی خود حفاظت کرد^۳ (۱).

۲. معماری اینترنت، معماری شبکه‌ای غالب در اوایل دهه ۲۰۰۰ است. اینترنت بر پروتکل اینترنت (آی‌پی) استوار است که می‌توان آن را روی همه انواع شبکه‌های فیزیکی و تحت همه انواع برنامه‌های کاربردی به کار انداخت. استقلال پروتکل اینترنت هم از شبکه‌های فیزیکی و هم از برنامه‌های کاربردی، نقطه قوت اصلی آن است. این پروتکل حتی با فن‌آوری‌های شبکه‌ای کاملاً جدید، مثل «شبکه محلی بیسیم» (دبیلولن) یا «سرویس رادیویی بسته‌ای عمومی» (جی‌پی‌آراس) و شبکه «سامانه عمومی ارتباطات همراه» (جی‌اس‌ام) نیز کار می‌کند. برنامه‌های جدید، مثل وب، «وو‌آی‌پی»، و بسیاری برنامه‌های دیگر را که در آینده عرضه می‌شوند، می‌توان به راحتی با سرویس استاندارد پروتکل اینترنت اجرا کرد. معماری اینترنت اساساً از سال ۱۹۷۴ ثابت مانده و همچنان قدرت خود را اثبات می‌کند. بنابراین شعار قدیمی «آی‌پی ورای همه، همه چیز بر روی آی‌پی» امروز بیش از هر زمان دیگری صدق می‌کند. عیب‌های اصلی «آی‌پی»، فضای ناکافی نشانی، عدم پشتیبانی از جابه‌جایی فیزیکی، فقدان کیفیت متمایز سرویس، و فقدان امنیت آن است (۲).

۳. گرچه بحث دسترسی به اطلاعات و از سوی دیگر امنیت و حفاظت از اطلاعات از زمان‌های قدیم برای تمام دولت‌ها مطرح بوده و دستیابی به اطلاعات نظامی و کشوری گاه موجب نابودی قومی می‌شده است اما با توسعه فن‌آوری اطلاعات و استفاده از اطلاعات به عنوان یک ابزار تجاری و سرمایه سودآور، بحث امنیت اطلاعات بعد جدیدی به خود می‌گیرد. در تجارت امروز، اطلاعات نقش سرمایه یک شرکت را ایفا می‌کند و حفاظت از اطلاعات سازمان یکی از ارکان مهم بقای آن می‌باشد. جهانی شدن اقتصاد منجر به ایجاد رقابت در سطح جهانی شده و بسیاری از شرکت‌ها برای ادامه حضور خود در عرصه جهانی، ناچار به همکاری با سایر شرکت‌ها هستند. به این ترتیب، طبقه بندی و ارزش‌گذاری و حفاظت از منابع اطلاعاتی سازمان (چه در مورد سیستم اطلاعاتی و چه اعضای سازمان) بسیار حیاتی و مهم به شمار می‌رود. سیستم مدیریت اطلاعات ابزاری در جهت طراحی، پیاده‌سازی و کنترل امنیت نرم‌افزار و سخت‌افزار یک سیستم اطلاعاتی است (۱).

برای دستیابی به این هدف، مدیریت حقوق دیجیتال^۴ مطرح شده است. البته آرزوی داشتن سیستم‌های مدیریت حقوق دیجیتال قوی در دنیای تجارت تازه نیست. به راستی، سیستم توسعه و پیشرفت علمی و صنعتی با شیوه‌های مدیریت حقوق دیجیتال سابقه طولانی دارد. البته هنوز صنعت موفقیت تجاری زیادی در ارسال کالا با این سیستم نداشته است. فاکتورهای زیادی در عدم پذیرش سیستم‌های مدیریت حقوق دیجیتال رایج دخیل هستند که لامکیا^۵ از شرکت ماکروسافت معتقد است که سه عامل در این زمینه از اهمیت ویژه‌ای برخوردارند، که عبارتند از: فقدان شیوه‌های محاسبه درست فراگیر، موتورهای مدیریت مطمئن و قوی و حقوق به یک مفهوم عمومی (۱۳).

با توجه به مسائل مطرح شده، این مقاله به بحث مدیریت حقوق دیجیتال می‌پردازد و مؤلفه‌های مطرح در مدیریت حقوق دیجیتال را مانند مدل حقوقی، مفاهیم اصلی، جنبه فنی، جنبه قانونی، جنبه اجتماعی، معماری اصلی، زبان‌های مهم و مسائلی از این قبیل را شرح می‌دهد.

مدیریت حقوق دیجیتال (DRM)

مدیریت حقوق دیجیتال به حمایت از حق نشر محتویات الکترونیکی مربوط می‌شود و در این رابطه بزرگ‌ترین چالش‌ها را برای کپی‌برداری غیر مجاز ایجاد می‌کند. با محدود کردن فعالیت‌ها و استفاده از محتویات

موردنظر به کاربر مجاز، به حمایت از حق نشر می‌پردازد. در دایره‌المعارف ویکی‌پدیا مدیریت حقوق دیجیتال چنین تعریف شده است: «چتری گسترده که به روش‌های فنی مختلف استفاده شده در توصیف، لایه‌بندی، تحلیل، ارزیابی، تجارت، و نظارت حقوق آثار دیجیتال برمی‌گردد» (۱۳). DRM به ناشران محتویات دیجیتال، توانایی توزیع مطمئن محتویات با ارزش آن‌ها را مثل نشریات، کتاب‌ها، عکس‌ها، مواد آموزشی، ویدئو و غیره را می‌دهد، تا استفاده از آن‌ها را کنترل کنند و از توزیع غیرمجاز آن‌ها ممانعت کنند (۱۱).

مدیریت حقوق دیجیتال، رشد تجارت محتویات الکترونیکی را ممکن می‌سازد (۱۱). با اجرای قانون مدیریت حقوق دیجیتال (DRM) فیلم‌ها، موسیقی‌ها و دیگر محصولات دیجیتال رمزگذاری شده و از کپی‌برداری مخفیانه آن‌ها جلوگیری می‌شود. بدین ترتیب تنها کسانی حق دسترسی به آثار مربوط را خواهند داشت که بابت دریافت کلید رمزها، مبلغی پرداخت کرده باشند (۳). متأسفانه، تا سال ۲۰۰۱ تعریف قابل قبولی برای DRM در میان کنسرسیوم‌هایی که سیستم‌های DRM را توسعه داده بودند، ارائه نشده بود. تا اینکه W3C (کنسرسیوم وب جهان‌گستر) یک گروه کاری DRM در ژانویه ۲۰۰۱، تنظیم کرد. ۶۵ نماینده اصلی را برای بحث و تفکر درباره مدیریت حقوق دیجیتال گرد آورد.

مدیریت حقوق دیجیتال پیشنهاد شده

در W3C مدیریت دیجیتال حقوق^۶ بود، نه مدیریت حقوق دیجیتال؛ که توصیف، شناسایی، تجارت، حفاظت، کنترل، و پیگیری همه قالب‌های استفاده حقوق و مدیریت روابط مالکان حقوق را در بر می‌گرفت (۱۲). بعد از آن مدیریت حقوق دیجیتال در سال‌های اخیر چنین تعریف شده است:

DRM واژه اختصاری «مدیریت حقوق دیجیتال» است. واژه‌ای کلی که برای شرح تعدادی از تکنیک‌های محدودکننده استفاده آزاد و انتقال محتوای دیجیتال، استفاده می‌شود (۱۲)؛ و مفهومی برای اداره، کنترل، دسترسی و استفاده از موجودی‌های دیجیتال است (۷). DRM یک سری تکنولوژی‌هایی است که با استفاده از آن مالکان محتوای دیجیتال می‌توانند از تکثیر غیرقانونی محتویات خود، حفاظت کنند؛ سیستمی است که محتویات رسانه دیجیتال را رمز گذاری می‌کند و دسترسی را فقط به افرادی که اجازه استفاده از آن محتویات را دارند، می‌دهد (۷). مدیریت حقوق دیجیتال سیستمی است که توزیع، گسترش و فروش محتویات را در اینترنت فراهم می‌کند.

فن‌آوری مدیریت حقوق دیجیتال، مانع از کپی برداری انبوه و غیرمجاز فایل‌های موسیقی شده و فایل‌هایی از این دست را که از طریق شبکه‌های P2P^۷ اشتراک گذارده می‌شوند، نیز غیر قابل اجرا می‌کند (۳).

به‌طور اساسی (DRM) یک روش فنی حمایت از محتویات دیجیتال است (۱۷)؛

که اعمالی برای مراقبت از حقوق پدیدآورنده متن، انجام می‌دهد. این اعمال شامل محدود نمودن دفعاتی که فایل می‌تواند اجرا شود، ممانعت از اجرای فایل در یک دستگاه بدون مجوز، و نظارت بر روی عمل تأیید و تصدیق کاری که حین انتقال فایل‌های رسانه‌ای میان کامپیوتر و دستگاه قابل حمل انجام می‌گیرد، است.

مسئله بحث درخصوص مدیریت حقوق دیجیتال بر سر این است که بدون یک سیستم پر قدرت و مناسب برای اطمینان از این‌که فقط مصرف‌کنندگانی که هزینه پرداخت می‌کنند، می‌توانند به رسانه‌ها دسترسی پیدا کنند؛ تکثیر غیرقانونی رواج پیدا می‌کند و سود تولیدکنندگان و توزیع‌کنندگان را به‌طور چشمگیری کاهش می‌دهد. بنابراین با کاهش فروش، بحث‌ها ادامه پیدا می‌کند، ورودی ایجاد شده نیز کاهش یافته و کیفیت کلی رسانه‌های تولید شده تنزل خواهد یافت (۱۷).

ماهیت تجارت دیجیتال

مدیریت حقوق دیجیتال به مجموعه‌ای از فن‌آوری و روش‌هایی اشاره دارد که اطمینان را پایه‌ریزی کرده، و امنیت تجارت محتوایی دیجیتال را ممکن می‌سازد. برای پی بردن به نقش DRM در تجارت محتوایی، خوب است ابتدا یک معامله فروش جزئی از طریق اینترنت بررسی شود.

یک معامله تجاری را در نظر بگیرید که از طریق اینترنت انجام شده است. در یک معامله

6. Digital management of rights

۷. Peer-to-Peer. برای کسب اطلاعات بیشتر می‌توانید به سایت ذیل مراجعه نمایید: <http://dret.net/glossary/drm>

دیجیتالی خریدار و فروشنده آن‌طور که انتظار می‌رود فرسنگ‌ها از هم دور هستند و شاید در دو قاره متفاوت باشند. اطمینانی که ناشی از نزدیکی طرفین است، وجود ندارد. مشتری برای شروع یک معامله دیجیتالی به اینترنت وصل می‌شود تا وب را برای کتاب‌های الکترونیکی نگاه کند. (آیا او می‌تواند مطمئن باشد که فروشگاه‌های پیوسته اینترنتی که وی پیدا می‌کند واقعاً کتاب‌فروشی‌های قانونی بوده و سایت‌های واقعی تبهکاران نیستند؟) او از یکی از وب‌سایت‌هایی که می‌شناسد، یک کتاب الکترونیکی انتخاب کرده و یک نقد از آن کتاب را نگاه می‌کند. (آیا او می‌تواند مطمئن باشد که الگوهای بررسی او برای یک تحلیل نظام‌مند جمع‌آوری نمی‌شود و احتمالاً به شرکت‌های تحقیقاتی فروخته نمی‌شود؟) بعد از انتخاب یک کتاب الکترونیکی برای خرید، کتاب موردنظر در سبد خرید دیجیتالی گذاشته شده و به طرف صندوق دیجیتال می‌رود. (آیا خریدار می‌تواند مطمئن باشد محتوای دیجیتالی خریداری شده‌ او، معتبر است و مطالب ناب ناشر یا نویسنده اصلی کتاب است؟) او آماده می‌شود تا کتاب الکترونیکی را برای خواندن به (کامپیوتر خود) منتقل کند. (آیا او می‌تواند مطمئن باشد که که قالب محتوا برای مطالعه او مناسب است و این که وقتی کتاب را تمام کرد، آن را به دوست خود هدیه بدهد؟ و مهم اینکه، فروشنده کتاب، ناشر و مؤلف می‌توانند مطمئن باشند که خریدار یک نسخه دیجیتالی غیرمجاز از این کتاب دیجیتالی ایجاد نمی‌نماید و با استفاده از کپی از منابع

اینترنتی محتوای آن را در همه جا توزیع نمی‌کند؟)

پاسخ به بسیاری از این سؤالات بدون DRM، «منفی» است.

شرکای بازاری باید مطمئن شوند که مشتریان به روش خاص معامله می‌کنند و یا اینکه آن‌ها نمی‌خواهند در سود سهیم گردند. تأمین‌کنندگان محتوا باید مطمئن شوند که اگر محتوا را به بازار کتاب الکترونیکی واگذار کنند، حق‌الزحمه خود را به‌طور کامل دریافت می‌کنند. مشتریان باید مطمئن باشند که مطلب معتبر دریافت می‌کنند و اینکه تجربیات خرید و مطالعه آن‌ها مثبت خواهد بود و حریم خصوصی آن‌ها حفظ می‌شود. DRM با فراهم کردن بنیاد اطمینان بین تأمین‌کنندگان محتوا و کاربران، تجارت قوی محتوای دیجیتالی را ممکن می‌سازد (۱۵).

روند تکامل DRM

مدیریت حقوق دیجیتال از زمان ظهور اینترنت در پارادایم پژوهش موجود بوده است. به هر حال، مدل‌های تجاری و استفاده‌های جدید، تحقیقات DRM را به بعد متفاوتی هدایت می‌کند (۱۴: ۱۱۰-۱۱۱).

نسل اول مدیریت حقوق دیجیتال بر امنیت سطح پایین و رمزگذاری انتشار غیرقانونی، به وسیله قفل‌گذاری بر روی منابع و محدودیت در توزیع آن‌ها، تنها به وسیله پرداخت هزینه متمرکز بوده است.

نسل دوم DRM از دیدگاه عملی، امنیت جاری و رمزگذاری، دور شده و توانایی‌هایش را به موضوع مدیریت گسترش داده است (۱۲).

نسل سوم سیستم DRM، کاربرد جنبه‌های قانونی، فنی و اخلاقی را با هم ترکیب می‌کند تا به یک مدل تجاری منطقی و مناسب با توجه به نیازهای کاربر تبدیل شود. اجزای این تکنولوژی شامل رمزگذاری، انگشت‌نگاری، توسعه اجرای فرمان و مواردی از این قبیل است. بسته به محیط ویژه، راه‌حل‌های مدیریت حقوق دیجیتال احتمالاً متنوع است. به هر حال مهم است که بین امنیت، توافقات حقوقی و کارپسندی و سادگی راه‌حل‌های DRM تعادل خوبی برقرار شود (۱۰).

کاربرد DRM

مدیریت حقوق دیجیتال در رسانه‌های مختلفی کاربرد دارد، اما اغلب در فایل‌های موسیقی، فیلم‌ها و ویدئوهای الکترونیکی دیده می‌شود. اکثر فروشگاه‌های موسیقی اینترنتی برای محدود کردن کاربرد موسیقی خریداری شده و انتقال آن به صورت پیوسته، DRM را به کار می‌برند (۷)؛ که این مسئله هنرمندان موسیقی را قادر می‌سازد تا خود از نتیجه تلاش‌هایشان بهره‌مند گردند، به این شکل که اگر کاربری مثلاً یک دلار برای انتقال یک ترانه می‌پردازد، بخشی از آن به شرکت موسیقی مورد نظر و درصدی نیز به آن هنرمند تعلق می‌گیرد (۱۵). با این که مدیریت حقوق دیجیتال بیشتر در فیلم‌ها استفاده می‌شود، اما اکنون برای رسانه‌های دیگری نیز به صورت گسترده استفاده می‌گردد. طرح‌های مختلف DRM می‌تواند تعداد دستگاه‌هایی را که یک فایل شنیداری در آن‌ها مورد استفاده

قرار می‌دهند، محدود کند. بسیاری از تولیدکنندگان کتاب‌های الکترونیکی نیز از سیستمی مشابه مدیریت حقوق دیجیتال برای محدود کردن تعداد رایانه‌هایی که یک کتاب می‌تواند در آن دیده شود، استفاده می‌کنند و حتی از این طریق می‌توانند تعداد دفعات استفاده از آن را محدود کنند. مدیریت حقوق دیجیتال منافع زیادی برای نویسندگان، ناشران و خرده‌فروشان دارد. DRM، تجارت، قصد و درک استفاده کاربر را اصلاح می‌کند و امنیت، پیگیری، حمایت پیوسته محتویات دیجیتالی را فراهم نموده و پذیرش حقوق دیجیتال را تضمین می‌کند. DRM برای مشتریان، خدمات و تولیدات را بهبود می‌دهد؛ دسترسی به محتویات دیجیتالی با کیفیت عالی‌تر و تعداد زیادی از آثار دیجیتالی را فراهم می‌کند. مهارت و سهولت استفاده کاربر را گسترش می‌دهد و در زمان و هزینه صرفه‌جویی می‌کند. DRM برای اقتصاد و تجارت، الگوهای شغلی جدیدی ایجاد می‌کند. مدیریت حقوق دیجیتال بازدهی و قدرت تولید را افزایش می‌دهد. در اواسط سال ۲۰۰۵، تعدادی از تهیه‌کنندگان تلویزیون به تدریج متقاضی استفاده از سیستم‌های DRM برای نمایش خود شدند (۱۲). مدیریت حقوق دیجیتال در اینترنت متحرک^۸ نیز کاربرد دارد (۱۰).

DRM امکان تجارت دیجیتالی را فراهم می‌کند. مدیریت حقوق دیجیتال امتیازات مهمی را فراهم می‌کند که این امتیازات انجام تجارت

دیجیتالی را ممکن می‌سازند. بسیاری از این امتیازات رمزنویسی DRM^۹، از علم استفاده از ریاضیات برای رمزنویسی و رمزگشایی متن (و پیام‌های دیگر) به دست آمده است. همه این امتیازات معمولاً برای تأمین بنیاد اطمینان بین صاحب محتوای دیجیتالی و کاربر استفاده می‌شود. با کمک‌های DRM امکان انجام موارد زیر فراهم می‌شود:

- حمایت از محتوای دیجیتالی
- توزیع مطمئن محتوای دیجیتالی^{۱۰}
- صحت و اعتبار محتوای دیجیتالی
- عدم انکار معامله
- شناسایی شریک بازاری

DRM از محتویات دیجیتالی حمایت می‌کند.

DRM، با رمزنویسی کردن محتوا این امکان را برای صاحبان محتویات دیجیتالی از جمله مؤلفان و ناشران، فراهم می‌کند که مطلب دیجیتالی را به سرتاسر یک شبکه غیرقابل اعتماد، مانند اینترنت بفروستند تا کاربران موردنظر بتوانند از آن استفاده کنند. DRM، از یک برنامه کامپیوتری به نام الگوریتم رمز استفاده می‌کند تا محتویات دیجیتالی را رمزنویسی کند. الگوریتم رمز به یک کلید رمز - یک عبارت خاص یا یک سری شماره - نیاز دارد، تا مطلب را رمزنویسی کند که فقط دارندگان این کلید از محتویات موردنظر استفاده کنند. چون همه دارندگان کلید رمز می‌توانند به سهولت به مطلب

رمزی دسترسی پیدا کنند، کنترل کردن کامل کلیدهای رمز بسیار مهم است و بیشتر برنامه‌های DRM، مربوط به این مورد است. DRM، امکان توزیع محتویات را فراهم می‌کند به طوری که از طریق رمزنویسی DRM، محتوا حفظ می‌شود و بدون کلید رمز، فایل نامفهوم است. درست است که هر کسی می‌تواند به آن دسترسی پیدا کند، اما این کار بدون کلید رمزگشایی فایده است (۱۰).

DRM اعتبار محتوا را تضمین می‌کند.

تغییر دادن محتویات دیجیتالی اصل، و قالب کردن آن به مشتریان ناآگاه به عنوان اصل، آسان است. اما DRM می‌تواند با استفاده از یک تکنیک ریاضی با نام تابع درهم‌ساز یک طرفه، محتویات دیجیتالی را از دخل و تصرف دیجیتالی حفظ نماید (۱۰).

DRM عدم انکار معامله را تأمین می‌کند.

در بازار الکترونیکی و دنیای واقعی، این مطلب حائز اهمیت است که شرکا بتوانند ثابت کنند که معامله موردنظر، واقعاً صورت گرفته است. رسید فروش یا قبض امضا شده برای استفاده از کارت اعتباری به عنوان مدرک فروش عمل می‌کند. بازارهای الکترونیکی باعث کاربرد وسیع معاملات با کارت اعتباری می‌شوند، اما باید به مشکل امضا کردن این قبض توجه داشته باشند. معادل امضای دیجیتالی ضروری است. یک امضای دیجیتالی را زمانی

۹. امنیت اطلاعات موضوعی چند بُعدی است که با جنبه‌های غیرفنی متعددی ارتباط دارد. همواره برای تحقق امنیت، ابزارهای فیزیکی، پرسنلی و اجرایی لازمند و ابزارهای فنی به تنهایی بی‌فایده‌اند. اما وقتی که در یک شبکه نامطمئن کار می‌کنید، امنیت بدون استفاده از رمزنگاری میسر نمی‌شود (۱).

۱۰. این کاربرد به طور ضمنی در بخش ماهیت تجارت دیجیتالی بحث شد؛ از پرداختن مجدد به آن خودداری می‌شود.

می‌توان ایجاد کرد که شریک معامله از کلید رمز خود برای رمزنویسی بخشی از اطلاعات مربوط به معامله استفاده کند. فقط از همین کلید رمز می‌توان برای رمزگشایی اطلاعات استفاده کرد. مادامی که کلید رمز مخفی است فقط صاحب اصلی رمز می‌تواند معامله را رمزنویسی کند. در عمل دو کلید رمزی مورد استفاده قرار می‌گیرند، یک رمز خصوصی و یک رمز عمومی. شریک معامله، مالک کلید رمز خصوصی است و آن را مخفی نگه می‌دارد. یک شریک وقتی معامله را با کلید رمز خصوصی خود رمزگشایی می‌کند، معامله امضا می‌شود. هر کس که علاقه‌مند به تغییر اعتبار معامله است می‌تواند کلید رمز عمومی شریک را به دست آورده و سعی کند امضا را رمزگشایی کند. اگر عمل رمزگشایی با موفقیت صورت گیرد شرکای بازاری مطمئن می‌شوند که دارنده رمز خصوصی در معامله اصلی شرکت کرده است (۱۰).

DRM از اوراق هویت شریک حمایت می‌کند.

در دنیای واقعی تعیین هویت شرکت‌کنندگان در معامله بسیار آسان است. اگر شکمی در مورد هویت وجود دارد، معمولاً با بررسی سریع در برگه هویت مشتری این مشکل حل می‌شود. البته در تجارت اینترنتی این امر آن قدر ساده نیست. هر کسی می‌تواند بدون مشکل زیاد یک وبسایت ایجاد کند که کاملاً قانونی به نظر برسد. بیشتر این وبسایت‌ها قانونی و بعضی غیر قانونی هستند. DRM، امکان شناسایی

شرکای بازاری را با استفاده از گواهی‌نامه دیجیتال فراهم می‌کند. یک گواهی دیجیتال، مانند شناسنامه یا شماره تأمین اجتماعی عمل می‌کند. گواهی‌نامه دیجیتال با استفاده از یک تکنیک رمزی ایجاد می‌شود که هویت شخص را با کلید رمز خصوصی و عمومی وی ربط می‌دهد؛ این گواهی‌نامه با ترکیب کلید رمز عمومی فرد، دیگر اطلاعات مربوط به هویت و یک یا چند امضای دیجیتال بوجود می‌آید. امضاهای دیجیتال متعلق به مراجع مطمئن صدور گواهی‌نامه است و مؤید این مطلب است که کلید رمز عمومی در واقع به شخصی که گواهی‌نامه به نام او است، تعلق دارد (۱۰). با وجود قابلیت‌های مفید DRM مهم است که با محدودیت‌های فن‌آوری و نیاز به چشم‌اندازی گسترده‌تر در حمایت محتوایی دیجیتال آشنا شویم؛ در بخش بعدی چشم‌اندازهای گسترده‌تر که لازمه حمایت محتوای دیجیتال است، ارائه می‌گردد.

چشم‌اندازهای چندجانبه DRM، که لازمه حمایت آن است.

استفاده‌کنندگان DRM نباید انتظار داشته باشند که فن‌آوری مدیریت حقوق دیجیتال، یا در واقع استانداردهای فنی آن، محتوای دیجیتال آن‌ها را کاملاً تضمین کند. برای بهینه‌سازی حمایت، باید از چشم‌انداز وسیع‌تری، DRM بررسی گردد؛ نه این‌که فقط از چشم‌انداز فن‌آوری به آن پرداخت.

قالب کتاب الکترونیکی باز^{۱۱}، و سازمان استانداردهای مهم کتاب الکترونیکی، پیشنهاد

11. Open eBook forum

می‌کنند که DRM از سه جنبه بررسی شود. جنبه فنی، اجتماعی و قانونی. جنبه فنی شامل زبان تصریح حقوقی، کنترل بسته‌های الکترونیکی و زیرساخت اطمینان است. جنبه اجتماعی شامل انتظارات، آداب و رسوم و آموزش است و جنبه قانونی شامل قانون‌گذاری، اطاعت، رسیدگی و اجراست. هر یک از این جنبه‌های DRM به‌طور خلاصه در ذیل ارائه می‌گردد (۷).

جنبه فنی DRM

این جنبه شامل سخت‌افزار و نرم‌افزارهایی است که برای امنیت محتوای دیجیتال استفاده می‌شود. بیشتر مردم، وقتی درباره‌ی DRM صحبت می‌کنند، جنبه فنی را مورد توجه قرار می‌دهند که شامل تعدادی از عناصر است که اغلب به صورت ترکیبی استفاده می‌شوند تا محتوا را حفاظت نمایند. بیشتر این عناصر بر مبنای ریاضیات رمزنویسی است که شامل موارد زیر است:

رمزنویسی؛ کلید رمزهای خصوصی / عمومی؛ گواهی‌نامه‌های دیجیتال؛ بررسی دستیابی؛ بررسی نقش‌های دیجیتال؛ تأیید (به)؛ پروتکل‌های ارتباطات مطمئن؛ امنیت ذخیره محتوا؛ زبان تصریح حقوق؛ زیرساخت اطمینان (۷).

جنبه قانونی DRM

همان‌طور که از عنوان «مدیریت حقوق دیجیتال» برمی‌آید، به محدودیت قانونی اشاره دارد. هر بخش در مورد مدیریت حقوق دیجیتال به طرز غیرقابل تفکیک با قانون مرتبط است. بحث قوانین مرتبط با حقوق از

محدوده این مقاله خارج است. جنبه قانونی شامل موارد زیر است:

قانون‌گذاری؛ اطاعت (از قانون)؛ رسیدگی؛ اجرای (قانون).

یکی از فن‌آوری‌های مربوط به DRM از دیدگاه قانونی، نقش‌های دیجیتالی است. نقش‌های دیجیتالی از نظر مفهومی، مشابه انواع قدیمی و سنتی آن است که با استفاده از کاغذ انجام می‌شد. به هر حال نقش‌های دیجیتالی برخلاف مشابه کاغذی آن‌ها، اغلب از یک سری بیت‌های دیجیتالی نامرئی تشکیل شده که این بیت‌ها در یک سند یا نسخه دوم پنهان هستند. بیت‌های نقش‌های دیجیتالی را می‌توان به‌گونه‌ای ایجاد کرد تا اطلاعات تعیین‌کننده هویت، مانند ناشر اصلی یا حتی نام یا شماره کارت اعتباری خریدار، در آن گنجانده شود. ممکن است نقش‌های دیجیتالی برای افراد قابل رؤیت نباشد؛ اما می‌توان آن‌ها را با نرم‌افزار خاصی به راحتی خواند که در این مقاله به آن پرداخته نمی‌شود.

فن‌آوری ایجاد نقش دیجیتالی از توزیع غیرقانونی منابع فکری جلوگیری نمی‌کند، اما امکان تشخیص کپی‌برداری‌های غیرقانونی را فراهم می‌سازد. بنابراین، اطاعت از قانون، رسیدگی و اجرای قانون‌گذاری فعلی را ممکن می‌سازد. رمزنویسی DRM و حتی نقش‌های دیجیتال نمی‌تواند امنیت محتوای دیجیتال را کاملاً تضمین کند. یک هکر با انگیزه، زمان و پول کافی و امکانات مالی دیگری که در اختیار دارد، می‌تواند بیشتر طرح‌های رمزی، اگر نه همه آن‌ها را، نابود کند. بسیاری از مجریان DRM که با آن‌ها مصاحبه شده

است، اظهار کرده‌اند که بهترین عملی که DRM می‌تواند انجام دهد این است که به صادق ماندن افراد صادق کمک کند (۷).

جنبه اجتماعی DRM

از نظر فنی این امکان برای مشتریان وجود دارد که نسخه‌هایی با کیفیت بالا، از آثار دارای حقوق انحصاری به دست آورند، بدون اینکه دارندگان حق انحصاری را از نظر مالی تأمین کنند، اما این کار غیرقانونی است. انتقال یک برنامه به معنای انتقال رایگان نیست و هنوز هم بسیاری از مشتریان نمی‌توانند بین این دو مورد تمایز قائل شوند. برخی نمی‌دانند که تمایزی بین آن‌ها وجود دارد و برخی نیز آن را نادیده می‌گیرند.

ناشران، سازمان‌های تجاری و شرکت‌های فن‌آوری باید همکاری داشته باشند تا به مشتریان راجع به مسائل مربوط به تکثیر غیرقانونی آموزش دهند. تلاش مشترک انجمن ناشران آمریکا (AAP) و شرکت مایکروسافت، نمونه خوبی از این همکاری‌هاست.

مشتریانی که با خطرهای تکثیر غیرقانونی محتوای الکترونیکی آشنا هستند، به احتمال قوی‌تر محتوا را از منابع قانونی به دست می‌آورند (۷).

معماری اصلی DRM

چارچوب مدیریت حقوق دیجیتال منطبق بر سیستم‌های حقوقی دیجیتالی می‌تواند در سه شاخه ذیل ارائه گردد:

● مالکیت هوشمند، ذخیره و خلق دارایی. چگونگی اداره خلق محتویات به‌گونه‌ای

که به آسانی مبادله شود. این مسئله شامل قوانین حمایتی می‌گردد وقتی که محتویات دیجیتالی برای اولین بار توسط تولیدکنندگان، خالقان مختلف محتویات دیجیتالی خلق می‌شوند.

● مدیریت مالکیت هوشمند سرمایه. چگونگی اداره و توانایی تجارت محتویات دیجیتالی. این مسئله شامل پذیرش محتویات از خالقان به سیستم مدیریت دارایی می‌شود. سیستم‌های تجاری نیاز به اداره ابر داده‌های توصیفی و ابر داده‌های حقوقی دارند.

● کاربرد مالکیت هوشمند سرمایه. چگونگی اداره، استفاده از محتویات، زمانی که تجارت شده‌اند؛ و شامل ممانعت‌های حمایتی از محتویات تجارت شده در نرم‌افزار/سیستم‌های نمایش خاص می‌شود.

مدل‌های بالا نواحی وسیعی که برای DRM نیاز است، دربرمی‌گیرد. این مدل‌ها نیاز دارند تا با معماری اساسی کامل شوند و چارچوبی برای طرح‌ها تهیه کنند تا عاملیت مدیریت حقوق دیجیتال اجرا شود (۶).

مؤلفه‌های مطرح DRM

سه مؤلفه مطرح هسته در مدیریت حقوق دیجیتال وجود دارد: کاربران، محتویات دیجیتالی و حقوق. «کاربران» می‌توانند هر نوعی از استفاده‌کننده مثل ناشران، شرکت‌های ثبت شده، استودیوهای فیلم، استفاده‌کننده نهایی و غیره باشند. این مؤلفه، محتویات دیجیتالی را خلق می‌کند و از آن استفاده می‌کند. «محتویات دیجیتالی»، می‌تواند هر نوعی از محتویات در هر سطحی باشد. «حقوق»، مجوزها،

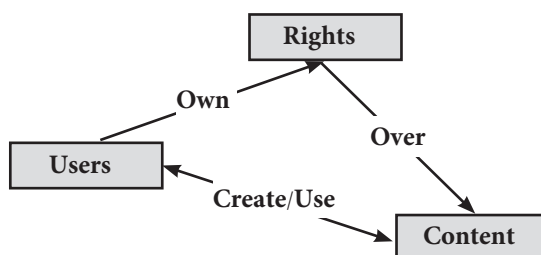
محدودیت‌ها و قید و بندهای محتویات دیجیتالی است که کاربران را می‌پذیرد. موجودیت حقوق، اصولی را برای مجوزها، محدودیت‌ها، قیدوبندها، و دیگر اطلاعات مرتبط حقوقی دربارهٔ کاربران و محتویات دیجیتالی می‌پذیرد. اصول حقوقی می‌توانند به سرعت تا حدودی پیچیده گردند. مدل حقوقی در مدیریت حقوق دیجیتال تعاریف متعددی را نیز دربرمی‌گیرد که در اینجا به مهم‌ترین تعاریف مربوط به آن اکتفا می‌شود:

• **اجازه.** آنچه که شما، مجاز به انجام آن هستید،

• **قید و بندها.** محدودیت در مورد اجازه،
• **تعهدات.** آنچه که باید انجام دهید،
فراهم کنید، بپذیرید،

• **دارندگان حقوق.** کسی که در مورد چیزی ذی‌حق است (۶).

به دلیل اینکه این مبحث موردنظر نگارنده نیست، از پرداختن بیشتر به آن خودداری می‌شود. روابط بین سه مؤلفهٔ مدیریت حقوق دیجیتال در نمودار ۱ نشان داده شده است (۱۲).



نمودار ۱. مؤلفه‌های هستهٔ مطرح (DRM) و روابط آن‌ها

محدودهٔ مرکزی برای ایجاد یک سیستم DRM کاری، ترکیب مدل حقوق، مدیریت حقوق و ابزار است. مدل حقوق را باید کاملاً شناخت تا بتوان مدیریت حقوق را در بالای آن بنا کرد. ابزار را باید مورد بررسی قرار داد و به دقت طراحی کنند تا مدیریت حقوق اجرا شود. ابزار را می‌توان به دو دستهٔ ابزار قانونی و تکنیکی تقسیم‌بندی کرد.

ابزار قانونی مجموعه ابزاری است که یک سیستم قانونی مقرر می‌کند تا از حقوق قانونی یک فرد حمایت کند. این ابزار شامل اجرای قانون، دادخواهی، داوری و اجرای قوانین دادگاه و غیره است. ابزار تکنیکی (فنی) برای اجرای DRM در نظر گرفته می‌شوند و برخی از آن‌ها مهم تلقی می‌گردند (۱۲). توضیحات بیشتر دربارهٔ این موضوع در این مقاله مطرح نمی‌شود.

ویژگی‌های مدیریت حقوق دیجیتال

• **اعمال و صلاح سیاست‌های مدیریت حقوق.** یک شخص (حقیقی یا حقوقی) باید فعالیت در زمینهٔ چگونگی اجرای حقوق خود در تولیدات اطلاعات را به عنوان بخشی از استراتژی مدیریت منابع فکری تعریف کرده و دائماً آن را بهبود بخشد.

• **انعقاد و اجرای توافق‌نامه‌ها.** DRM باید توافق‌نامه‌هایی در مورد حقوق در تولیدات اطلاعاتی منعقد کند و مدیریت قرارداد را با آن توافق‌نامه‌ها مرتبط سازد.

• **مدیریت اطلاعات مربوط به حقوق حاصل شده.** وقتی بعضی حقوق از شرکت‌های دیگر اعطا می‌شوند دانستن این

فعالیت یکپارچه برای تأمین‌کنندگان محتوا و کاربران ایجاد شود. بنابراین حصول اطمینان از عمل‌پذیری متقابل و مناسب سیستم‌های DRM حائز اهمیت است. نخستین گام مفید برای استاندارد کردن DRM زبان حقوق دیجیتال است (۱۲).

سازمان‌های درگیر در استانداردسازی DRM

مدیریت حقوق دیجیتال فضای فنی گسترده‌ای را دربرمی‌گیرد. استانداردسازی آن، اکنون در تعدادی از سازمان‌های باز صورت می‌گیرد. فعالیت چندین کنسرسیوم میزبان در این زمینه مؤثر است. به عنوان مثال حمایت و مدیریت منابع فکری^{۱۲}؛ برنامه‌های توصیفی چندرسانه‌ای^{۱۳} MPEG7، نظام‌های لایه‌ای، توصیف و تعریف مواد دیجیتال- MPEG-21، W3C: RDF، DAML، امضاها: W3C: XML، پروتکل XML، پنهان کردن XML و طرح‌های دیگر «وب معنایی»^{۱۴}، قالب کتاب الکترونیکی باز فعالیت WBX قبلی بر روی زیرساخت اطمینان و «حقوق و قوانین WG» فعلی. اما هیچ کدام از این فعالیت‌ها مشکل استانداردسازی و عمل‌پذیری مدیریت حقوق دیجیتال را حل نمی‌کنند؛ مخصوصاً این که هیچ‌کدام این موارد به آنچه که به عنوان گام نخست و اصلی وب در نظر می‌گیریم، یعنی بیان ساده و ارتباط سیاست‌ها و اطلاعات IPR نمی‌پردازند. ODRL، XrML و XML در این زمینه تلاشی انجام داده‌اند (۱۲).

مطلب حائز اهمیت است که این حقوق از چه شرکتی گرفته شده، محدوده آن‌ها چقدر است، چه مقدار و چه زمانی شرکت دارای آن حقوق باید مبالغی پرداخت کند و غیره.

• **کنترل و اجرای مجوزها.** در بیشتر موارد، تجارت معقول مستلزم این است که یک شرکت امتیاز بعضی حقوق را به شرکت‌های دیگر اعطا کند. بنابراین لازم است که شرکت بتواند بر آنچه دیگران تولید می‌کنند نظارت کند و شرایط توافق‌نامهٔ مربوط به مجوز را در صورت لزوم اجرا نماید.

• **حمایت از بازاریابی.** فعالیت‌های DRM باید انعطاف‌پذیری کافی داشته باشند تا از هر روشی که شرکت به استفاده از آن مصمم است، حمایت کند.

• **حمایت از وصول درآمد و سهام.** DRM باید روشی مقرر کند تا بتواند درآمدهای کاربران اطلاعات در شرکت‌های تجاری را وصول، محاسبه و تقسیم کند.

• **خطرپذیری (ریسک) در مدیریت.** خطرهای مربوط به DRM، زیان‌های احتمالی مربوط به اطلاعات دیجیتال در آینده است. بنابراین بهتر است این خطرها از قبل مهار شود (۱۲).

استانداردسازی

اکنون، صنعت محتوای الکترونیکی با یک مانع جدی مواجه شده است، فقدان استانداردهایی که براساس آن‌ها این امکان برای سیستم‌های کاربران فراهم شود تا با هم کار کنند و یک

12. Intellectual Property Management and Protection (IPMP)

13. Multimedia Description Schemes

14. Semantic web

XrML (زبان نشانه‌گذاری صحیح و قابل گسترش) و DRM

XrML^{۱۵} یک زبان در XML^{۱۶} (زبان نشانه‌گذاری گسترش‌پذیر) است که برای توصیف خصوصیات حقوق، هزینه‌های پرداختی و شرایط استفاده از محتواهای دیجیتال به همراه ادغام پیام و اعتبار شرکت استفاده می‌شود. مدارک XrML مطابق XML است؛ بنابراین آن‌ها با ابزار استاندارد XML، به عنوان مثال XML SPY، به آسانی مشاهده، ویرایش و تأیید می‌شوند. هدف حمایت از تجارت با محتواهای دیجیتال و همچنین حمایت از خصوصیات دستیابی و نظارت‌های کاربردی برای تأمین مدارک دیجیتال در مواردی است که مبادله بخشی از شرایط کاربرد منظور نمی‌شود. به علاوه، XrML از استاندارد صنعتی دیگری، مانند SSL، رمزگذاری کلید عمومی - خصوصی و ابتکار DOI، حمایت کرده و با این استاندارد مطابقت دارد.

XrML به شرح حقوق، هزینه‌ها و شرایط مناسب مدل‌های تجاری می‌پردازد که آن‌ها انتخاب می‌کنند، شرایط استاندارد برای حقوق کاربران با مطالب مفید، مختصر و کاملاً قابل فهم، مقرر می‌کند؛ تعاریف عملیاتی از سیستم‌های مطمئن برای آزمون پذیرش و ارزیابی به فروشندگان ارائه می‌دهد، قابلیت

گسترش ویژگی‌های جدید زبانی را فراهم می‌کند، بدون اینکه دیگر اهداف XrML به مخاطره بیفتد. معماری باز، قابلیت اندازه‌گیری، سفارشی کردن، قابلیت گسترش یافتن و توانایی ادغام با سیستم‌های فعلی و سیستم‌های جدیدی را که به وجود می‌آیند، تأمین می‌کند (۱۲).

دیگر زبان‌های مهم DRM

ODRL^{۱۷} (زبان حقوق دیجیتال باز) و XMCL^{۱۸} (زبان تجاری رسانه‌ای قابل گسترش) دو زبان دیگر از زبان‌های مهم مدیریت حقوق دیجیتال هستند که علاوه بر XrML آن‌ها نیز در حال گسترش هستند.

زبان حقوق دیجیتال باز (ODRL) که برای زبان توصیفی مدیریت حقوق دیجیتال معنا ارائه می‌دهد و فرهنگ داده‌های مربوط به همه اشکال محتوای دیجیتال است. ODRL یک لغت برای بیان شرایط و موقعیت‌ها از طریق محتوای دیجیتال است که شامل اجازه، قیدوبندها، تعهدات و انعقاد توافق‌نامه‌ها با دارندگان حقوق است. امکان گسترش ODRL به وسیله بخش‌های مختلف صنعتی (به عنوان مثال کتاب‌های الکترونیکی، موسیقی، وسیله سمعی و شنیداری موبایل و نرم‌افزار) وجود دارد و می‌تواند به عنوان یک زبان مقیم تعامل‌پذیر بوده و هیچ نیازی به

15. eXtensible Rights Markup Language(XrML)

16. eXtensible Markup Language(XML)

برای کسب اطلاعات بیشتر در مورد XML می‌توانید به این منبع مراجعه نمایید: لیلیا خلیلی. مترجم، «مقدمه‌ای بر اکس. ال. ام XML»، *مجله الکترونیکی نما*، دوره چهارم، ۴ (مرداد ۱۳۸۴). [قابل دسترسی در]: http://www.irandoc.ac.ir/data/E_J/vol4/khalili_abs.htm

17. Open Digital Rights Languages(ODRL)

18. Extensible Media Commerce Language(XMCL)

مجوز نداشته باشد.

XMCL در ۲۰ ژوئن سال ۲۰۰۱ توسط Real Network و تعداد زیادی از مدیران صنایع ارائه شد. XMCL یک زبان بر پایه XML است که برای ایجاد استانداردهایی برای تجارت اینترنتی رسانه‌ها در تمام بخش‌های صنعت طراحی شده است. با استانداردسازی زبان برای قوانین تجاری، XMCL این امکان را فراهم می‌کند که مدیریت محتوا به نحوی باشد که به کدک‌ها، سیستم‌های مدیریت حقوق دیجیتال و سیستم‌های تجاری وابسته نباشد. XMCL آماده‌سازی را بسیار ساده می‌کند و بازار را برای تجارت رسانه‌ها از طریق اینترنت بهبود می‌بخشد. هدف Real Network تسلیم پیشنهاد XMCL به سازمان استانداردهای مقتضی است. این شبکه‌ها با دیگر مدیران صنایع کار می‌کنند تا اطمینان حاصل کنند که ابداعات به یک استاندارد همگانی قابل قبول تبدیل می‌شوند. خیلی زود است که گفته شود کدام زبان در آینده زبان استاندارد DRM خواهد بود. اما بدون شک این زبان‌ها در استانداردسازی زبان DRM سهیم هستند و باعث رشد سریع اقتصاد محتوای دیجیتالی می‌شوند (۱۲).

امنیت DRM

مدیریت حقوق دیجیتال به یک زیرساخت مطمئن نیاز دارد. زبان حقوق و مدل معماری باید بتوانند با سیستم‌های مهمی که در محل دیگر توسعه یافته‌اند، مرتبط شوند. خلاصه‌ای از برخی از نگرانی‌ها در مورد زیرساخت اطمینان از کارگاه w3c عبارتند از:

این «زیرساخت اطمینان» چگونه است؟؛ مدیریت آن به عهده کیست؟؛ چگونه دارای ویژگی عمل‌پذیری متقابل خواهد بود؟؛ مسائل اجتماعی / قانونی (به عنوان مثال مسئولیت) چه هستند؟؛ چگونه با اجزای مورد اطمینان ارتباط دارد (سخت‌افزار و نرم‌افزار)؟ تجارت الکترونیکی و همه انواع خدمات در دنیای دیجیتال مبتنی بر ساخت‌های اطمینان است. ساخت‌های اطمینان در واقع آن قدر مهم هستند که باید خارج از فعالیت مدیریت حقوق دیجیتال در نظر گرفته شوند. توضیحات بیشتر در این باره، در این مقاله بحث و بررسی نمی‌شود (۱۲).

نمونه‌هایی از اجرای سیستم DRM

در حال حاضر، در بازار سیستم‌های DRM، خدمات و تصمیماتی در مورد برنامه‌های مختلف وجود دارد که هدفشان گسترش محتوای دیجیتالی و مدیریت حقوق آنهاست. فعال‌ترین این سیستم‌ها به وسیله شرکت‌های Adobe Systems-Glass book-Soft lock -Inter Trust- Content Guard و غیره توسعه یافته است.

Adobe Systems یک تکنولوژی خاص به نام Web Buy و Merchant PDF برای فروش انتشارات الکترونیکی در خدمت قالب PDF ایجاد کرده است.

Glass book, Soft lock تصمیمات خود را در مورد نظارت بر محتوای الکترونیکی و حقوق آن توسعه داده است. گروه تولید آن، شامل Glass book Reader/Glass book Content Server سیستم فروش اسناد

الکترونیکی شبکه در تجارت الکترونیکی با قالب PDF است.

Content Guard در آوریل سال ۲۰۰۰ توسط شرکت‌های زیراکس و مایکروسافت بر مبنای زیرشاخه گروه مدیریت حقوق زیراکس پایه‌ریزی شد. این سیستم برای توسعه یک سیستم DRM ایجاد شد که بتواند انواع گسترده محتوای دیجیتالی را از قبیل، کتاب‌های الکترونیکی، ویدئو و وسیله صوتی دیجیتالی، کنترل کند (۱۲).

اگر چه تعداد بی‌شماری از شرکت‌ها در ایجاد فن‌آوری DRM نقش داشته‌اند، اما دو شرکت در میان آن‌ها نقش مهم و برجسته‌ای در بازار DRM دارند: شرکت‌های Audio و Microsoft Liquid.

شرکت مایکروسافت تمام تلاش خود را صرف طراحی و توسعه بخش‌های زیرساختاری مدیریت حقوق دیجیتال که در محصولات نرم‌افزاری شرکت‌های دیگر قابل استفاده باشند، نموده است (۳).

فرصت‌ها و چالش‌های مطرح مدیریت حقوق دیجیتال

تکنولوژی‌های مدیریت حقوق دیجیتال ممکن است که خبر خوبی برای مالکان محتویات دیجیتالی، شرکت‌ها، استودیوهای فیلم، سازمان‌های جدید یا انتشارات پیوسته (online) باشد، اما پی‌آمد قطعی اجرای تکنولوژی‌های مدیریت حقوق دیجیتال محدودیت‌های غیرضروری و گرفتاری‌هایی برای کاربران رسانه‌های دیجیتالی و شبکه

است (۱۸). یک نمونه از آن، استفاده از DVD کدگذاری شده منطقه‌ای است. به‌طور مثال اگر فردی یک DVD از اروپا بخرد، نمی‌تواند آن DVD را مثلاً در کانادا حتی بر روی سیستم خود استفاده نماید (۱۷).

اگر چه تولیدکنندگان (DRM) امکانات محصولاتی را اصلاح نموده‌اند، ولی رابط‌های کاربر آن‌ها هنوز کامل نیست. مثلاً ممکن است، کاربر سعی نماید تا ترانه‌ای را پخش کند، برای اینکه مطمئن شود بر روی یکی از PD های او قرار گرفته، اما نمی‌داند روی کدام یک از PD ها قرار دارد (۴).

استدلال طرفداران آزادی‌های مدنی این است که استفاده از تکنولوژی دیجیتالی باید بدون قیدوبند باشد و انتقال حق نظارت به تولیدکنندگان حتی پس از فروش، در نهایت به بیان خلاق، زیان رسانده و باعث تضییع حقوق مصرف‌کننده می‌شود. بیشتر رسانه‌ها به وسیله حق انحصاری حمایت می‌شوند، اما شرطی برای استفاده منصفانه وجود دارد که استفاده بدون قیدوبند در بعضی شرایط را مجاز می‌داند. هیچ‌کدام از تکنولوژی‌های مدیریت حقوق دیجیتال فعلی نمی‌توانند امتیاز کافی برای استفاده منصفانه به‌دست آورند. این امر باعث می‌شود که بسیاری از طرفداران مدنی این‌گونه استدلال کنند که آن‌ها استفاده قانونی از محتوا را محدود کرده‌اند (۱۶).

منتقدان این قانون معتقدند که اجرای نظام DRM که با تغییر ساختارهای رایانه‌ای همراه خواهد بود، امکان نظارت تمام و کمال بر

۱۹. خوشبختانه Audio Liquid قول داده است که این مسئله را در محصول بعدی خود یعنی Net DRM در نظر بگیرد (۳).

شبکه را فراهم کرده و آزادی کاربران را سلب خواهد کرد.

هنگامی که کالایی تحت حمایت قانون کپی رایت فروخته می‌شود، مؤلف آن هیچ‌گونه کنترلی بر روی چگونگی به‌کارگیری محتویات، نخواهد داشت. اما همان‌طور که اشاره شد، سیستم‌های مدیریت حقوق دیجیتال به مالکان برنامه‌ها اجازه می‌دهد تا این قانون را از طریق محدود نمودن برنامه‌های اجراکننده یک فایل با محدود نمودن نسخه‌های پشتیبان، نقض کنند. علاوه بر این هنگامی که فن‌آوری DRM فراگیر گردد، مالکان محتویات می‌توانند جلوی کاربر را بگیرند تا نتواند تراک‌هایی را از CD مورد علاقه خود برداشته و بر روی یک CD فایل ضبط (جهت استفاده‌های شخصی) کپی کند.

پردرسترین مورد حالتی است که خطرات برخی سوءاستفاده‌ها از اطلاعات شخصی توسط مدیریت حقوق دیجیتال به نمایش گذاشته می‌شوند. زیرا سیستم‌های DRM، به‌طور ضمنی با اولویت‌های افراد آشنا می‌شوند، تولیدکنندگانی که به اصول اخلاقی پایبند نیستند می‌توانند این اطلاعات را به‌دست آورده و از آن برای تخریب فرد استفاده نموده و یا حتی این اطلاعات را به فروش برسانند^{۲۰} (۳).

ویلیام بوش از شرکت دیجیتال ورلد سرویس، یکی از بنیان‌گذاران طرح «جعبه کلید» در دفاع از طرح خود می‌گوید که

اطلاعات موجود در این زمینه کاملاً ناشناس خواهند ماند و هیچ‌کس نمی‌تواند آن را به فرد دیگری واگذار کند. با وجود این بسیاری از منتقدان معتقدند که جمع‌آوری اطلاعات دیجیتال مصرف‌کنندگان و ذخیره‌سازی این اطلاعات در مرکز مشخص، امنیت آن‌ها را به خطر می‌اندازد. در این خصوص گفته می‌شود که طرح DRM نمی‌خواهد تا آن حد پیش برود که در پایان هیچ نقطه امنی برای کاربران باقی نماند و اصطلاحاً همه تبدیل به کاربران شیشه‌ای شوند (۴).

کارشناسان بر این باورند که هیچ سیستمی اعم از مدیریت حقوق دیجیتال و یا دیگر سیستم‌های محافظتی را نمی‌توان برای همیشه از گزند هکرها دور نگه داشت و به محض ورود یک هکر به سیستم دفاعی موردنظر در اصل‌گویی درهای تمام جهان به روی آن گشوده شده است (۴).

سازمان‌ها و افراد برجسته و مهندسان کامپیوتر زیادی تقریباً با قالب‌های پیشنهادی جاری مختلف DRM مخالف هستند. دو مخالف برجسته DRM عبارتند از: جان والکر و ریچارد استالمن^{۲۱} (۸).

منتقدان طرح‌های جدید از جمله جنبش جدیدی که هدفش «نجات دادن نسخه‌برداری شخصی از آثار هنری است» نگران آن هستند که سیستم‌های جدید در دفاع به حق خود از حقوق صاحبان آثار هنری زیاده‌روی کرده و به دیگر ارزش‌های اجتماعی لطمه بزنند. زیرا

۲۰. به نظر می‌رسد که تولیدکنندگان (DRM) و سازمان‌های مربوط به آن از این مطالب چشم‌پوشی نموده‌اند؛ چرا که برای ارائه محتویات محرمانه دیجیتال عجله کرده‌اند (۳).

21. John Walkler & Richard Stallman

وقتی قرار باشد سیستم DRM حتی آخرین کپی از یک موسیقی را که یک دانش‌آموز دبیرستانی برای هم‌کلاسی‌اش تهیه می‌کند، زیر نظر بگیرد (۴) و حتی کپی‌برداری از ویرایش‌های کتاب الکترونیکی که یک اثر عمومی است، نیز امکان‌پذیر نکند (۱۷). در آن صورت، جنگل پر از خلاقیت اینترنت بی‌شک به یک پارک تفریحی یکنواخت و دلسردکننده تبدیل خواهد شد.

جان پری بارلو^{۲۲}، می‌گوید: «من به هوش و خلاقیت مشترک انسان‌ها- و اینترنت به عنوان ابزاری برای بروز آن- به چشم یک چرخه زیست محیطی می‌نگرم و معتقدم در حال حاضر صاحبان صنایع با طرح‌ها و اهداف خود می‌خواهند جنگل طبیعی اندیشه‌های بشری را خالی از درخت کنند» (۴).

البته بارلو راه‌حل مناسبی برای این مشکل سراغ ندارد، اما معتقد است که به عنوان مثال می‌توان از سیستمی استفاده کرد که به‌طور ماهیانه مبالغی ثابت را از کاربران اینترنتی دریافت کرده و مبالغ جمع‌آوری شده را با توجه به تعداد موسیقی‌های بارگیری شده (Download) از هر هنرمند، میان آن‌ها تقسیم کرد (۴).

البته مشکلات مدیریت حقوق دیجیتال تنها به این مسائل منتهی نمی‌شود. DRM، در کشورهای توسعه‌یافته و در کشورهای در حال توسعه مسائل مختلفی را مطرح می‌کند. مثلاً DRM خطرهای بزرگی را برای پیشرفت

و پایداری دنیای توسعه‌یافته عرضه کرده است. خطرهای DRM در مورد کشورهای در حال توسعه بیشتر نیز هست، چرا که علاوه بر این که خطرهای کشورهای توسعه‌یافته در این کشورها صادق است، همین‌طور خطر تحلیل رفتن فرهنگ و و پیشرفت نیز در این کشورها به همراه دیگر مشکل‌های خاص آن‌ها نیز مطرح می‌شود (۹).

کری راسل^{۲۳} متخصص کپی‌رایت انجمن کتابخانه آمریکا با برخی از راه‌حل‌های DRM که تهدیدی برای کاهش عاملیت کاربر و تجهیزات الکترونیکی کتابخانه است، مخالف است (۱۵). هنوز به هیچ‌وجه مشخص نیست که آیا طرح سیستم نظارت بی‌قید و شرط بر روند تبادل اطلاعات در اینترنت در آینده به مورد اجرا گذاشته خواهد شد یا خیر. شاید آزادی‌های بی‌قید و شرط کنونی و رشد بی‌هرج و مرج اینترنت در آینده چنان اخلاقیات را تحت تأثیر قرار دهد که مصرف‌کنندگان حاضر نباشند به راحتی تن به استفاده از رایانه‌های قابل کنترل بدهند. به راستی آیا نظام اخلاقی در اینترنت آن‌قدر افول یافته که در آن همه کاربران به راه‌زنان اطلاعاتی تبدیل شده‌اند؟ به سودجویانی که قصد ندارند حق و حقوق هنرمندان را به آن‌ها بپردازند؟ رانیتور کوهلن^{۲۴}، قاطعانه به این پرسش پاسخ منفی می‌دهد ولی در عین حال متذکر می‌شود که مصرف‌کنندگان نسبت به کسانی که در پی سودجویی‌های کلان

۲۲. John Perry Barlow کسی که در گذشته نویسنده متن ترانه‌های باند Grateful Dead را برعهده داشته و اکنون یکی از جدی‌ترین طرفداران تبادل آزاد اطلاعات است.

23. Carrie Russell

۲۴. کارشناس علوم ارتباط

هستند و در عصری که قیمت‌ها دائماً رو به کاهش است، قصد ندارند کوچک‌ترین تغییری در قیمت محصولات خود بدهند، احساس خوشایندی نداشته و با آن‌ها همراه نخواهند شد. او می‌گوید: «نمی‌توان برای مدت طولانی با استفاده از قانون‌های پی‌درپی به جنگ باورهای جدید و معمولی مردم رفت» (۴).

ضعیف‌ترین نقطه در موضوع امنیت، همچنان افراد و نگرش‌های آن‌ها خواهد بود. مدت‌هاست که علت اصلی در عمده نقض امنیت‌ها، رفتار غیرمجاز افراد غیرمجاز در کارهای روزانه‌شان است. در حالی که ابزارهای فنی و سکوها فنی امن و قابل اندازه‌گیری برای موفقیت در کار الکترونیکی ضرورت دارند، اما کمبودهای موجود در جنبه‌های غیرفنی امنیت را جبران نمی‌کنند. امنیت را باید تعریف، طراحی، و در فرایندهای کاری تعبیه کرد. افراد باید به خوبی راهنمایی شوند، آموزش ببینند و انگیزه‌مند شوند. همچنین باید به نظارت و بازخورد، و نیز به بازرسی مستقل توجه کرد. این امر مستلزم آن است که کل سازمان‌ها، کار را از رده بالای مدیریت خود شروع کنند. امکانات حاصل از کار الکترونیکی چنان است که باید در درازمدت، اطمینان حاصل شود که از زمان و کار به بهترین صورت استفاده می‌شود (۲).

مبالغه زیادی در مورد ظرفیت و دشواری‌های مدیریت حقوق دیجیتال صورت گرفته است و صورت خواهد گرفت. از یک طرف فروشندگان ادعای ایمن نگه داشتن محتوا را دارند و از طرف دیگر دوراندیش‌مآبان پیش‌بینی می‌کنند، زمانی که

جریان آزاد اطلاعات باشد، تجارت بر پایه محتوا از بین می‌رود (۷).

بدون شک بر سر فن‌آوری‌های DRM در آینده برای سال‌های طولانی جنگ خواهد بود. با این‌که تعداد زیادی از افراد در صنعت رسانه‌ها معتقدند که DRM تنها راه نجات الگوی تجارت فعلی آن‌هاست، این الگو مبتنی بر ایده جمع‌آوری حقالزحمه برای هرگونه استفاده است، تعدادی از مبتکران که شکست نهایی را برای DRM پیش‌بینی می‌کنند به جستجوی جایگزین مبادرت نموده‌اند (۱۶).

نتیجه‌گیری

مدیریت حقوق دیجیتال چیزی است که برای مقابله با نسخه‌برداری انبوه از آثار دیجیتال به وجود آمده است. در کل نظامی است که اعمالی برای حمایت از حقوق پدیدآورنده (گان) متن (ها)، انجام می‌دهد. این اعمال شامل محدود نمودن دفاعتی که فایل می‌تواند اجرا شود، ممانعت از اجرای فایل در یک دستگاه بدون مجوز، و نظارت بر روی عمل تأیید و تصدیق کاری که حین انتقال فایل‌های رسانه‌ای میان کامپیوتر و دستگاه قابل حمل انجام می‌گیرد، است.

نسل اول مدیریت حقوق دیجیتال DRM بر امنیت سطح پایین و رمزگذاری انتشار غیرقانونی، به وسیله قفل‌گذاری بر روی منابع و محدودیت در توزیع آن‌ها تنها به وسیله پرداخت هزینه متمرکز شد.

نسل دوم از مدیریت حقوق دیجیتال از دیدگاه عملی، امنیت جاری و رمزگذاری دور شد. توانایی‌هایش را به موضوع مدیریت

گسترش داد.

نسل سوم سیستم DRM، کاربرد جنبه‌های قانونی، فنی و اخلاقی را با هم ترکیب می‌کند تا به یک مدل تجاری منطقی و ارض‌کننده احتیاجات کاربر برسد.

DRM در رسانه‌های مختلفی کاربرد دارد، اما اغلب در فایل‌های موسیقی و ویدئویی دیده می‌شود.

استفاده‌کنندگان مدیریت حقوق دیجیتال نباید انتظار داشته باشند که فن‌آوری DRM، یا در واقع استانداردهای فنی آن، محتوای دیجیتالی آن‌ها را کاملاً تضمین کند. برای بهینه‌سازی حمایت، باید از چشم‌انداز وسیع‌تری، DRM بررسی گردد؛ نه این‌که فقط از چشم‌انداز فن‌آوری به آن پرداخت.

هنوز استانداردسازی مناسبی بر این سیستم صورت نگرفته است و سازمان‌های زیادی درگیر استانداردسازی آن هستند. از زبان‌های مهم DRM می‌توان به XrML (زبان نشانه‌گذاری صحیح و قابل گسترش)، ODRL (زبان حقوق دیجیتال باز) و XMCL (زبان تجاری رسانه‌ای قابل گسترش) اشاره کرد.

تکنولوژی‌های مدیریت حقوق دیجیتال ممکن است که خبر خوبی برای مالکان محتویات دیجیتالی، شرکت‌ها، استودیوهای فیلم، سازمان‌های جدید یا انتشارات پیوسته (online) باشد، اما پی‌آمد قطعی اجرای تکنولوژی‌های DRM محدودیت‌های غیرضروری و گرفتاری‌هایی برای کاربران رسانه‌های دیجیتالی و شبکه است. متأسفانه سیستم‌های DRM دارای مفاهیم منفی شامل کاهش حقوق افراد تحت قوانین کپی‌رایت

موجود و زمینه‌ای جدید برای تولیدکنندگان بدانندیش برای ردیابی سلیقه‌های افراد و فروش این اطلاعات به دیگران است. مبالغه زیادی در مورد ظرفیت و دشواری‌های DRM صورت گرفته است و صورت خواهد گرفت. از یک طرف فروشندگان ادعای ایمن نگه داشتن محتوا را دارند و از طرف دیگر دوران‌دیش‌مآبان پیش‌بینی می‌کنند، زمانی که جریان آزاد اطلاعات باشد، تجارت بر پایه محتوا از بین می‌رود. بدون شک بر سر فن‌آوری‌های DRM در آینده برای سال‌های طولانی، جنگ خواهد بود.

منابع

۱. اسدی شالی، عدله. «مدیریت سیستم‌های امنیت اطلاعات». *مجله الکترونیکی*، دوره چهارم، ۴ (۱۳۸۶). [قابل دسترسی در]:

http://www.irandoc.ac.ir/data/e_i/vol4/asadi_shali.pdf

۲. کاریلا، آرتور. «امنیت اطلاعات در کار الکترونیکی». ترجمه حمید دلیلی. *مجله الکترونیکی*، دوره دوم، ۲ (۱۳۸۶). [قابل دسترسی در]:

<http://www.irandoc.ac.ir/e-journal.htm>

۳. «مدیریت حقوق دیجیتال». *بزرگراه رایانه*، ۷۳ (۱۳۸۴): ۱۳۲-۱۳۵.

۴. همو. ترجمه رضا هدایتی. *آسیا*. ۲۰ مهر ۱۳۸۶، [قابل دسترسی در]:

<http://hamvatansalam.com/news39947.html>

۵. نقشینه، نادر. «رویکرد متفاوت به ملاحظات امنیتی

fi/studies/T-110.501/2001/papers/ index.html. [17Jan. 2008].

13. LaMacchia, Brian A. "Key challenges in DRM: an industry perspective". 2002. [on-line]. Available: <http://crypto.stanford.edu/DRM2002/abstract-bal.doc>. [17Jan. 2008].

14. Liong, Yin-Ling; Dixit, Sudhir. "Digital Right Management for the mobile internet". *Wireless Personal Communications*, No.29 (2004): 109- 119.

15. McCoyd, Edward. *Digital Right Management for Ebook: Publisher Requirements*. U. S. A: Association American Publisher, Inc, 2000. [on-line]. Available: <http://www.ebooks.com/ebooks/drm.pdf>

16. McGuigan, Brendan. "What is DRM". [on-line]. Available: http://www.wisegeek.com/what-is-drm.htm?referrer=adwords_campaign=drm_ad=1...2005

17. Reitz, John M. "DRM. ODLIS-Online Dictionary for Library and Information Science". 2006. [on-line]. Available: http://lu.com/odlis/odlis_d/cfm

18. Russ, Austin. "Digital Right Management overview: security essentials". 2001. [on-line]. Available: <http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html>. [17Jan. 2008].

تاریخ تأیید: ۱۳۸۷/۶/۳

در ابتکارات کتابخانه‌های دیجیتالی». *مجله الکترونیکی*، دوره پنجم، ۱ (۱۳۸۴). [قابل دسترسی در]:

http://www.irandoc.ac.ir/data/e_i/vol5/na ghshineh.pdf

6. Annella, Renato. "Digital Rights Management (DRM) architectures". *D-Lib Magazine*, Vol.27, No.6 (2001). [on-line]. Available: <http://www.dlib.org/dlib/june01/iannella/06iannella.html>. [17Jan. 2008].

7. Burner, Feed. *Digital Right Management Gone wrong: an overview of the past couple months*. 2005. [on-line]. Available: <http://feeds.feedburner.com/ericgoodwin>

8. "Digital Rights Management". *Wikipedia the free Encyclopedia*. 2006. [on-line]. Available: http://en.wikipedia.org/wiki/Digital_rights_management

9. Doctorow, Cory. "Digital Rights Management: a failure in the developed world, a danger to the developing world". [on-line]. Available: http://www.eff.org/IP/DRM/ITU_DRM_paper.pdf. [17Jan. 2008].

10. DRM. "Computer Encyclopedia". 2006. [on-line]. Available: <http://www.answers.com/topic/digital-rights-management?gwp=19>. [17Jan. 2008].

11. Ibid. "Web and XML Glossary". 2006. [on-line]. Available: <http://dret.net/glossary/drm>. [17Jan. 2008].

12. Guo, Heng. "Digital Right Management (DRM) using XrML". 2001. [on-line]. Available: <http://www.tml.hut>