KÜRESEL EKONOMİDE ŞİRKETLERİN MODERN FİKRİ MÜLKİYET STRATEJİSİ VE SAYISAL MÜLKİYET HAKKININ KORUNMASI

Cüneyt YÜKSEL[1] **Ender YÜKSEL[2]**

[1]İşletme Bölümü
İktisadi ve İdari Bilimler Fakültesi
Boğaziçi Üniversitesi, 80815, Bebek, İstanbul

[2]Bilgisayar Mühendisliği Bölümü
Elektrik-Elektronik Fakültesi
İstanbul Teknik Üniversitesi, 80626, Maslak, İstanbul

[1]e-posta: cuneyt.yuksel@boun.edu.tr [2] e-posta: ender@cs.itu.edu.tr

Anahtar sözcükler: Fikri Mülkiyet, Mülkiyet Hakkının Korunması, Damga, Parmak İzi

ABSTRACT

This paper discusses the protection of the intellectual properties such as trade secrets, trade marks and domain names by means of law. In addition, the protection of the digital data and the copyright is discussed with technical details.

1. YENİ BİR DEĞER OLARAK FİKRİ MÜLKİYETİN ÖNEMİ

Elektronik ekonominin ön plana çıktığı günümüzde bilgi, iş yöntemleri ve ticari sırların önemi gittikçe artmaktadır. Bu gerçeğin süratle farkına varan iş ortakları ve rakip kuruluşlar patent, marka, ticari sır ve internet alan adı gibi değerlerin korunabilmesi için hukuki yollara başvurmaktadırlar. Son yıllarda özellikle ABD'de, Avrupa Birliği ülkelerinde ve hatta Türkiye'de günlük iş münasebetlerinin içine giren patent, marka ve alan adları, şirketlerin modern fikri mülkiyet stratejilerinin önemini göstermektedir [2].

Fikri mülkiyet hakları: "Patentler ve Faydalı Modeller"i, "Ticaret ve Hizmet Markaları"nı, "Endüstriyel Tasarımlar"ı ve "İnternet Alan Adları"nı kapsamaktadır.

Türkiye, fikri mülkiyet konusunda birçok uluslararası antlaşmaya taraf olmanın yanısıra, iç mevzuat açısından da uluslararası mevzuat ile uyum içerisindedir. Bu sayede, günümüzde, yapılacak tek bir başvuru ile gerek marka gerekse patentlerin Türkiye ile birlikte birçok ülkede korunması imkânı doğmuştur. Özellikle uluslararası iş yapan ve küresel düşünen şirketlerimiz patent ve markalarının gerek Türkiye'de gerek ise diğer ülkelerde tescili yoluna gitmeli ve böylelikle yeni bir değer olarak karşımıza çıkan fikri mülkiyet varlıklarına küresel alanda koruma sağlamalıdırlar.

İnternet alan adlarının gerek Türkiye'de gerek ise diğer ülkelerde alınmasına öncelik verilerek küresel bazda korunma sağlanmalıdır. Zira günümüzde tanınmış kişi ve kurumların internet alan adlarının kötü niyetli kişilerce, örneğin "com.tr" olan internet alan adlarının ABD'de "com" olarak tescil olunması, sık sık gündeme gelmektedir. Bu ihlallere ilişkin olarak sevindirici gelişme ise başvurulabilecek hukuki yolların son yıllarda hem basit hem de hızlı bir hale getirilmiş olmasıdır. Dünyada ve Türkiye'de internet alan adları konusunda çok hızlı gelişmeler olmaktadır ve bu nedenle söz konusu gelişmelerin dikkatle takibi gerekmektedir. Örneğin, son olarak, ABD'de internet alan adlarının tescilleri ile iştigal eden bir firma (http://www.networksolutions.com/) artık sadece İngilizce harflerden oluşan alan adlarının değil bazı diğer dillerin alfabe harflerin kullanılabildiği (multilingual) internet alan adlarını deneme amaçlı olarak müüşterilerine teklif etmeye başlamıştır.

2. ŞİRKETLERİN MODERN FİKRİ MÜLKİYET STRATEJİSİ

Bir şirketin fikri mülkiyet stratejisi, o şirketin fikri mülkiyete konu varlıklarının değerini belirleyecek, koruyacak ve artıracak nitelikte olmalıdır. Böylesi

bir strateji öncelikle aşağıdaki sebeplerden dolayı önemlidir:

1. Fikri mülkiyetin korunmasına yönelik tedbirler şirkete getirecekleri yöntem bilgisi (know-how) ve uzmanlık sayesinde şirketin rekabet gücünü artıracaktır.
2. Fikri mülkiyete konu varlıkların doğru kullanımı şirkete lisans sözleşmeleri uyarınca sürekli bir gelir kaynağı oluşturacaktır. (Ayrıca 2005 yılından itibaren, AB şartlarına tabi olan her şirketin uyması gereken "Uluslararası Finansal Raporlama Standartları" uyarınca fikri mülkiyete konu varlıklar şirket bilançolarında gösterilebilecektir.)
3. Bir şirket rakiplerinin fikri mülkiyet faaliyetlerini de yakından takip etmelidir. Aksi takdirde şirket hem kendi haklarını kaybedecek hem de başkalarının fikri mülkiyet haklarını ihlal etmiş olmak iddiası ile karşı karşıya kalacaktır.

3. ŞİRKET FİKRİ MÜLKİYET VARLIKLARININ İNCELENMESİ

Bir şirket fikri mülkiyet varlıklarına ilişkin incelemesini aşağıdaki evrelerden geçirerek gerçekleştirmelidir.

3.1. Fikri Mülkiyet Varlıklarının Belirlenmesi

Bir şirketin fikri mülkiyet stratejisinin belirleyebilmesi için öncelikle hangi fikri mülkiyet varlıklarına sahip olduğunu saptaması gerekir. Bunun için aşağıdaki tanım ve kriterlerden faydalanılabilir.

Patent: Türkiye'de ve dünyada yeni olan, sanayiye uygulanabilen ve tekniğin bilinen durumunun aşılması kriterine uygun olan buluşların sahiplerine belirli bir süre bu buluş konusu ürünü üretme ve pazarlama hakkının tanınmasıdır.
Marka: Bir teşebbüsün mal veya hizmetlerini bir başka teşebbüsün mal veya hizmetlerinden ayırt etmeyi sağlaması koşuluyla kişi adları dahil, özellikle sözcükler, şekiller, harfler, sayılar, malların biçimi ve ambalajları gibi çizimle görüntülenebilen veya benzer biçimde ifade edilebilen baskı yoluyla yayınlanabilen ve de çoğaltılabilen her türlü işaretlerdir. Markaların belli bir süre tescili ile korunması mümkündür.
Telif Hakkı (Copyright): Özellikle bilgisayar programları gibi eserler ve diğer orijinal eserlerin ancak eser sahibinin izni ile çoğaltılması ve kopyalanması mümkündür [4,6].

3.2. Fikri Mülkiyet Varlıklarının Değerlendirilmesi

Öncelikle, şirket, mevcut ve potansiyel fikri mülkiyet kaynakları hakkında, operasyonlar konusunda uzman çalışanlarla görüşerek bilgi toplamalıdır. Sonrasında ise fikri mülkiyetin idaresi için mevcut prosedür ve yönetmelikleri incelemelidir. Ayrıca fikri mülkiyet kaynaklarının tesbit ve değerlemesine yardımcı olabilecek belgeler, sözleşmeler ve diğer materyaller analiz edilmelidir. Son olarak tüm bu çalışmaları özetleyen bir rapor üst yönetime sunulmalıdır.

4. FİKRİ MÜLKİYET STRATEJİSİNİN UYGULANMASI

Fikri mülkiyet stratejisinin uygulanması birkaç adımdan oluşmaktadır. Bu adımları şu şekilde özetleyebiliriz. Fikri mülkiyetin temel kaynaklarını belirleyen ve kontrol noktalarını oluşturan organizasyonel bir şema hazırlanmalıdır. Kontrol mekanizmalarına sahip prosedürler belirlenmeli ve yönetimin bu prosedürlerle ilgili onayı alınmalıdır. Fikri mülkiyet haklarını korumak ve maksimize etmek üzere mevcut sözleşme ve formlar geliştirilmelidir. Patent davaları, marka ve telif hakkı korumalarına ilişkin karar mekanizmalarını hızlandırmak amacıyla bir kılavuz hazırlanmalıdır. Sistemin geliştirilmesinden sorumlu olacak şirket personeline gerekli eğitim verilmelidir. Fikri mülkiyete konu varlıkların değerlemesinde kullanılacak bir fikri mülkiyet yöntemi geliştirilmelidir. Rakip firmaların ve iş ortaklarının fikri mülkiyet aktivitelerini takip etmeye ve örnek teşkil edebilecek e-ticaret operasyonlarını görüntülemeye olanak tanıyacak kıstasları içeren bir metod geliştirilmelidir.

5. SAYISAL MÜLKİYET HAKKININ KORUNMASI

Sayısal mülkiyet hakkının korunması ile ilgili geçerli bir çözüm sınırsız kopyalama ve kullanıma izin vermek fakat kötüye kullanım durumlarında elde kanıtlar olmasını sağlamaktır. Bu çözüm "sayısal mülkiyet hakkı etiketleme teknikleri"ni kullanır. Bu teknikler, mülkiyet hakkıyla ilgili olan kaynak, sahip, içerik veya alıcı gibi bilgileri, korunan materyale sayısal işaretler halinde gömerek belirtmeye dayanır. Sonuç olarak, bu yöntemle mülkiyet hakkının çiğnenmesi durumlarında olaydan sonra elde kanıtlar bulunmuş olur. Ayrıca bu teknikler sayesinde yasadışı kopyalamalar ve yayım için yanlış kullanımların izi sürülebilir ve kanıt gösterilebilir olması caydırıcılık sağlamış olur. Ancak sayısal mülkiyet hakkı etiketleme teknikleri, mülkiyet hakkı sahiplerinin yasadışı olaylar karşısında dava açabilmesine olanak veren bir yasal sistem gerektirir [1].

Genel olarak, çoğul ortam dokümanlarıyla ilgili mülkiyet haklarının tanınması ve korunması için iki tür etiketleme vardır:
Sahiplik Etiketleme: Doküman, mülkiyet hakkı sahibini eşi olmayacak (unique) şekilde tanımlayan bir etiketle işaretlenir.

Alıcı Etiketleme: Doküman, dağıtımının tek şekilde izlenebilmesine izin veren bir yapıda işaretlenir.

Sayısal mülkiyet hakkı etiketleme teknikleri izin verilen kopya sayısını sınırlamaz ancak korunan materyalin yasal sahibinin ve karşılık gelen mülkiyet hakkının belirlenmesine izin vererek (**Sahiplik Etiketleme Modeli**) veya yasadışı yoldan dağıtılan kopyanın gerçek alıcısına kadar izlenebilmesini sağlayarak (**Alıcı Etiketleme**) kullanıcıları yasadışı kopyalama yapmaktan caydırır. Literatürde sahiplik etiketleri **damga (watermark)** alıcı etiketleri de **parmak izi (fingerprint)** olarak geçer.

5.1 DAMGA (WATERMARK)

Damgalama, fiziksel dünyada kâğıda özel bir yazı veya resim işaret (damga) basılması tekniğine verilen isimdir.

Fiziksel dünyadakine benzer şekilde, çoğul ortam dokümanları gibi sayısal bilgilere eklenen ve daha sonra bilgi hakkında iddia veya açıklama yapmak üzere ortaya çıkarılan işarete ***sayısal damga*** denir. Sayısal damga, sahiplik iddiası, asıllama, bütünlük doğrulama, içerik etiketleme, kullanım kontrolü ve koruması gibi çeşitli amaçlara hizmet edebilir [5].

Tüm uygulamaların gereksinimlerini karşılayacak yaygın bir damgalama tekniği mevcut değildir. Her damgalama tekniğinin, kullanıldığı sistem bağlamında tasarlanması gerekir.

Bir damga görünür veya görünmez olabilir:

Görünür Damga: Kullanıcının görebildiği damgadır.

Görünmez Damga: Uygun bir yazılım tarafından bulunur (detection) ve ortaya çıkarılır (extraction).

Kullanıcılar damgalı dokümanın aslından farklı davranmamasını ve kalitesinde hiçbir görünür düşüş olmamasını isterler. Bu yüzden kullanıcılar genelde görünmez damga kullanmayı tercih ederler.

Bir damga narin (fragile) veya sağlam (robust) olabilir:

Narin Damga: Herhangi bir (görüntü işleme) dönüşüm sonucunda bozulabilir. Örnek: resim bütünlük kontrolleri.

Sağlam Damga: Genel (görüntü işleme) dönüşümlere karşı dayanıklıdır. Örneğin, resimler için kullanılacak damgalamanın filtreleme, ölçekleme gibi görüntü işleme operasyonlarına karşı dayanıklı olması gerekir.

Sağlamlık çoğu uygulama için anahtar gereksinimdir. Örneğin, sahiplik iddiası için kullanılan damganın sağlam olması gerekir. Ancak sağlam damgalama tekniklerinin geliştirilmesi kolay değildir. Sağlam damgalama için tüm gereksinimleri sağlayacak bir teknik geliştirmek zor bir problemdir ve günümüzdeki araştırma geliştirme konularından bir tanesidir.

Bir damga genel (public) veya özel (private) olabilir:

Genel Damga: Gizli bilgilere erişimi olmasına gerek olmadan herhangi bir kullanıcı tarafından tanınabilir ve okunabilir. Kullanıcının tek ihtiyacı uygun bir damga tanıma yazılımıdır

Özel Damga: Sadece gizli bilgilere ve uygun damga tanıma yazılımına erişimi olan bir kullanıcı tarafından tanınabilir ve okunabilir.

Özel damgalama, açıklamalar için veya kullanıcıyı mülkiyet hakkı durumundan haberdar etmek için kullanılamaz çünkü sadece içerik sahibi damgayı tanımak için gereken gizli bilgiye sahiptir. Bu yöntemde damga sadece içerik sahibi yasadışı kullanım saptadığında içeriğin sahibini göstermek amacıyla kullanılır.

Genel damgalama ise bir çok uygulama için caziptir. Örneğin, web üzerindeki bir resim için kullanım hakkı ihlallerini saptamak istersek Google gibi arama motorlarından bulabildiğimiz kadar resme kimlik testi uygulayabiliriz.

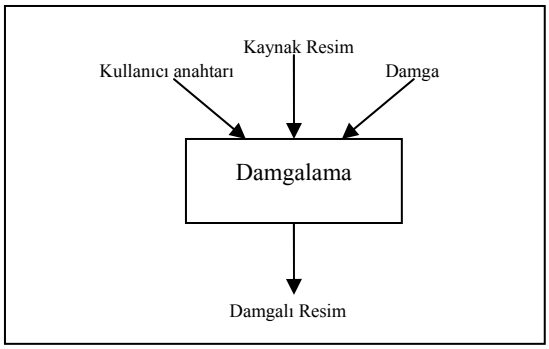
Özel damgalamada kullanılan anahtarın tipine göre damgalama teknikleri bulunur:

Simetrik Anahtar Damgalama Tekniği: Damga yerleştirilmesi ve tanınması için aynı anahtarı kullanır. Bu teknik, anahtar bilgisinin iletimi için, resim sahibi ve resim alıcısı arasında güvenli bir iletişim kanalı bulunmasını gerektirir.

Açık Anahtar Damgalama Tekniği: Damga yerleştirilmesi ve tanınması için ayrı anahtarlar kullanılır. Bir gizli anahtar sadece resim sahibi tarafından bilinir ve damga eklenmesi için kullanılır. Açık anahtar ise herkes tarafından bilinir ve damganın ortaya çıkarılması veya tanınmasında kullanılır.

5.1.1 DAMGALAMA

Şekil-1'de görüldüğü gibi, damgalama işleminde bir kullanıcı anahtarı, bir resim ve bir damga giriş olarak alınır ve çıkışta damgalı resim elde edilir.



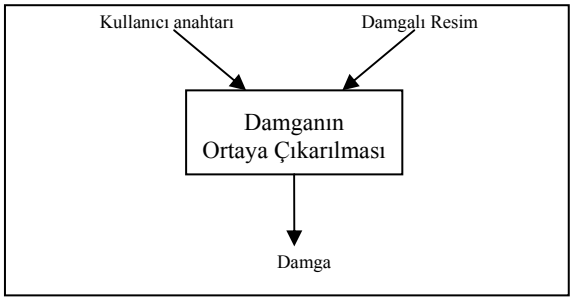
Şekil 1 – Damgalama

Basit bir damgalama tekniği şu şekilde olabilir: $x_1,x_2,x_3,\ldots$ piksel değerlerinden oluşan bir diziyle ifade edilen bir X resmi olsun. Bu resme damga yerleştirmek için önce bir anahtar kullanılarak rasgele sayı üretecine tohum (seed) değeri verilir ve bir m-dizisi (maksimum uzunlukta rasgele sayı dizisi) elde edilir. Bu m-dizisi kullanılarak bir damga işareti üretilir. İkili kodlanmış m-dizisinin elemanları 2 boyutlu bir damga matrisine yani damga işaretine dönüştürülür. Son olarak damga işareti bit bit kaynak resmin piksellerinin en düşük anlamlı bitlerine yerleştirilir. damga en düşük anlamlı bitlere (LSB) yerleştirildiği için görünmezdir. Yine aynı sebepten ötürü damga sağlam değildir çünkü kolayca bozulabilir.

5.1.2 DAMGA BULUNMASI VE ORTAYA ÇIKARILMASI

Bazı damgalama düzenlerinde bir damga tamamen ortaya çıkarılabilir.

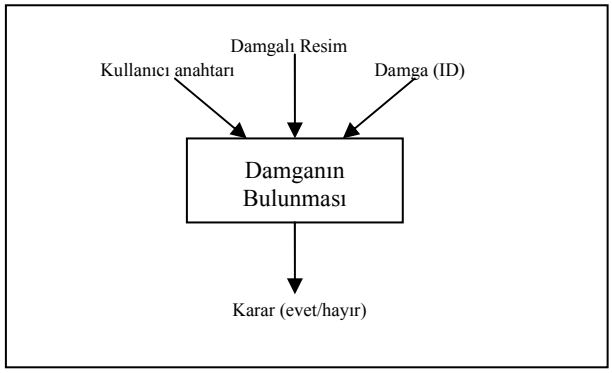
Şekil-2'de görüldüğü gibi, damga ortaya çıkarılması işleminde bir kullanıcı anahtarı ve bir damgalı resim giriş olarak alınır ve çıkışta damga elde edilir.



Şekil 2 – Damganın ortaya çıkarılması

Diğer damgalama düzenlerinde sadece bir resimde damga olup olmadığının anlaşılabilir. Bu işleme damganın bulunması denir.

Şekil-3'te görüldüğü gibi, damganın bulunması işleminde bir kullanıcı anahtarı, belirli bir damga (ID) ve bir damgalı resim giriş olarak alınır ve çıkışta resimde damga bulunup bulunmadığı kararı verilir.



Şekil 3 – Damganın Bulunması

Damga bulunması veya ortaya çıkarılması hassas ve karışık bir iştir. Çoğu algoritma, işaretlerin zayıflatılmış hallerini işleyemeyecek kadar yetersizdir.

5.1.3 OLASI SALDIRILAR

Damga tekniklerinin analizi için kriptanalizde kullanılana benzer şekilde bir terminoloji geliştirilmiştir. Damga tekniklerine karşı olası saldırılar dört sınıfa ayrılır:

Sağlamlık Saldırıları damgalı bir resimde resme zarar vermeden damgayı yok etmeyi veya azaltmayı amaçlar. Tipik işaret işleme saldırıları yaygın kullanılan veri sıkıştırma, filtreleme, boyut değiştirme, yazdırma ve tarama işlemlerinin çevresinde oluşur. Bu saldırılara bir örnek çarpışma saldırısı (collusion attack) dır. Bu saldırıda aynı resmin farklı damgalar yerleştirilmiş versiyonları, yeni bir resim yaratmak üzere birleştirilir, böylece damganın toplam gücü azaltılmış olur.

Sunum Saldırıları damgayı yok etmeye uğraşmaz. Bunun yerine damga tanınamasın diye resimle oynar ve resmi işler.

Yorumlama Saldırıları damganın varlığının çoklu veya geçersiz yorumlamalarını taklit etmeyi amaçlar. Örneğin, bir saldırgan bir resimdeki damgayla aynı güçte başka bir damga olmasını sağlayarak bir mülkiyet ölümcül kilitlenmesi (ownership deadlock) yaratabilir.

Yasal Saldırılar teknik değerlerin ve bilimsel kanıtların ötesindedir. Yasal saldırılar, mülkiyet hakkı kanunları ve sayısal bilgi mülkiyetiyle ilgili varolan ve gelecek yasal düzenlemeleri, kanunların çeşitli yargılamalarda farklı yorumlanmasını, sahip ile saldırganın güvenilirliklerini ve saldırganın mahkemede damgalama düzeni hakkında şüphe uyandırabilme yeteneklerini kullanır.

5.2 PARMAK İZİ

Dokümanlara parmak izi eklemek, sayısal damgalamadan farklı olarak, satılan veya dağıtılan her kopyaya özel işaretler ekleyerek, tıpkı insanlardaki parmak izleri gibi, kopyaların eşsiz olmalarını sağlamak demektir. Yasadışı bir kopya olduğunda, içerik sağlayıcı hangi orijinal kopyanın yasadışı dağıtıldığını parmak izinden anlayabilir. Sonuç olarak, bulunan taraf kendi kopyasını yasadışı dağıttığı için dava edilebilir.

Parmak izi teknikleri ve parmak izine karşı yapılan saldırılar damgadakilerle prensipte aynıdır.

5.2.1 SİMETRİK YÖNTEMLER

Parmak izi teknikleri, içerik sağlayıcısının yasadışı dağıtılan kopyanın gerçek sahibini tanımlayabilmesine imkan vererek, insanları yasadışı kopyalamadan alıkoymak içindir. Çoğu parmak izi tekniği hem içerik sağlayıcının hem de satın alanın parmak izi olan kopyayı bilmesi bakımından simetriktir. Ancak içerik sağlayıcı, satın alanın kopyayı yaydığını, yasal olarak, kanıtlayamaz.

5.2.2 ASİMETRİK YÖNTEMLER

Simetrik yönteme karşılık, Birgit Pfitzmann ve Matthias Schunter, satıştan sonra sadece satın alanın asıl parmak izine sahip kopyayı bilmesi bakımından asimetrik bir parmak izi tekniği önerdiler [3]. Bununla birlikte, içerik sağlayıcı daha sonra verinin bir kopyasını bulursa, parmak izinden satın alan kişiyi bulabilir ve bu kişinin kopyayı satın alan kişi olduğunu kanıtlayabilir.

5.2.2.1 ŞİFRELİ YAYIN ÖRNEĞİ

Asimetrik parmak izi yönteminin açık bir uygulaması, şifreli yayın düzenlerinde kaçak kullanımı izlemek (traitor tracing) üzere kullanılır. Şifreli yayın, bir içerik sağlayıcının çok miktarda veriyi şifrelenmiş halde yayınlaması ve sadece yasal abonelerin bu verileri çözüp alabilmesidir. Bu konunun tipik bir örneği Ödemeli-TV'dir. Ödemeli-TV, bir video akışının bir yayın kanalından şifrelenmiş halde iletilmesidir. Kaçak kullanım izleme yöntemleri, fazladan ve yasal olmayan kullanıcıların veri akışını çözebilmesini sağlayarak şifreli yayını kötüye kullanan veya haksız kullananları izlenmesini sağlar. Bir çok kaçak kullanım izleme yöntemi, şifreli yayının yasal abonelerinin tüm sırlarını bilgi sağlayıcıyla paylaşmaları bakımından simetriktir. Buna karşın, Pfitzmann asimetrik bir kaçak kullanım izleme yöntemi fikri sunmuştur. Bu fikre göre, içerik sağlayıcı sahteciliğe karşı koyarak, kendi kendine üretemeyeceği bilgiler elde eder. Sonuç olarak, bu bilgi yasal olarak çok daha iyi bir kanıt oluşturur. Asimetrik parmak izi tekniklerinin ve asimetrik kaçak kullanım izleme yöntemlerinin gelecekte mülkiyet hakkının korunması açısından daha önemli olacağı düşünülmektedir [3].

6. SONUÇ

Şirketlerin fikri mülkiyet stratejileri, şirketin fikri mülkiyete konu varlıklarının değerini belirlemesi, koruması ve artırmasının yanı sıra şirketin rekabet gücünü arttırması, şirkete sürekli bir gelir kaynağı oluşturması açısından da önemlidir. Fikri mülkiyet sistemi şirket kültürü ile uyumlu olmalı ve şirketin işleyişini gereksiz yere aksatmamalıdır. Şirketin fikri mülkiyet sistemi dış danışmanlardan bağımsız, iç kaynaklarla yönetilebilen bir işleyişe sahip olmalıdır, idari sorumlulukta bu kaynaklara ait olmalıdır. Fikri mülkiyeti maksimize etmeye yönelik çalışmalar değerlendirilmeli, organizasyonel ve ekonomik teşvikler verilmelidir. Maddi varlıkların mülkiyetinin korunması için kullanılan teknikler mümkün olduğu ölçüde fikri mülkiyet varlıklarının korunmasına da uyarlanmalıdır.

Sayısal mülkiyet hakkı etiketleme tekniklerinin ticari kullanımı başlamış olmasına rağmen hâlâ bu tekniklerin etkili ve yaygın kullanımını engelleyen unsurlar bulunmaktadır. En büyük sorun, etiketleri gizli tutarken, güvenilir ve sağlam bir koruma sistemi geliştirmektir. Varolan hiçbir sistem etiketlerinin tüm büyük işaret işleme ve dönüşümlerine karşı ayakta kalabileceğini iddia edemez.

KAYNAKLAR

[1] R Oppliger, Security Technologies for the World Wide Web, Artech House, 2000.

[2] B A Lehman, R H Brown, Intellectual Property And The National Information Infrastructure, The Report Of The Working Group On Intellectual Property Rights, 1995.

[3] B Pfitzmann, M Schunter, Asymmetric Fingerprinting, Proceedings of EUROCRYPT, 1996

[4] GNU Project, http://www.gnu.org

[5] J Zhao, E Koch, C Luo, In Business Today and Tomorrow, Communications of the ACM, Vol. 41, July 1998

[6] Free Software Foundation, http://www.fsf.org