

## ELEKTRONİK UZAYDA SUÇ VE CEZA

Dr. S. Serap Kurbanoglu (\*)

### GİRİŞ

Son zamanlarda günlük gazetelerde yer alan haberlerin içeriğinde bazı değişiklikler oldu. 18 Şubat 1995 tarihli Yeni Yüzyıl gazetesinden bir haber başlığı: "*Bilgisayar sığıpı yakalandı: ABD'de NASA, Pentagon ve büyük şirketlerin başbelası bilgi hırsızı ele geçirildi*". Haber aynen şöyle:

"... Hakkında ulusal telefon ağlarına girmek, resmi dairelerin, büyük şirketlerin ve üniversitelerin sistemlerini tahrip etmek ve kredi kartlarının şifrelerini çalmak gibi suçlamalar bulunan Kevin Mitnick .... yakayı ele verdi... Mitnick, dün mahkemeye çıkarılarak hakkında suç bildirimi yapıldı. Mahkeme sonucunda işlediği suçlar sabit görülmüşse bilgi hırsızı 55 yıla kadar hapis ve 500 bin dolar (20 milyar lira) para cezası ödemeye mahkum olabilecek... Bilgisayar delisini tanıyanlara göre bilgi hırsızlığının asıl amacı, teknik becerisinin sistemleri korumakla görevli olanlardan daha iyi olduğunu göstermek..." (s: 14).

Haberde ayrıca Mitnick'in ABD'de iki büyük şirketin sistemlerine izinsiz girmekten daha önce bir yıl hapse mahkum edildiği, mahkemede avukatı tarafından bilgisayarlara psikolojik saplantısı olduğu kanıtlandığı için bağımlılık bozukluklarıyla ilgilenen bir tedavi merkezinde 6 ay geçirdiği, bu süre boyunca bilgisayar kullanımının yasaklandığı ve aynı koşulla serbest bırakıldığı anlatılıyor.

Aynı gazetenin 19 Şubat 1995 tarihli sayısında da benzer bir haber var. Bu defa başlık: "*Enformasyon çağının Robin Hoodları*". Burada da

(\*) Hacettepe Üniversitesi Edebiyat Fakültesi Kütüphanecilik Bölümü.

yine ABD'de çeşitli şirketlerin bilgisayarlarına izinsiz giren ve bu suçtan dolayı 1993 yılında yargılanıp hapse giren bir gruptan söz ediliyor. Suçluların hapse girmesiyle ilgili paragraf şu cümle ile son buluyor: *"...Elektronik uzayın demir parmaklıkları da bu kararla kurulmuş oldu"* (s: 11).

Benzer fakat biraz daha farklı alanda Türkiye'de cereyan eden bir davanın öyküsünü de Hülya Küçükaras Bilişim Dergisi'nde kaleme almış. Yazının kaleme alındığı tarihte (Ekim 1993) dava henüz sonuçlanmamıştı. Aradan geçen zaman zarfında çözümlenmiş midir bilemiyoruz. Küçükaras'ın yazıda davanın çıkmazını vurguladığı kısım trajik-komik öyküyü de özetler nitelikte:

*"...bu olay 'yok'lar üzerine kurulu; belgeleri olmayan davanın yokları 'var'larından çok daha fazla: davacı davalıdan program yazmasını istememiş, ama davalı kendi kendine program yazmış; yazılması istenmeyen programları davalı da davacı da sahiplenmiş ama telif hakları zaten hak getire! Bu da yetmemiş yazılması istenmeyen, ama yazılmış olan sahipsiz programlar kullanıcılara satılmış, ama satıldığına ve alındığına ilişkin sözleşmeler olmadığından programlar aslında satılmamış; ancak yazılmayan ve satılmayan programları kullananlara bakım hizmeti verilmiş ve bunun sonucunda programlar çalışmamış!...Eh, yazılmayan ve satılmayan programlar için bu dava boyunca duyulabilecek en mantıklı cümle de bu: 'ÇALIŞMIYOR'" (ss: 154-155).*

Küçükaras'ın olayı özetlediği cümle de burada tekrarlanmaya değer: *"...suç tanımsız, suçlu belirsiz, bilirkişi de zaten cezasını çekti..."*

Belirlenmesi ve ispatlanması zor suçlar, belirlenmesi ve yakalanması zor suçlular, bu tür suçları kapsamayan yasalar, yasalardaki boşlukları kullananlar, fazla tanımadıkları bir alanın sorunlarıyla karşı karşıya kalan hukukçular. Bilgi çağında elektronik bilginin doğasından kaynaklanan ve gelişen teknolojinin bir sonucu olarak ortaya çıkan ahlaksal sorunlar.

## Bilgi Çağında Bilgi Teknolojisi ile Ortaya Çıkan Ahlaksal Sorunlar

Bilgi çağına geçişi sağlayan teknolojik gelişmeler hayatımızı kolaylaştırmaya devam ederken bazı problemlerle karşılaşmamıza da neden oluyor. Kimisi suç unsuru teşkil eden bu problemleri bilgi çağında ahlaksal sorunlar başlığı altında incelemek mümkün.

### Kişisel Bilginin Mahremiyeti

Kişisel bilginin mahremiyeti herkesi ilgilendiren bir konudur. Günümüzde pek çok kişi bilgisayara dayalı kayıt tutma sistemlerinin kişisel bilginin ortaya çıkarılması konusunda çok fazla fırsat yarattığından korkmaktadır. Bu korkular çok da yersiz değil aslında. Örneğin, kredi kartı kullananlar farkında bile olmadan kişilikleri ve özel yaşantıları ile ilgili pek çok ipucu bırakmaktalar. Kredi kartı kullanımı ile ilgili tüm tarihler ve yerler kaydedilmektedir. Kredi kartınızı bir restoranda, benzin istasyonunda, alışveriş merkezinde kullandığınız zaman aslında yemek yediğiniz restoranlar, alışveriş ettiğiniz mağazalar ile yaşam tarzınız ve seçimleriniz konusunda pek çok ipucu veriyorsunuz. Aynı durum kütüphane kullanımında da ortaya çıkmaktadır. Kütüphaneden ödünç aldığınız kitaplar sizin zevkleriniz, ilgili alanlarınız, hobileriniz ve hatta siyasi görüşleriniz hakkında ipuçları vermektedir. Bu tür kayıtları inceleyen bir kişi sizin hakkınızda çok özel bilgilere sahip olabilir. Başka bir örnek vermek gerekirse; yaptığınız tüm telefon konuşmalarının tarihi, süresi ve aradığınız numaraların kayıtları tutulmaktadır. Yine bilgisayarlar aracılığı ile aradığınız numaraları kontrol edip kimin adına kayıtlı olduklarını bulmak mümkün. Böylelikle her telefon açışınızda siz aslında özel yaşamınızla ilgili ipuçları bırakıyorsunuz.

İnanılmayacak kadar büyük miktarlarda kişisel veri değişik amaçlarla değişik veri tabanlarında tutuluyor. Nüfus kayıtları, üniversite-

okul kayıtları, kredi kayıtları, hastane kayıtları, kütüphane kayıtları, sigorta kayıtları, vergi kayıtları, tapu kayıtları, mahkeme kayıtları, dernek kayıtları, özlük hakları kayıtları, banka kayıtları vs. vs.. The United States Congress' Privacy Protection Commission'un tahminlerine göre ABD'de her vatandaşın farklı veri tabanlarında ortalama 17 değişik kaydı var (Mason, 1986; 7). Ülkemizde de bilgisayar kullanımı yaygınlaştıkça elektronik ortamda bulunan kişisel kayıtların sayısı gün geçtikçe artmakta.

Hakkımızda tutulan tüm bu kayıtların doğru ve güncel olmasını diliyoruz. Ne yazık ki bu her zaman mümkün değil. Nerelerde ne tür kayıtlarımız olduğunu tam olarak bilsek bile yasalar her zaman için bu kayıtları görmemize ve düzeltilmesi veya güncelleştirilmesi için girişimde bulunmamıza olanak tanımıyorlar. Doğru olduğu sürece farklı yerlerde farklı kayıtlarınız olmasına itiraz etmeyebilirsiniz. Fakat tüm bu kayıtların sizin haberiniz ve izniniz olmadan biraraya getirilmesini (ki elektronik ortamdaki bilgiler için bugünkü teknoloji ile bu çok kolay) onaylamayabilirsiniz. Bunu yapan kişi belki de hakkınızda sizden fazla şey biliyor duruma gelecektir (!) ki bu da kişi haklarına tecavüzdür.

Kişisel bilgi içeren farklı veri tabanlarının karşılaştırılması sonucu bir kişi hakkında çok yönlü bilgi elde etmek de mümkün olabiliyor. Yine ABD'de vergi kaçakçılarını yakalamak için bu yöntemin kullanıldığı oluyor. The Internal Revenue Service bu yöntemi kullanarak kişilerin yaşadıkları muhit, kullandıkları araba vs. gibi konularda topladığı bilgiler ile bir yaşam standardı profili çıkartıp bunu söz konusu kişiler tarafından devlete bildirilen vergiye tabi gelir ile karşılaştırıyor. Gelir düzeyi ile yaşam standardı profili birbirini tutmazsa kişinin hesapları gözden geçiriliyor.

Kişisel bilginin mahremiyetinin ihlali ihtimali her zaman için mevcut. Önemli olan ihlalin gerçekleşip gerçekleşmediği ve kişisel bilginin kötü amaçlı kullanılıp kullanılmadığı. Bugün ABD'de şahsa ait bilgileri

-att oldukları şahıslardan izin alma gereğini duymadan- satan bir takım kuruluşlar türemiştir. Örneğin, herkese açık olan tapu kayıtlarını tüm eyaletlerde inceleyip yeni ev satın alanların isim ve adresleriyle bir veri tabanı oluşturan ve bu veri tabanındaki bilgiyi kendilerine yeni müşteriler arayan sigorta şirketlerine, tamir ve boya işi yapan şirketlere, mobilyacılara, avukatlara, doktorlara, oy toplamak için çaba gösteren Kongre üyelerine satan şirketler vardır. Bu tip durumlarda listede yer alan herkes isteği ve kontrolü dışında ticari hedef haline gelmektedir (Long, 1991:347-348).

Kişisel bilginin kazanç amacıyla veya kötü amaçlı kullanımı giderek artıyor. Bunun da başlıca nedeni yasaların yetersizliği ve hukukçuların henüz konuya aşina olmamaları sonucu kişisel bilginin mahremiyetinin ihlali eyleminin genellikle cezasız kalmasıdır.

Yukarıda verilen örnekler elektronik ortamda bulunan bilginin güvende olmadığı kuşkusunu yaratsa da bilgisayar uzmanları kişisel bilgilerin veri tabanlarında, dosya dolaplarında olduğundan daha emniyette olduğunu savunuyorlar. Ve eğer uygun koruma tedbirleri alınırsa bilginin amaç dışı ve kötüye kullanımı engellenebilir diyolarlar.

Kişisel hakların ihlali kapsamında tartışılan bir diğer uygulama da bilgisayarlarla izlemedir. Burada bilgisayarlar çalışanların iş performanslarını ölçmek ve değerlendirmek amacıyla sürekli veri topluyorlar. Ana bilgisayara bağlı terminaller veya PC'lerle veya bir bilgisayara bağlı herhangi bir elektronik veya mekanik ekipmanla çalışan 7 milyonun üzerinde Amerikan işçisinin performansı bu yöntemle ölçülüyor. Terminalde harcanan zaman, yapılan hata oranları, çalışanların telefon kullanma sıklığı vs. değerlendirme ölçütlerinden bir kısmını oluşturuyor (Long, 1991: 349). Her dakika izlendiğini bilmenin çalışanlar üzerinde yarattığı olumsuz etkileri ise burada ayrıca vurgulamaya gerek görmüyoruz.

### Bilginin Doğruluğu

Doğru olmayan bilgi insanların hayatını umulmadık derecede etkilemektedir. Yazılı bilgi kadar elektronik ortamdaki bilginin doğruluğu da önemli. Kuşkusuz yazılı bilginin elektronik ortama aktarılması aşamasında çok büyük özen ve dikkat göstermek gerekiyor. Bilginin hatalı olması kadar bilgisayar sistemlerine girdi verirken ve çıktı alınırken yapılan hatalar da insanların yaşamını güçleştiriyor. Tüm bunlara 'bilgisayar hata yapmaz, bu bilgi kesinlikle doğru' şeklindeki yaygın yaklaşımı da eklersek durum iyice güçleşiyor.

Mason'un (1986: 7-8) kaleme aldığı gerçek bir hikaye durumun vahametini göstermek için iyi bir örnek. 1950'lerde Los Angeles'de uzun vadeli banka kredisi ile ev satın alan göçmen işçi çift 1980'lerde kredi aldıkları banka otomasyona geçene kadar hiç bir problemle karşılaşmadan aylık ödemelerini düzenli yapıyorlar. Otomasyona geçiş sırasında yapılan bir hata sonucu bir aylık ödemeyi yapmadı görünen çift ellerindeki damgalı ödendi dekontuna rağmen banka yetkililerini ikna edemiyorlar ve bir önceki ödemeyi yapmadıkları için her ay o ayın ödemesini yapamadan bankadan ayrılmak zorunda kalıyorlar. Ödemeler yapılmadığı için bankanın eve haciz koymaya karar vermesi üzerine yeni kalp ameliyatı geçirmiş olan evin hanımı felç geçiriyor. Sonunda olay mahkemede göçmen çiftin lehine sonuçlanıyor. Banka yaptığı hatadan ve hatanın sonuçlarından dolayı tazminat ödemek zorunda kalıyor. Taksitleri ödenmiş bir arabaya kayıtlardaki hata yüzünden haciz konulmasının Long (1991: 358) tarafından kaleme alınan hikayesi de benzer bir hikaye. Bu olayda da araba satıcısı firma tazminat ödemek durumunda kalmış. Mahkemede suç bilgisayara yüklenmek istenmiş; fakat yargıç, veriler bilgisayara insanlar tarafından girildiği için firmayı suçlu bulmuş.

Bilginin doğruluğunun önemi ölüm kalım durumlarında daha çok ortaya çıkıyor. 1980 yılında hava durumu raporlarının hortum tehlikesi olmadığını garanti etmeleri üzerine Georges Bank'tan denize açıl-

lip hortumda hayatını kaybeden Amerikalı denizcinin hikayesi iyi bir örnek. Bu vakada da mahkeme denizcinin eşine tazminat ödenmesine karar vermiş (Mason, 1986: 8).

Bu örneklerle vurgulamak istediğimiz nokta gelişen teknolojinin de etkisiyle giderek daha fazla bilgi toplayıp depoladığımız bu çağda bilgilerde hata yapılması olasılığının da varolduğuna dikkati çekmek ve hataların çok ciddi sonuçlar doğurabileceğini vurgulamak. Bilgi çağında bilginin güvenliği kadar doğruluğunu sağlamak da bizim sorumluluğumuzda.

Bilginin doğruluğunu sağlamak ve kişisel bilginin ihlaline engel olabilmek için çeşitli öneriler sunuluyor: Elektronik ortamda gizli bilgi bulundurmamak (burada elektronik olmayan ortamdaki gizli bilginin ne kadar güvende olduğu sorunu ortaya çıkıyor), sadece gerekli kişilerle ilgili gerektiği kadar, tam ve doğru bilgi depolamak, gereksiz bilgiyi hemen ortadan kaldırmak (çünkü ne amaçla kim tarafından kullanılacağı belli olmaz), kişilere kendileriyle ilgili bilgileri görme ve güncelleştirme olanağı tanımak, bilgi hangi amaçla toplandıysa sadece o amaçla kullanmak, yetkisi ve izni olmayan kişilerin bu bilgilere erişmesini ve kullanmasını çeşitli yöntemlerle engellemek.

### Bilişim Suçları

Ülkemizde yaygın kullanılan terimiyle 'bilişim suçları' nı ifade etmek amacıyla farklı ülkelerde farklı terimler kullanılmaktadır: Bilgisayar suçları, bilgisayar ile ilgili suçlar, bilgisayarın kötüye kullanılması, bilgisayar yardımıyla işlenen suçlar, elektronik suçlar bunlardan sadece birkaçı.

Bilişim suçları için çok çeşitli tanımlar yapılmış ve bu tanımlarda farklı noktalara değinilmiştir. Aydın'ın (1993: 73-74) literatürde yapılmış tanımları incelemesi sonucu kaleme aldığı tanımlardan birisine göre bilişim suçu, otomatik işlem ve/veya veri transferi ile ilgili her

türlü gayrimeşru davranıştır. Diğer bir tanıma göre ise gerçekleşmesi için bilgisayar teknolojisinin kullanılması esas olan her türlü gayrimeşru hareket bilişim suçudur.

Sonuçta elektronik bilgi ve programlarla ilgili tüm gayrimeşru fiiller bilişim suçu kapsamına girmektedir. Bilişim suçunu diğer suçlardan ayıran özellik burada suçun işlenmesi için bilgisayarın kullanılmasıdır. Bu da failin suçu işleyebilmesi için suçun mahiyetine göre iyi veya kötü bilgisayar kullanabilmesini gerektirir.

Bilişim suçları çeşitlilik gösterir. Bu çeşitlilikten yola çıkarak bilişim suçlarını sınıflamaya çalışanlar olmuştur. Bu konudaki yaklaşımlardan birisi şöyle: Enformatik hile (girdi, işlem ve/veya çıktıya kasıtlı, çıkar amaçlı müdahale), bilgi hırsızlığı (bilgi casusluğu, gizliliğin ihlali), yazılım hırsızlığı, sabotaj (Aydın, 1993: 74).

Bir diğer sınıflama yaklaşımı da şöyle: 1) Truva atları, virüsler ve mantık bombaları ile bilgisayarın içinde tahribe sebep olan suçlar. 2) Kişisel kazanç için bir bilgisayar sistemine yasal olmayan erişim yoluyla zimmete para geçirmek ve sahtekarlık gibi bilgisayar sistemleri ve verilerinin manipulasyonunu içeren suçlar. 3) Yasal olmayan bilgisayarlı bilgi servisleri (bulletin board), elektronik posta veya telefon sistemlerinin kötüye kullanımı, uzakiletişim yoluyla herhangi bir bilgisayar sistemine izinsiz erişim gibi uzakiletişim ağları kullanılarak işlenen suçlar. 4) Kişisel bilginin kötüye kullanımı ile ilgili suçlar. 5) ihmalkarlık sonucu işlenen suçlar. 6) Uyuşturucu dağıtımını destekleyen veri tabanları veya para aklama gibi suç teşebbüslerini destekleyen suçlar. 7) Yazılım hırsızlığı ve telif haklarının ihlali ile ilgili suçlar (Long, 1991: 350).

Kişisel kazanç elde etmek amacıyla işlenen bilişim suçlarına gerçek hayattan pek çok örnek vermek mümkün. Yazımızın başında örneklerini verdiğimiz gazete haberleri bu tip suçlarla ilgili. Zimmete para geçirme ve yazılım hırsızlığı en sık rastlanan örnekler. ABD'de bilgi-

sayar yolu ile kendi adına 160 bin dolarlık çek düzenleyen bir gümrük memuru ile AT&T bilgisayarlarına girip 1 milyon dolar değerinde yazılım çalanı 13 yaşındaki bir ortaokul öğrencisi sadece iki örnek.

Tahminlere göre bilişim suçları sonucunda kaybedilen para her tür soygunda kaybedilenden fazla. Aslında kimse bu işin gerçek boyutlarını bilmiyor. Çünkü bilişim suçlarının çoğu ya belirlenememiş ya da rapor edilmemiş oluyor. Özellikle bankalar müşterilerinin güvenini kaybetmektense genellikle kayıplarını sineye çekip ikinci yolu tercih edenler arasında (Long, 1991: 351).

Daha önce de vurguladığımız gibi bilişim suçu tecrübeli bir bilgisayar uzmanının yardımını gerektiren bir suç türü. Kuşkusuz sokak hırsızlarının çoğu bu bilgiden yoksun. Fakat tabii ki suçun belli bir eğitim düzeyi gerektirmesi suçu suç olmaktan çıkartmıyor.

Bilişim suçu nispeten yeni bir suç türü. Dolayısıyla yasal düzenlemeler henüz bu suçlarla başa çıkabilecek ölçüde geliştirilmiş değil. Hangi ülkede kaç polis, kaç hukukçu bu tür vakaları inceleyebilecek düzeyde bilgisayar teknolojisine hakim?

Yerel bankaların sistemlerinden, ulusal düzeyde çok gizli savunma sistemlerine kadar hemen her tür sisteme izinsiz girebilenler sadece bununla da kalmayıp bazen girdikleri sisteme virüs bulaştırmak yoluyla kasıtlı zarar da verebiliyorlar. Sistemdeki programları etkileyen ve bir sistemden diğerine atlayabilen virüslerin çok değişik derecelerde hasara sebep olabilen farklı türleri mevcut. Kazancın söz konusu olmadığı ve tek amacın zarar vermeye yönelik olduğu bu eylemleri terörizm olarak adlandıranlar da var.

### **Bilginin Mülkiyeti: Telif Hakları ve Yazılım Hırsızlığı**

Toplum olarak karşılaştığımız en karmaşık sorunlardan birisi de telif haklarıdır. Bilgi bir kez üretildikten sonra yeniden üretilmesi,

kopyalanması ve paylaşılması kolaydır. Söz konusu kopyalama orijinale zarar verilmeden gerçekleştirilebilir. Bu da bilginin bir mülk olarak korunmasını güçleştirir. Bilginin iletilebilir olma özelliği kişiye bağlı kalmasını ve başkaları tarafından istek dışı kullanılmasını engellemeyi zorlaştırır. Bu yüzden hemen her ülkede fikir ve sanat ürünlerini korumak amacıyla bir takım patent ve telif hakkı yasaları geliştirilmiştir.

Teknoloji geliştikçe fikir ve sanat ürünlerinin kapsamı genişlemekte, fikir ve sanat ürünlerinin üzerine kaydedildiği ortamlar da çeşitlilik göstermekte. Yeni teknolojiler bilginin depolanması, kopyalanması, ihtiyaca göre yepyeni şekillere sokulması konusunda neredeyse sınırsız imkanlar tanıyor. Bu durum söz konusu elektronik bilginin hak sahiplerini tehdit eden bir sürü problemi de beraberinde getiriyor. Gerçekte kopyalamadaki kolaylık problemi büyütmekte. Öyle ki kopyaların kalitesi kaçınıcı kopya olduğunun anlaşılmasını bile engellemekte. Kolaylık ve kalite bir araya gelince izinsiz kopyalamaya karşı eğilim artıyor ki aslında kopyalama eyleminin kontrol edilmesi yani elektronik ortamdaki bilginin de korunması lazım.

Üzerinde durulması gereken noktalardan birisi de koruma kavramının yanlış anlaşılması gerektiğidir. *"Koruma ile kullanımın engellenmesi değil kullanımın kontrolü anlaşılmalıdır yoksa şu veya bu formda eser üretmek anlamsız olurdu"* diyor Cornish (1993: 16). Bir eseri yayınlamak ise zaten onu herkesçe elde edilebilir hale getirmek anlamına gelmektedir. Tabii bu da eser sahibinin başka bir deyişle hak sahibinin hakları çığnenebilir anlamına gelmiyor. Gelişen teknolojinin ışığında eser sahibinin eser üzerindeki kontrolünün şu hususları kapsamaması bekleniyor; kağıttan kağıda kopya, kağıttan elektronik ortama kopya, elektronik ortamdan kağıda kopya ve elektronik ortamdan elektronik ortama kopya (Cornish, 1993: 16).

