ISSN-1301-6229

EKEV

AKADEMİ DERGİSİ

Academic Review

- Sosyal Bilimler -

Social Sciences

Yıl *Year* 6 *Sayı* *Number* 11 *Bahar* *Spring* 2002

İNTERNET ORTAMINDA
ETİK İHLALLER

Özet: Bilgi teknolojilerindeki hızlı değişimle birlikte gelişen ağ teknolojisi ve İnternet daha önce tanımlanmamış birtakım suç ve etik ihlallerin ortaya çıkmasına neden olmuştur. Ekonomik ve sosyal kayıpları beraberinde getiren bu tür problemlerin önlenebilmesi yasal yetersizliklerden ve boşluklardan dolayı mümkün olmamıştır. Çoğu ülkelerde bu çalışmada yer verilen etik ihlalleri tanımlayan ve yaptırım öngören kurallar henüz belirlenmemiştir. Çalışmada etik olarak olumsuzluklar incelenmiş ortaya çıkış nedenleri belirtilmiş ve önerilerde bulunulmuştur.

I-GİRİŞ

Günümüzde hızla gelişen iletişim araçlarından biri sayılan bilgisayar, teknolojideki gelişme ve buna bağlı olarak maliyetinin düşmesiyle kolayca elde edilebilir hale gelmiş ancak yaygınlaşmasına paralel olarak da bir takım etik problemler de ortaya çıkmıştır. Toplumların sosyal ve kültürel yapıları dikkate alındığında etik kuralların ve değerlerin değişiklik göstermesi son derece doğaldır. Bireylerin davranışlarına yön veren değerlerin bir kısmı toplumlara göre farklılık göstermez ve evrenseldir. Bu tür davranışların aksi davranışlar "suç" kavramı altında incelenmekte ve cezai yaptırımlarla sakındırılmaktadır. Örneğin kişisel bilgilerin gizliliği, sınai ve fikri mülkiyetlerin korunması, haber alma serbestliği hukuk devletlerinin vazgeçilmeyen kurallarındandır. Coğrafi sınırları kaldıran, dünyayı adeta küçülten İnternet ortamında bu gibi kurallar sıklıkla ihlal edilmektedir. Bu ihlaller sonucu bir takım kişi ve kuruluşlar zarara uğramakta diğer yandan buna sebep olanlar haksız bir kazanç elde etmektedirler.

Kullanıcıya, bilgiye ulaşma ve paylaşma kolaylığı veren İnternet aynı zamanda suç teşkil edecek veya etik açıdan zarar verecek bilgiye ulaşma imkanı da vermektedir. İnternet ortamında denetimsiz bir şekilde bilgilerin paylaşıma açılmasının suç oluşturması yanı sıra İnternet üzerinde bulunmasının bile suç oluşturduğu bilgiler vardır. Bu bağlamda söz konusu bilginin İnternet ortamına taşınması durumunda bilgiyi sunan, bilginin paylaşılması durumunda ise hem bilgiyi paylaştıran hem de bilgiyi kullanan kimseler suç işlemiş olmaktadır. İnternet'in sınırsız olmasına karşın kullanıcılarının bulundukları ülkedeki hukuk normlarının aynı olmaması bu ihlallere uygulanacak yaptırımların neler olacağı konusunda birlikteliğin oluşmamasına neden olmakta ve bu tür ihlaller engellenememektedir.

Bilgi teknolojilerinin güvenliği, zorunlu yedi kısımdan oluşmaktadır (Hannaford, 1995, s.10). Bunlar;

1- İdari ve organizasyon güvenliği,
2- Personel güvenliği,
3- Fiziksel ve çevresel güvenlik,
4- Donanım güvenliği,
5- Haberleşme güvenliği,
6- Yazılımların güvenliği,
7- İşlem güvenliğidir.

Bunlardan birinin veya birden fazlasının yetersiz olması durumunda bu güvenlik noktalarının açıklarını kullanarak sisteme yetkisiz kişilerin ulaşması ve zarar vermesi gibi sorunların ve problemlerin ortaya çıkması kaçınılmaz olacaktır.

II- ETİK KURALLARIN İHLAL EDİLDİĞİ KONULAR

Bu çalışmada evrensel anlamda etik kuralların ihlal edildiği konular ayrı başlıklar altında incelenecek ve kişisel anlamda uygun davranış biçimlerine yer verilecektir.

A. FİKRİ HAKLARIN İHLALİ

En fazla ihlal edilen konu fikri mülkiyet haklarıdır. Bir fikir ve sanat eserinin izinsiz olarak çoğaltılması, yayılması, çeşitli vasıtalarla yayımlanması ve işlenmesi şeklinde ortaya çıkan bu durum eser sahibinin maddi ve manevi haklarını ciddi bir şekilde ihlal etmektedir.

Bu ihlaller daha çok yazılı bir eserin yayımlanması, müzik eserlerinin çoğaltılması, resim-grafik ve filmlerin gösterilmesi ile bazı bilgisayar programlarının kullandırılması şeklinde görülmektedir (Lang, 2001, s.8-26). Bu türden içerikleri bulunduran sitelere herhangi bir sınırlama olmaksızın girilebilmekte ve basit bir işlemle dosyalara ulaşılıp çoğaltılabilmektedir. Söz konusu sitelerin kâr amacı gütmediklerini sadece kullanıcılarına hizmet verdiklerini ifade etmiş olmalarına karşın çeşitli ülkelerde yasal yollara başvurular olmuş ancak gerçek anlamda sınırlama getirilememiştir. Bu tür ihlallerin gerçekleşme şekilleri 3 başlık altında toplanabilir.

1. Download: Fikri bir çalışma sonucu üretilmiş bir ürünün sahibinden izin alınmaksızın paylaşıma açık bir adresten kullanıcının makinesine kopyalanması işlemidir.

2. Cracking: Belirli amaçlar için geliştirilmiş yazılımların, oyunların izinsiz kopyalanmalarına ve kullanımlarına engel olmak için içlerine belirli kodlar ve şifreler yerleştirilmiştir. Bu kod ve şifreler doğru olarak girilmediği takdirde yazılımı kullanmak veya

kopyalamak imkansız hale gelir. Orijinal bir yazılımın içindeki söz konusu kodların çözülerek kodsuz olarak çoğaltılması veya kullanılması "cracking" olarak adlandırılır.

3. Usulsüz Güncelleme: Bazı yazılım üreticileri bir programın yeni sürümleri üretildiğinde o programın eski sürümünü lisanslı olarak edinmiş kimselere ürünlerini bedelsiz olarak güncelleme imkanı vermektedir. Bu güncelleme için önceki sürüme ait seri numarası gerekmektedir. Cracking ile elde edilmiş kopya programı güncellemek için geçerli seri numarası ise Internet ortamında bu tür seri numaraları bulunduran sitelerden alınmaktadır. Bu şekilde yazılımcı kuruluş satmadığı binlerce kopya programı güncelleme durumunda kalmaktadır.

B. HACKING (Sabotaj)

İnternet üzerinde dolaşmayı sağlayan tarayıcının veya işletim sisteminin güvenlik açıklarını (Hopwood, 2000, s.48-49) kullanarak başkasına ait bir sitenin kodunun kırılarak içeriğinin ele geçirilmesi ve değiştirilmesi "hacking" olarak adlandırılmaktadır. Genel anlamda hacking üç farklı nedene dayandırılır.

1. Politik Amaçlı Hacking: Devlet kuruluşlarına ait sayfalar ile siyasi içerik bulunduran sitelere yönelik olarak gerçekleştirilir. Genellikle sayfaya, slogan türünde belirli bir olayı protesto mahiyetinde not bırakılır ve zaman zaman sitede bulunan linkler başka adreslere yönlendirilir.

2. Zarar Amaçlı Hacking: Bu tip hackingde siteyi ele geçirmek amaç olmayıp sitenin bulunduğu bilgi sistemine ve ağına girerek veri tabanlarını ve paylaşılmamış bilgi dosyalarını ele geçirmek amaçlanır. Bu şekilde ele geçirilen bilgiler arasında kredi kartı bilgileri e-mail hesapları gibi kişisel bilgiler bulunduğundan hacker(lar) bu bilgileri kullanarak başkasının adına kredi kartı ile alış veriş yapabilir veya e-maillerini okuyabilirler.

3. Kişisel Amaçlı Hacking: Hacker(ler) ile kişisel problemleri nedeniyle veya bir hacker'in diğer hacker'e kendini kanıtlama amacıyla yapılan sabote işlemleridir.

Hacking, siteler açısından bir olumsuzluk olmasının yanında güvenlik açıkları konusunda fikir vermesi nedeniyle sistem yöneticilerine yol gösterici olabilmektedir. Bu bağlamda gelişmiş ülkelerde çeşitli kuruluşlar sistemlerinin güvenlik açıklarının bulunması amacıyla örgütlü bir şekilde faaliyet gösteren Hacker gruplarına (Evans, Furnell, 2000, s.239) görevler vermekte, tespit edilen açıklar böylelikle giderilmektedir (Furnell, Chiliarchaki, v.d., 2001, s.93-100). Ancak amacı ne olursa olsun bir sitenin sabote edilmesi etik açıdan doğru kabul edilemez.

C. PORNOGRAFİ

Toplumların ahlaki ve kültürel gelişimi dikkate alınarak pornografik yayınların belirli bir yaşa gelmemiş kişilere ulaşmaması için birçok ülkede yasa koyucular tarafından önlemler öngörülmüştür. Bu önlemler söz konusu yayınların 16-18 yaş altındakilere satılmaması ve umuma açık mekanlarda gösterilmesi durumunda belirtilen yaştakilerin gösterime alınmaması şeklinde olmaktadır. Ancak İnternet üzerinde pornografik içerik bulunduran sitelere ulaşmada herhangi bir yaş sınırı bulunmamaktadır (Thomas, 1997, s.202). Sitenin giriş sayfasında içeriğin pornografik olduğu ve 16-18 yaş üzeri bulunulması gerektiği belirtilmektedir. Bu uyarı siteyi kanunlar karşısında sorumluluktan kurtarmaktan öte bir şey değildir. Oysa etik sorumluluk sadece yazılı kanunlara uymak demek değildir. Bu tür sitelere girip 16-18 yaş üzerinde bulunduğunu belirten kimsenin bu bildiriminin doğru olduğu varsayılmakta ve siteye giriş izni verilmektedir. Kullanıcıların tamamen kişisel etik kurallarıyla ilgili olan bu durum tartışılamaz. Ancak belirli yaş grubu ve altındakilerin bu tür yayınlardan etkilenmemelerini sağlayamamak asıl tartışılacak olan ihlallerdendir.

Ayrıca müzik eserlerinin paylaşımına imkan tanıyan siteler olduğu gibi pornografik dosyaların da paylaşımını sağlayan siteler bulunmakta, kredi kartı bilgileri veya yaş sorgulaması gibi sınırlamalar gerektirmeyen söz konusu sitelerde bu başlık altında incelenen etik ihlaller endişe verecek şekilde yaygınlaşmaktadır.

D.SPAM MAİL

İstem dışı alınan elektronik postalar "spam mail" olarak adlandırılır (Jackson, DeCormier,1999, s.135). Genelde reklam amaçlı veya belirli bir siteye yönlendirme amaçlı olarak gönderilirler. Spam mail için elektronik posta adreslerinin elde edilmesi ise adres sahibinin dikkatsizliği veya yasadışı yollarla olmaktadır.

Gezinti veya bilgi alma amacıyla girilen sitelerde kullanıcı ile irtibat kurmak veya bir takım bilgilerin kendine gönderilebilmesi içine-mail adresi istenir. Ancak satır aralarında kolayca görülemeyen bir yerlerde girilen site ile ilgili *"haberler, değişiklikler veya tanıtımlar için mail almak istiyor musunuz?"* şeklindeki bir seçenek kullanıcı sayfasına nedense sürekli seçili olarak gelir. Bu durumda kullanıcı kendi isteğiyle ama farkında olmadan sayfa ile ilgili tüm reklamlar ve ürünler ile ilgili olarak spam mail almayı kabul etmiş demektir. Kullanıcının dikkatsizliğinden bu şekilde yararlananlar, adresleri başkalarıyla da paylaşmaktadırlar.

Kişisel ilişkide saygılı reklamcı ve tanıtımcılar gönderdikleri maillerde "*bu maili istem dışı aldığınızı düşünüyorsanız bizi uyarın*" şeklinde bir yaklaşımla spam mail durumuna son vereceklerini belirtirler. Mail almak istenmediğinin belirtilmesi durumunda spam mailler

kesilir. Ne var ki verilen e-mail adresleri hiçbir zaman kalıcı olarak karşı tarafın veri tabanlarından silinmezler. Bir süre sonra yeniden spam mailler alınmaya başlanır ve bu maillere son verme isteği işlemi (unsubscribe) yeni baştan başlar.

Yasa dışı yollardan elektronik posta adreslerinin ele geçirilmesi ise; adres sağlayıcı kurumun adres veri tabanını çıkar amacıyla başka kuruluşlarla paylaşması veya gönderilen postanın alıcısına ulaştırılırken üzerinden geçtiği kanallarda adreslerinin alınması şeklinde ortaya çıkmaktadır. Kaynağı belirsiz bir adresten alınan yardım çağrısı kullanıcıya *"... bu maili adres defterinizdeki herkese ulaştırarak bizlere yardımcı olun.."* şeklindeki bir mailde çoğunlukla mail gövdesi içinde gömülü gizli kodlarda, mailin iletildiği kişilerin e-mail adreslerini alarak e-mail avcılarının adresine gönderen bir yazılım bulunur bu şekilde elde edilen yüz binlerce adres reklam ve tanıtım işi yapan kuruluşlara pazarlanır.

Belirsiz bir adresten binlerle ifade edilen sayıda anlamsız mailler göndererek kullanıcıyı ve bağlı bulunduğu sistemi çalışamaz duruma getirip çökertme işlemi "mail bomb" olarak adlandırılır ki bu da istem dışı mailler konusunda değerlendirilebilir. Yalnız burada amaç kullanıcıyı ve sistemi meşgul edip kilitlenmesini sağlamak suretiyle devreden çıkartmaktır. Özellikle İnternet'e, dail-up şeklinde modem vasıtasıyla bağlanan kişiler bağlantı yaptıklarında bekledikleri bir maile ulaşabilmek için beklemedikleri söz konusu istem dışı mailleri de almak durumunda olduklarından uzun bir süre sisteme bağlı kalmaları gerekmekte bu da hem kaynak hem de zaman kaybına neden olmaktadır.

E. VİRÜSLER

Yeni olmamasına karşın İnternet yoluyla daha hızlı yayılması ile yeniden gündeme gelen bir etik ihlal de virüslerdir. Eskiden olduğu gibi virüsler artık sadece programlara zarar vermekle kalmıyor donanıma da etki ediyor. Hard diski kullanılamaz hale getiren veya sistem bilgilerini tutan belleği yeniden programlayan virüs yazılımları daha korkutucu olmaktadır. İnternet'le bağlantısı bulunan neredeyse her kullanıcının elektronik posta adresine sahip olmasını değerlendiren virüs yazarları e-posta ile yayılan virüslere ağırlık vermektedirler. Bu şekilde sadece e-posta alan veya gönderenler değil bu kişilerin adres defterlerinde bulunan kişilere de kendini gönderebilen virüslerin yanı sıra sürekli isim ve yapı değiştiren virüsler de yaygın olarak görülmektedir (Sanderson, Forcht, 1996, s.35). Zarar verme dışında başka amacı olmayan virüslerin, anti-virüs yazılımının üretilip dağıtılması virüs kadar hızlı olmadığından ortaya çıkan zarar telafi edilemez boyutta olmaktadır.

F. ALDATICI VE ŞİDDETE YÖNELİK İÇERİK

Reklam, tanıtım ve ürün satış amaçlı içerik bulunduran birtakım siteler de etik kuralları hiçe saymaktadırlar. Sergilenen ürün veya hizmetin kalitesinin ve niteliklerinin, tüketicinin uzaklığı dezavantajından yararlanılarak olduğundan daha farklı gösterilerek sunulması ile tüketici aldatılmaktadır. Aldatıldığını anlayan kişinin mamulü iadesi veya değiştirmesi, alınan ürünün düşük bedelli olması nedeniyle zaman ve kaynak israfına neden olacağından genelde beklenmemektedir. Hemen tüketilen hizmet şeklindeki sunumların bedelinin iadesi de hiçbir zaman mümkün olmamaktadır.

Bu başlık altında söylenebilecek diğer bir etik ihlal ise bir konu hakkında toplumu yönlendirmeye yönelik yapılan gerçek dışı bilgilendirmelerdir. Gerek kişisel gerekse kurumsal bazda hedef alınan kişi veya kurum aleyhinde bilgiler ile masum bir görüntü ve halkı bilgilendirme maskesi altında çıkar amaçlı faaliyetler görülmektedir. Ekonomik konularda daha başarılı olan spekülatif amaçlı yönlendirmeler ve şirket bazında karalamalar ile çıkar sağlamak, bu tür etik ihlallerin en başında gelmektedir.

Politik siyasi ve etnik sorunların irdelendiği yanlı ve illegal siteler de toplumun belirli bir kesimini diğer bir kesim üzerinde baskı kurmaya ve şiddet kullanmaya çağırmakta, toplumu galeyana getirecek materyaller bulundurup toplumsal barışı ve huzuru bozucu faaliyette bulunmaktadırlar.

III- SOHBET ODALARINDA VE HABER GRUPLARINDA ETİK KURALLARA UYGUN DAVRANMA

İnternetde kişisel etkileşimli haber grupları sohbet odaları ve açık liste grupları vardır. Buralardaki etik kurallar evrensellikten de öte insan olmanın verdiği sorumlulukla bağdaşır olmalıdır. Bu tür sitelerde belirli yazılı kurallar yoktur. İkili sohbetlerin yapıldığı odalardaki olabilecek etik olumsuzluklar sadece iki kişi ile sınırlı kalacağından çevreyi etkilemeyecektir. Ancak çok sayıda kişinin buluştuğu bir sohbet odasında meydana gelecek etik olumsuzluk rahatsızlık verici olacaktır. Bu durumda sohbet kanalının yönetici operatörü belirlediği kurallara uygun davranmayan kimseleri odadan atmaktadır. Bu işlem her ne kadar olumsuzluğa bir son verse de pek de sevimli olduğu söylenemez.

Haber gruplarında da çeşitli siyasi ve güncel konular tartışılmakta yazılar yazılmaktadır. Siyasi ve ekonomik haber gruplarında genelde eleştirisel boyutlar aşılarak hakaret ve aşağılamaya giden yazılar ve söylemler yer alabilmektedir. Haber grubu yöneticisi de bu tür hakaretlere ve aşırı davranışlara müdahale ederek seviyeyi korumaya çalışmaktadır.

Açık liste gruplarında da liste üyelerinin çoğunluğunun katıldığı oturumlarda sık sık tartışmalar olmakta, liste yönetici ise bu tartışmalara gerekmedikçe müdahale etmemektedir. Zaman zaman yönetici tarafından listeden uzaklaştırılan kişi olmakta ise de bu kişi genelde çoğunluğun isteği ile liste dışına alınmaktadır.

Kişilerin doğasında bulunan farklılıkların sonucu fikir ve söylem ayrılıkları kaçınılmazdır. Belirli bir fikir ve söylemin bir diğer kişiye kabul ettirilmesi için baskı yapılması ve hakarete varan sözler söylenmesinin tartışma mantığından uzak olduğu açıktır. Yazılı etik kuralları olmamakla birlikte bu tür ortamlarda uyulması gereken asgari davranış biçimlerinden bazıları şöyledir;

- Başkasından görmek istemediğiniz davranışları siz sergilemeyiniz
- Düşüncelerinizi anlatırken ısrarcı ve önyargılı olmayınız.
- Kişilerin özel yaşamlarını ilgilendiren konulardan uzak durunuz.
- İstenmeden ortaya çıkan yanlış anlaşılmalara hoşgörülü yaklaşınız.
- Kişileri eleştirmekten uzak durun ve buna fırsat yaratmayın.
- Eleştirilerde hakaret ve şiddet ifade eden kelimeler kullanmayın.
- Kişisel bazdaki tartışmalara liste üyelerini rahatsız edebileceğinizi düşünerek girmeyiniz veya çok kısa tutunuz.
- Kişilerin duygusal zafiyetlerinin kullanılmasına imkan tanımayınız ve araç olmayınız.

Bu kurallara ek olarak genel anlamda bilgisayar kullanım etiğinin kuralları da söyle sıralanabilir (Scheuermann, Taylor, 1997, s.269).

1- Bilgisayarı başkalarına zarar vermekte kullanmayacaksın.
2- Bilgisayar ile başkalarının işlerine engel olmayacaksın.
3- Başkalarının dosyalarını ele geçirmenin yollarını aramayacaksın.
4- Bilgisayarı hırsızlık yapmak için kullanmayacaksın.
5- Bilgisayarı sahte delil hazırlamakta kullanmayacaksın.
6- Bedelini ödemediğin kopya programları kullanmayacaksın.
7- Yetkin olmadığı halde diğer insanların bilgisayar kaynaklarını kullanmayacaksın.
8- Başkalarının fikri çalışmalarının sonuçlarını kendine mal etmeyeceksin.
9- Bir program yazarken sosyal sonucunu düşüneceksin.
10- Bir bilgisayarı dikkatle ve itina göstererek kullanacaksın.

IV- İHLALLERİN HUKUKİ BOYUTU

Yapıları itibariyle kişisel hakların ihlali veya ticari ve sınai mülkiyetlerin ihlali olarak karşımıza çıkan hukuki durum için ülkelerdeki farklı hukuk düzenlemelerinden dolayı caydırıcı nitelikte bir ceza ortaya konulmasında güçlükler yaşanmaktadır.

Bu güçlükleri aşabilmek için etkin İnternet bağlantısına sahip ülkelerin ortak çabalarıyla, bilgisayar yoluyla işlenen suçlar ve hukuk ihlalleri için "suç ve ceza" tanımlamaları yapmaları "Siber Hukuk Normları" geliştirilmesi gerekmektedir.

Günümüzde bir ülkeden diğer bir ülkeye ait sitelere yönelik saldırı gerçekleştiği veya mülkiyet haklarının ihlali söz konusu olduğunda hangi ülkenin yasalarına göre yargılanacağı ve cezasının ne olacağı belirli değildir. Bir ülkenin hukuk kurallarına göre suç sayılan bir durumun diğer bir ülkede tanımı dahi yapılmamış olabilmektedir. Bu durumda bir ülkede bilgisayar aracılığıyla gerçekleştirilen ve suç sayılan bir eylemin söz konusu eylemi suç olarak tanımlamayan bir diğer ülke üzerinden yapılacağını beklemek son derece doğaldır. Bu durumun önüne geçilebilmesi için ortak bir hukuk düzenlemesine gereksinim vardır. Dünya üzerindeki ülkelerinin aynı siyasal ve ekonomik gelişmişlik düzeyine ve ortak bir hukuk yapısına sahip olmamaları geniş bir katılımla yapılacak bir düzenlemenin önünde engel olarak görülmektedir. Ancak aynı düzeyde ve yapıdaki ülkelerin bir araya gelerek ortak bir düzenleme yapmaları mümkün görülmektedir.

Bu konuda ileri sürülen olumlu düşünceler sadece tasarım aşamasında kalmış ortak bir metin haline henüz getirilememiştir. Ülkeler bazında yapılan düzenlemeler ise geneli ilgilendirmeyen konularla sınırlı kalmış zaman zaman da katı bir sansür görüntüsü verecek uygulamalara yer verilmiştir. Günümüzde büyük bir katılımla imza altına alınmış ve uygulanmakta olan herhangi bir iletişim ve erişim kuralları maalesef yoktur.

Dünya Fikri Mülkiyet Teşkilatı WIPO (World Intellectual Property Organization) fikir ve sanat eserlerinin elektronik ortamda korunması ile ilgili bir çalışmalar yapmaktadır. WIPO' nun hazırladığı metinler sadece fikir ve sanat eserlerinin korunması ile ilgili düzenlemeler içermektedir. Oysa İnternet yoluyla ihlal edilen etik kurallar sadece fikir ve sanat eserleriyle sınırlı değildir.

İnternet'in sürekli gelişip büyüdüğü dikkate alınarak benzer kaygıları bulunan ülkelerin ortak çabalarıyla evrensel etik kuralların neler olduğunun tanımlandığı, korunduğu ve ihlalleri durumunda uygulanacak yaptırımlar konusunda kararlar içeren bir metnin hazırlanması ve uygulamaya konulması gerekmektedir. Değişen ve gelişen teknolojik ve toplumsal değer yargılarının olacağı, etik normların sistemin gelişimi ile birlikte değişebileceği dikkate alınarak sürekli güncellenen tanımlar ve kararlar ile düzenlenen

kurallar bütününün uygulanabilirliği devam ettirilmelidir. Bu yapılırken de katı bir kuralcılığın İnternet'i geliştirmek yerine kısırlaştıracağı unutulmamalıdır.

V. ÖNERİLER

Yapılacak öneriler, kullanıcıların etik açıdan karşılaştıkları olumsuzlukları tamamen ortadan kaldırmaktan çok, en alt düzeyde etkilenmelerini sağlayacak bazı yol göstermeleri içermektedir.

Fikri bir çalışmanın sonucu olan ürünler bilgisayar ortamına aktarılmış ise bunlar kesinlikle sadece kişinin kullanımında ve paylaşıma açılmamış olmalıdır. Legal olarak bedel ödenip elde edilen bir fikri ürünü bir başkasının bedelsiz olarak elde etmesi sadece fikri eser sahibinin değil, bedel ödeyerek satın alan kişilerin de haklarının ihlal edildiği anlamı taşıdığı bilinmelidir.

Amacı ne olursa olsun başkasına ait bir sitenin sabote edilmesini haklı gösterecek bir sebep olamaz. Sabote olmamak için güvenlik açıkları bulunan programların yama (patch) larını kullanmak veya tam sürümlerini yüklemek ile güvenlik duvarı ardında bulunmak (fire wall) fayda sağlayacaktır. Bunun yanında sisteme dışarıdan erişimin engellenmesi için "erişim kontrol sistemleri" nin kullanılarak o anda sistemde olmaması gereken kişilerin yetkisiyle erişimin engellenmesi de mümkündür. Ayrıca gizli ve çok önemli bilgilerin şifreli bir şekilde bulundurulması da yetkisiz kişilerin bir şekilde bunlara ulaşması durumunda bilgileri kullanması engellenmiş olacaktır (David, v.d., 1999, s.357-358).

Spam maillerden korunmak için farklı birkaç yol kullanılabilir. Bunlardan birincisi; birden fazla ve farklı adreslere sahip olmak. Resmi veya ticari amaçla kullanılan adresleri sadece asıl uğraş ile ilgili kişi ve kuruluşlara vermek, bunu dışındaki kişisel işler için ise ikinci derecedeki adresi kullanmak (Attaran, VanLaar, 1999, s. 243). Bu şekilde asıl uğraş için kullanılan adresin kontrol dışında yayılması önlenmiş olacaktır. Aşırı derecede istem dışı mailler ile dolan bir adresi terk edip kullanmamak yeni bir adres almak en iyi yoldur. Spam maillerden korunmanın diğer bir yolu ise kullanılan mail istemcisinde istenmeyen mail adreslerini belirtmek suretiyle belirtilen adreslerden gelen maillerin doğrudan çöp kutusuna atılması sağlanabilir. Bu şekilde sadece kullanıcı spam mailleri okumaktan kurtulur ancak mail sunucusu üzerinde bu mailler yine yer tutacaktır. Bunu önlemenin yolu da sistem yöneticisinin kullanıcı istekleri veya kendi tespitleri doğrultusunda bir takım adresleri kara listeye almak suretiyle listedeki sunuculardan gelen mailleri engellemektir.

Virüslerden etkilenmemek için ise anti-virüs programı kullanmak ve sürekli güncellemek gerekir. Virüs içerdiğinden kuşkulanılan bir dosya başkasına gönderilecek ise

bunun karşı tarafa bildirilmesi yerinde bir davranış olacaktır. Düzenli olarak anti-virüs forumlarını izlemek veya konu ile ilgili açık listelerde yeni bulgu ve tanımları takip etmek de fayda sağlayacaktır.

İnternet üzerinden bir hizmet veya ürün alınacak ise ürün garantisi, iade garantisi, değiştirme gibi imkanları sağlayanlar tercih edilmeli belirtilen özellikleri veya kaliteyi taşımadığı anlaşıldığında hukuk kuralları çerçevesinde hak arama yoluna gidilmelidir. Ayrıca tüketici forumlarında ve tartışmalarda açıklamalar ile başkalarına yardımcı olmak ve tüketici hakları koruma örgütlerine de firma ile ilgili şikayette bulunmak etkili olacaktır.

VI. SONUÇ

Ülkelerin öncelikle hukuk sistemlerinde ve suç ceza tanımlarında düzenleme yapmalarına gereksinim vardır. Bu düzenleme, ülke içinden ve dışından ihlalleri ayrı ayrı değerlendiren bakış açıları içermelidir. Evrensel değerlerin korunması için yine evrensel anlamda hukuksal birliktelik ile sağlanacak bir "Siber Hukuk Normları" na olan ihtiyaç her geçen gün artmaktadır. Sadece İnternet ve bilgisayar yoluyla işlenen suçlarla ilgilenen bir güvenlik birimi ve mahkeme henüz bulunmamakla birlikte, bu tür birimlerin olması gerektiğini söylemek artık ütopik bir düşünce değildir.

İnternet üzerindeki bilgiyi "paylaşan" ve "paylaştıran" gibi iki ayrı hareket noktasına sahip etik sorgulamanın, "paylaştıran" noktasındaki sınırlarını doğru olarak belirlemek "sansür" anlamını taşımayacak şekilde olmalıdır. Genelde "paylaştıran" üzerinde yoğunlaşan etik baskı ve yaptırımlara karşın, "paylaşan" lar için aynı şeyler söz konusu olmamaktadır. Çünkü bilgiyi paylaşanların kimler olduğunu tespit etmek neredeyse mümkün değildir. Bu, "paylaşan" ın herhangi bir sorumluluk almadığı anlamına gelmez. Kurallara uygun bir bilgisayar denetlemesinde lisansını belirtemediği illegal yollarla elde edilmiş program veya telif bedelini ödemeyerek elde ettiği bir fikir ve sanat eserini bilgisayarında bulunduranın da cezai sorumluluktan kaçamayacağı açıktır.

Etik ihlallerden bazılarının nedeni olan programlardaki güvenlik açıkların giderilmesi ile olumsuzluklar en aza indirilebilir ancak tamamen ortadan kaldırılamaz. Çünkü program kaynak kodlarının o ana kadarki saldırıları karşılayabilecek durumda olması yeni gelişen saldırı teknikleri ile karşısında başarılı olmasını engelleyecektir. Sürekli olarak güncellenen ve yama programlarla desteklenen programlar da kısmen başarı sağlayabilecektir.

İnternet'in sürekli geliştiği değiştiği ve yeni teknolojiler ile desteklendiği bir ortamda aynı hızda artan ve şekil değiştiren etik ihlaller her zaman var olacaktır. Bu ihlallere karşı

uygulanacak yaptırımlar geniş bir katılımla ortaya konulmazsa ihlaller var olmaya devam edecektir.

Abstract: Explosive growth in use information systems and almost all parts of life has found out some ethical problems and cyber crimes. This article will provide some of the typical computer crimes and ethical infractions such as hackers, crackers, pornography, viruses and spam mail. This computer-based and information technology (IT) crimes has been recognized as an unlucky side effect of information technology revolution for many years. Many countries do not have laws that deal specifically with computer and IT crimes. The legal solution to such problems is not clear. Computer crimes do occur and it is anticipated that the number of such crimes will grow over the next years.

Kaynaklar

Attaran, Mohsen, Ilja VanLaar (1999), "Privacy and Securit on The Internet: How to Secura Your Personal Information and Company Data", *Information Management & Computer Security,* vol. 7, No: 5.

Chou, David C., David C. Yen, Philip Hong-Lam Cheng (1999), " Cyberspace Security Management", *Industrial Management & Data System,* vol. 99, No: 8.

Evans, M. P. , Staven M. Furnell (2000), "Internet-Based Security Incidents and The Potential for False Alarms", *Internet Research:Electronic Networking Applications and Policy,* vol. 10, Number 3.

Furnell, Steven M., Pelagia Chiliarchaki, Paul S. Dowland (2001), "Securit Analysers: Administrator Assistants or Hacker Helpers?", *Information Management & Computer Security,* vol. 9, No: 2.

Furnell, Staven M., Paul S. Dowland, P. W. Sanders (1999), "Dissecting the "Hacker Manifesto"", *Information Management & Computer Security,* vol. 7, No:2.

Hannabuss, Stuart (1998), "Information Ethics: a Contemporary Challenge for Professionals and The Community", *Library Review*, vol. 47, Number: 2.

Hannaford, Craig S. (1995). "Can Computer Security Really Make A Difference", *Managerial Auditing Journal,* vol.10, No: 5.

Hopwood, William S. (2000), "Security in A Web-Based Environment", *Managerial Finance,* Barmarick Publications, vol. 26, No: 11.

Jackson, Anita, Ray DeCormier (1999), "E-mail Survey Response Rate: Targeting Increases Response", *Marketing Intelligence & Planning,* vol. 17, No: 3.

Kramerae Cheris, Jana Kramer (1995), "Legal Snarls for Women in Cyberspace", *Internet Research:Electronic Networking Applications and Policy,* vol. 5, Number:2.

Kwok, Lam-For, Dennis Longley (1999), "Information Security Management and Modelling", *Information Management & Computer Security,* vol. 7, No: 1.

Lang, Josephine Chinying (2001), "Management of Intellectual Property Rights Strategic Patenting", *Journal of Intellectual Capital*, vol. 2, No: 1.

Sanderson, Ethan, Karen A. Forcht (1996), "Information Security in Bussiness Environments", *Information Management & Computer Security,* vol. 4, No: 1.

Scheuermann, Larry, Gary Taylor (1997), "Netiquette", *Internet Research:Electronic Networking Applications and Policy,* vol. 7, Number: 4.

Schneier, Bruce (1998), "Security Pitfallas in Cryptografic Design", *Information Management & Computer Security,* vol. 6, No: 3.

Thomas, Daphyne Saunders (1997), "Cyberspace Pornography:Problems With Enforcement", *Internet Research:Electronic Networking Applications and Policy,* vol. 7, Number: 3.