Marmara İletişim Dergisi, Sayı: 1, Aralık 1992

BİLİŞİM SİSTEMLERİNDE, GÜVENLİK, GÜVENİRLİK, MAHREMİYET VE BİLİŞİM SUÇLARI

Yrd.Doç.Dr. Emin Doğan AYDIN
Marmara Üniversitesi
İletişim Fakültesi

1. GİRİŞ

Bilişim suçu son yıllarda kriminologların, hukukçuların, bilişim uzmanlarının ve bilgisayar kullanıcılarının giderek daha fazla ilgisini çekmektedir.

Ancak, bilişim suçu olgusunun sınırlarının belirlenmesinde ve tanımlanmasında belirsizlikler bulunmaktadır. Kriminolojide bilişim suçuna ne gibi bir önem verilmelidir? Bu suçlar ciddi bir sosyal sorun mu, oluşturmaktadır yoksa, bu soruna pek fazla önem verilmemeli midir?

Fenomenolojik özelliği olan diğer bir tartışmalı soru da bilişim suçunun mülkiyete karşı işlenmiş geleneksel bir suç olarak mı yoksa yeni bir kriminal olgu olarak mı kabul edilmesi gerektiğidir. Bu soruya verilecek cevap suçun önlenmesi ve ceza politikasının belirli sonuçlarını içermektedir. Burada sadece, **Bilişim suçunun başlangıcı, fırsat yapısı ve tanımı** ile ilgili teorik konulara yer verilmektedir.

2. BİLİŞİM SUÇUNUN BAŞLANGICI VE FIRSAT YAPISI(*)

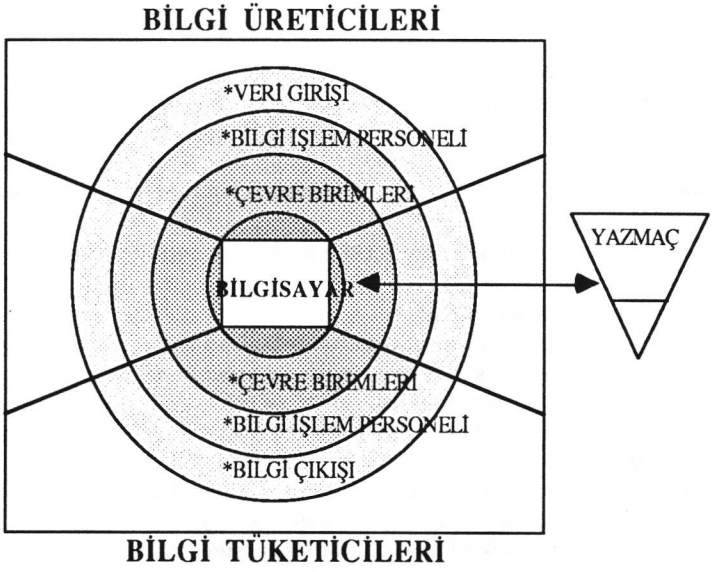
2.1. Teknik kavramlar

2.1.1. Bilişim (Informatics) aşağıda belirtilen alanları içeren bilim ve teknoloji olarak tanımlanmaktadır; Bilginin ve iletişim yapısının ve özelliklerinin; bilginin aktarılması, organize edilmesi, saklanması, tekrar elde edilmesi, değerlendirilmesi ve dağıtımı için gerekli kuram ve yöntemler ve öte yandan da; bilgiyi kaynağından alıp kullanıcıya aktaran ve genel sistem bilimi, sibernetik, otomasyon ile insanın çalışma çevrelerindeki yerinde ve zamanında kullanılan teknolojileri temel olarak alan bilgi sistemleri, şebekeleri, işlevleri, süreçleri ve etkinlikleridir. (Aydın, E.D., 1984 s. 256) Kısacası, bu bilim ve teknoloji dalı bir veri işlem sürecidir. Buradaki **veri** (Aydın, E.D., 1984 s. 112) deyimi ile kesin ve formal biçimde, yani, sayılar, harfler veya diğer tipografik karakterlerle (virgül, tire vs.) ifade edilen isimler, adresler, tarihler, tutarlar, araştırma değişkenleri vs. kastedilmektedir. **Bilgi** (Aydın, E.D., 1984 S. 256) ise, alıcı için bir anlam oluşturacak şekilde derlenmekte ve sunulmaktadır.

(*) Fırsat yapısı suçu teşvik edici faktörler kompleksi olarak kabul edilebilir. Bu yapı olmaksızın yasaklanan eylemlerin yapılması çok daha zor olur ve hatta bazı hallerde ortada suç fırsatı dahi olmaz.

Veri işlem (Aydın, E.D., 1984 s. 118) belirli verilerin toplanması, çıkarılması, çarpılması ve bölünmesini ifade eder. Bu kavram işlem için özel yardımcı araçlardan yararlanılıp yararlanılmadığına bakılmaksızın kullanılmaktadır. Bir markette yapılan alımların listesini çıkarttığımızda bilgi işlem yapmış oluruz. İş yerlerinde, devlet kurumlarında ve diğer kuruluşlarda idari işlerin büyük bir kısmı, bordrolar, muhasebe defterleri, faturalar, irsaliyeler, banka işlemleri, istatistikler gibi verilerin saklanması, çağırılması ve işlenmesinden ibarettir. Veriler elle veya bir makine aracılığı ile işlenebilir. Bilgi işlem için bilgisayar kullanıldığı taktirde elektronik bilgi işlem (EBİ) söz konusu olmaktadır.

Bir bilgi işlem sistemi olan EBİ sistemi temel verilerin önceden belirlenen kurallar çerçevesinde elle yapılan/manuel veya bilgisayarlı bir yordam serisindeki değerli bilgilere çevrilmesi için insanlar ile bilgi işlem donanımı arasındaki kombinasyondur (Şekil 1).



Şekil 1 - Basit bir EBİ sistemine örnek

Bilgisayarın elle yapılan/manuel bilgi işlem sistemlerine olan üstünlüğü, süratinde, yorulmazlığında ve doğruluğunda yatmaktadır.

Bir bilgisayar aşağıda yer alan varsayımlar çerçevesinde hızla hesaplama ve işlem yapabilir, bilgi depolayabilir, (Aydın, E.D., 1988 s. 23-24) veri aktarabilir.

- Bilgisayar tarafından yapılacak her görev alt problemlerden ve her biri sadece "evet" veya "hayır" olmak üzere iki şekilde cevaplandırılacak küçük sorulardan oluşan mantıksal serilere bölünmektedir.

- Bilgisayar tarafından alınan bütün emirler ve bilgisayara yüklenen bütün veriler sadece 1 ve/veya 0 olmak üzere iki sembolü içeren sembolik bir dile çevrilmektedir. (Aydın, E.D., 1988 s. 36-39)

- Bilgisayar ne yapacağı ve bunu nasıl yapacağı hakkında çok kesin açıklamalar (emirler/"komut"lar) almaktadır. Bu açıklama (bu komutlar topluluğuna da program diyebiliriz) programla verilmektedir. (Aydın, E.D., 1984 s. 56-60)

Bu şartlar sağlandığı taktirde, bilgisayar teknolojisi teorik olarak sanayi, ticaret, yönetim ve bilim alanlarında bir çok amaç için kullanılabilir.

2.1.2. Bilgisayarın gelişimi genellikle otomobilin gelişimine benzer. Henry Ford ilk otomobilini yaptığı zaman bunun geleceği olacağı sanılmıyordu. Tartışılan önemli konulardan biri üzerinde otomobil sürmeye elverişli yollar bulunmamasıydı. ABD'de 1952 yılında her biri 1 milyon Dolar değerinde (paranın bugünkü değeri ile yaklaşık 12 milyon Dolar) birkaç bilgisayar bulunmaktaydı. (1946'daki dünyanın ilk sayısal bilgisayarı "ENIAC" 30 ton ağırlığında ve 18000 vakum tüpünden oluşuyordu) (Aydın, E.D., 1989 s. 11-12)· Her bilgisayar 20x10 m.lik bir alana gerek duyuluyor ve 100.000 kişiden sadece bir tanesi bunların ne için kullanılabileceğini biliyordu. O tarihlerde on bilgisayarın mevcut bütün EBİ problemlerini çözebileceğini düşünen uzmanlar bile vardı.

Ancak, bilgisayar alanındaki teknolojik gelişme çok hızlı olmuş ve artık bilgisayarlar pahalı olmaktan çıkmış ve daha kolay kullanılır hale gelmiştir. Bugün birkaç yüz Liralık programlanabilir bir hesap makinası/kalkülatör 1952 yılında 1 milyon Dolar'a mal olan bilgisayarın yerini alabilmektedir. Bugün yıllık cirosu 250-500 milyon TL olan bir firma 5-10 milyon TL karşılığında ihtiyaçlarını karşılayabilecek bir bilgisayar edinebilmektedir.

Bilişim sistemleri artık sınırları çizilebilecek bir teknoloji olmaktan çıkmıştır. Bilişim sistemleri günümüzde hayatın hemen hemen bütün sektörlerinde kullanılmakta ve bilgisayar teknolojisi sadece başlangıç aşamasında bulunmaktadır. Gelecekteki toplumlar günümüzde olduğundan çok daha fazla bilgi işlem yapacaklardır. Bugün insanlar tarafından yapılan birçok iş gelecekte bilgisayarlar tarafından üstlenilebilecektir. Örneğin, bilgisayarlar bir çok işletmede ve sanayi dalında Bilgisayar destekli üretim ve proses kontrol sistemleri ile önemli değişikliklere neden olabilirler. (Aydın, E.D., 1988 s. 95-101)

Küçük çaplı işletmelere adapte edilen küçük ve ucuz bilgisayarlar ile basit

yönetim program paketleri 1980 yılından sonra bir hayli artış göstermiştir. En küçük ve en ucuz olan bilgisayarlar **kişisel bilgisayarlardır.** Bu ad bilgisayarın tek bir kişiyi desteklemek üzere tasarımlanmış olmasından gelmektedir. Bu tür bilgisayarların fiyatı 2 ila 25 milyon TL arasında değişmektedir. Bilgisayar pazarlama şirketleri bu küçük bilgisayarları, evlerinde veya iş yerlerinde muhasebe fatura ödeme ve hesap bakiyelerini vs. kontrol etmek için masa üstü yayımcılık kullanan küçük müşterilere satmaktadırlar.

Bilgisayar dünyasıyla, telekominikasyon dünyalarının evlenmesi, bilgi işlemde telekomünikasyonun ve terminallerin kullanılması giderek artmaktadır. Bu da veri giriş ve çıkışı için kullanılan donanımın merkezi işlem ünitesi ve bellekle fiziksel olarak aynı yerde bulunma zorunluluğunun olmadığını, bunların telekomünikasyon ile birbirlerine bağlanabileceğini ifade eder. (Aydın, E.D., 1989 s. 19) Büyük EBİ kullanıcıları için bu durum fiziksel ve coğrafi olarak birbirlerinden ayrılmış bilgisayarları gelişmiş bilgi iletişim sistemi ile tek bir sistem, yani bir veri şebekesi halinde birbirlerine bağlayabilmesi sonucunu getirmiştir.

Diğer bir olanak sınır ötesi veri akışı'nın telefon veya teleks şebekeleri ile organize edilebilmesidir. Günümüzde, bankalar (Aydın, E.D., 1989 s. 11) (the Society for Worldwide International Fund Transfer - SWIFT) kanalıyla, sigorta şirketleri, otomobil imalatçıları, ilaç şirketleri, seyahat acenteleri, petrol şirketleri ve finansal kiralama sektörü gibi çeşitli sanayi ve ticaret sektörleri arasında uluslararası düzeyde bilgi akışı bulunmaktadır.

Bilişim teknolojisinin gelecekteki diğer uygulamaları, bunların belirli yan etkileri olup olmadığına bakılmaksızın ilginç olabilir. Bunlara örnek olarak: (Aydın, E.D., 1988 s. 95-101)

- Çeşitli mal ve hizmetlerin (gıda ve yatırım mallarından sinema ve tren biletlerine kadar) ev terminalleri aracılığı ile satın alınması.

- Senet ve çek kullanmadan kağıtsız elektronik ödeme işlemleri,

- Yangın ve hırsızlığa karşı denetim,

- Videoteks, uydu TV, elektronik posta gibi yeni iletişim sistemleri,

- Otomobillerde şanzıman, göstergeler, güvenlik ve servis fonksiyonları gibi hemen hemen bütün fonksiyonların harekete geçirilmesinde kullanılan mikrobilgisayarla gösterilebilir. Birçok yeni otomobilde mikrobilgisayarlar, aralarında lastik havası, emniyet kemerleri, hız sınırlaması vs.nin de bulunduğu sistemleri denetlemekte/ denetleyeceklerdir. Bu listeye alkollü kişilerin otomobil kullanmasını engelleyen elektronik alkol testi de bulunmaktadır.

2.2. Bilişim Suçunun Ortaya Çıkışı

2.2.1. Bilişim alanındaki gelişmeler toplumu ve bireyi birçok yönde etkilemektedir. Her teknoloji devriminde olduğu gibi, gelişmenin getirdiği yararların yanısıra birtakım olumsuz etkiler de söz konusu olmaktadır. Örneğin, kimya bilimi çeşitli alanlarda kaydedilen gelişmeye büyük katkılarda bulunmuş ancak bu arada insan ve çevre için zararlı ürünler ortaya çıkmıştır. Motorlu araçlar yaşam tarzımızı, iş yaşamımızı, boş zamanımızı değerlendirme şeklimizi değiştirmiş, ancak bu arada trafik kazaları, alkollü araç kullanma sorunlarını ve çevre kirliliğini beraberinde getirmiştir.

Elektroniğin ve bilişim sistemlerinin insanın durumunu çeşitli şekillerde değiştireceği kabul edilmektedir. Örneğin bilgisayarlar uzmanlaşma eğilimini güçlendirmiş ve bunun sonucunda bügün bir çok iş olağan bir hale gelmiştir. Bu durum bazı kişiler için bir anlamsızlık ve yabancılaşma duygusu yaratmaktadır. Bilişim sistemleri çeşitli resmi fonksiyonları ve etkinlikleri geliştirmiş, ancak aynı zamanda örneğin bilgisayar güvenliği ve kişisel gizlilik gibi konularla ilgili yeni sorunların ortaya çıkmasına neden olmuştur. Büyük miktarda bilgi birikimi ve bilgi işlem bunların zarar görme olanağını da arttırmıştır. Hızlı otomasyonun olumsuz etkileri arasında **Bilişim suçundan** da söz edilmesi gerekmektedir.

2.2.2. Bilişim ile ilgili suçlar altmışlı yılların sonuna kadar bilinmeyen bir olguydu. Bilgisayarlaşmanın yaşamımızda bir parantez açacağı kabul edilmekte ve on kadar bilgisayarın otomatik bilgi işlem ile ilgili olarak mevcut bütün sorunların üstesinden geleceği düşünülmekteydi. Ancak, bilgisayarın yayılma süreci bütün tahminleri alt üst etti. Gelişmeyle birlikte, diğer olumsuz sonuçların yanısıra bilişim ile ilgili suçlar da ortaya çıktı. Bilinen ilk bilişim suçu 18 Ekim 1966 tarihli Minneapolis Tribune'da yayınlanan "Bilgisayar uzmanı banka hesabında tahrifat yapmakla suçlanıyor" başlıklı makale ile kamuoyuna yansıdı. Bu vaka Donn B. Parker'in dikkatini çekti. Parker bu sorunla ilgilenmeye başladı ve bilişim suçu ile ilgili diğer vakaları da ortaya çıkardı (Parker, D.B, 1968). 1970 yılında Stanford Araştırma Enstitüsü'nde "Bilgisayarın Kötüye Kullanılması" adı altında bir proje başlattı. Giderek son yıllarda bilişim suçları; bilgisayar programcıları, sistem programcıları, sistem analistleri, operatörleri, teknisyenleri, bilgisayar üreticileri, bilgisayar kullanıcıları, hukukçular ve suç araştırmacılarının, kısacası tüm bilişim uzmanlarının ve kullanıcılarının ilgisini çekmeye başlamıştır.

2.3. Bilişim sistemlerinin kriminojenik (suç yaratıcı) faktörleri (fırsat yapısı).

2.3.1. Suç amaçlı uygulamalar bilgilerin işlendiği her türlü sistemde olabilir ve olmaktadır. Elle yapılan/manuel işlem sistemlerinde de zimmete geçirme, sahtekarlık, dolandırıcılık ve hırsızlık olayları kaydedilmiştir. Ancak, suç yaratıcı faktörler

sorunun Bilişim sistemine getirilmesinin belli nedenleri vardır. Bunlar dünyada, büyük bir hızla yayılmakla birlikte, halkın büyük bir kesimi tarafından henüz bilinmemektedir. Bu da kişilerin sundukları sonuçlara dayandıklarını ifade eder. Sistemlerde yalnızca kar amaçlı uygulamalara veya diğer bilgisayar suçlarına karşı bazı tedbirler bulunduğuna inanılmaktadır. Başlangıçta, manuel yordamların sayısını azaltmak ve önceden dağıtılmış olan dosyaları ve dokümanları kolaylıkla denetlenebilen bilgisayar tesisine yoğunlaştırmak suretiyle suç oluşturan uygulamaların azaltılabileceği sanılmaktaydı. Ancak, birinci aşamada toplanan bilgilerin yoğunlaştırılmasıyla sağlanan daha büyük orandaki fiziksel koruma **Bilişim sistemlerinin ve terminal işlemlerinin geliştirilmesi aşamasında** kısmen kaybolmuştur.

2.3.2. Bilişim sistemlerinin yaygınlığı ve çalışması hakkında daha yakından inceleme yapıldığında bunların çeşitli suç yaratıcı faktörler içeren bir fırsat yapısı yarattıkları anlaşılmıştır. Bu faktörlerin belirlenmesi suçun önlenmesi için alınacak makro tedbirlerin hareket noktasını oluşturmalıdır;

- Bilgi yoğunlaştırma,
- Kontrol mekanizmasındaki eksiklikler,
- Anonimlik.

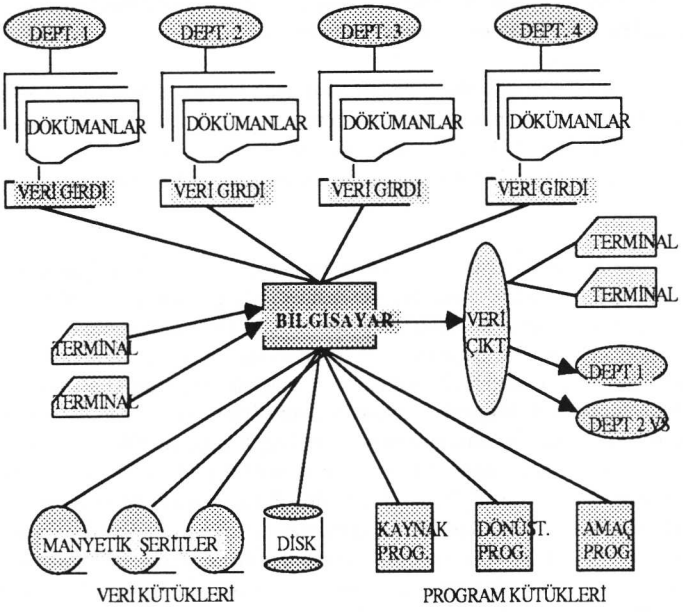
Hukuksal açıdan önemli olan bugünkü bilişim sistemlerinin bazı özellikleri rehber sözcük kullanarak liste şu şekilde şekillendirilebilir:

- Yüksek bilgi işlem hızı,
- Bilgilerin kitlesel olarak saklanabilmesi,
- Bilgi iletişimi, dağıtılmış bilgilerin işlenmesi,
- Esneklik,
- Evrensellik,
- Entegrasyon,
- Bağımlılık
- Formalizasyon,
- Hassaslık,
- Yazılım ve donanım birliği.

2.3.2.1. Bilgisayarlar bilgilerin çok büyük oranda yoğunlaştırılabilmesine imkan sağlar. Büyük sistemlerde bir gün içerisinde onbinlerce hatta yüzbinlerce işlemin yapılması olağandışı bir olay değildir. Aynı zamanda beher gün ve kişi başına yapılan işlem sayısında da artış olmaktadır. Bilişim sistemler de giderek daha karmaşık hale gelmektedir (Şekil 2). Bir şirketin bütün bilgisayar sisteminin tek bir kişi tarafından incelenmesi hemen hemen imkansızdır.

Bilgisayar başlangıçta suç oluşturan uygulamalara karşı daha iyi koruma sağlamıştır. Ancak aynı zamanda çok büyük miktarlarda bilginin tek noktada toplan-

masına izin vermiştir. Manuel sistemlerde birkaç ton kağıt üzerinde saklanabilen bilgiler bilgisayarlı sistemlerde tek bir manyetik bant üzerindeki elektronik karakterlere sıkıştırılabilmektedir. Büyük bilgisayar kullanıcılarından bazıları, örneğin bankalar, şubelerinde yaygın terminal sistemleri kurmuşlardır. Ticari bankaların her birinde yüzlerce terminal bağlantısı bulunmaktadır.



Şekil 2 - Bilişim sisteminde bilgi toplanmasına örnek

Bilişim sistemleri sanayi ve ticaret alanında büyük çapta stok kontrol, muhasebe, dağıtım vs. konularında yardımcı olmak üzere kullanılmaktadır. Bu amaçla bölgesel depolardaki terminaller telefon şebekesi aracılığı ile merkezi bir bilgisayara bağlanmıştır. Depo terminallerinden stokların yenilenmesi için sipariş verilmektedir.

Bilgisayardan üretilen, satın alma listeleri, yapılacak alımlarda olduğu kadar, satış istatistikleri, stok pozisyonları vs. için de esas alınmaktadır. Fatura işlemleri de bilgisayarla yapılmaktadır. Ödemelerin, giderek büyük bir kısmı otomatik banka giro'su ile yapılmaktadır.

Bilgi işlem devlet işlerinde de yaygın olarak kullanılmaktadır. Büyük çaplı bilgi işlem kullanıcıları arasında Sosyal Sigortalar Kurumu (sağlık sigortası ve emeklilik sigortası), PTT İdaresi, Elektrik İdaresi, Hava Yolları, Vergi Daireleri, Mülki

İdareler, Saymanlıklar ve yerel yönetimler (personel ve maaş muhasebesi, sosyal yardımlar vs.).

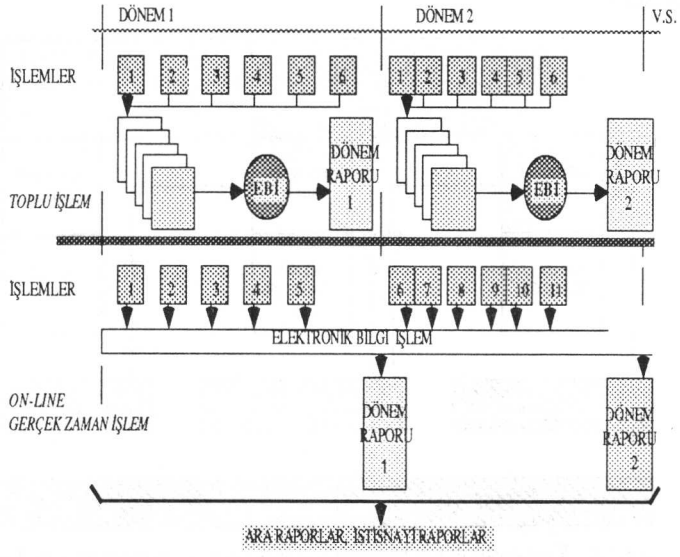
Büyük miktarda bilgi toplanması ve çok sayıda günlük işlem yapılması kontrollarda güçlüklere ve bilgi işlemde fazla miktarda yanlış yapılmasına yol açmaktadır. Bu durum bir fırsat yapısı oluşturmakta ve bilişim sistemlerini kasıtlı hareketlere karşı savunmasız bırakmaktadır.

ABD'de Senatör Abe Rebicoff tarafından bilgisayarların kötüye kullanılması ile ilgili olarak hazırlanan bir rapor bir ankete verilen cevapları sunmaktadır. Ankete katılan 205 kişiden 131'i bilgisayarlardaki yüksek hata düzeyinin yapılması gerekli olan çok miktardaki işlemden kaynaklandığı düşüncesindedir (Resmi İşlemler Komitesi, Birleşik Devletler Senatosu, 1976).

2.3.2.2. Bilgisayar teknolojisi uzmanlaşma ve iş bölümü eğilimini arttırmaktadır. Bilişim sistemleri sonucunda veri kalitesi ile ilgili eski sorumluluk daha büyük sayıda çalışan ve departmanlara dağıtılmaktadır. Bilişim teknolojisindeki uzmanlaşma, gelişme ile işlemler arasında daha kesin bir ayırım ile planlama ve uygulama aşamalarında daha kesin bir iş bölümünden oluşmaktadır. **Bilgiyi işleyenler sonuçta çıkacak bilginin kalitesinden sorumlu değildirler.** Veri sistemine giren bilgiler, muhasebe fişlerinde/kartlarından veya temel bilgileri içeren diğer dokümanlardan tamamen ayrı olarak, "manyetik ortamlarda noktalar" şeklinde kendi varlıklarını sürdürmektedir. (Aydın, E.D., 1988 s. 40-46) Bu durum bilgiler üzerinde suç oluşturacak eylemlerin daha kolaylıkla yapılabilmesini sağlamaktadır. Aynı zamanda, bilişim sistemlerinde aşırı bir kontrol yapısı bulunmamaktadır. Eski manuel sistemde görevi kontrol etmek olan çeşitli personel bulunmaktaydı. Manuel defter tutma sistemi büyük miktarlarda belge içerir ve her kağıt çeşitli memur ve yöneticiler arasında yavaş hareketlerle dolaşır. Tonlarca belgenin elektronik karakterler halinde sıkıştırıldığı bilişim sistemlerinde kontrol görevi yapan personel ve yönetici sayısı azalır.

Bilgisayarlaşmanın başarılı şekilde büyümesi manuel yordamlar ile ilgili olarak benimsenen kontrol yöntemlerinin genellikle elimine edildiğini ve EBİ'me geçişte bunların yerine pek başka bir şey konulmadığını ifade eder. Kullanılmakta olan kontrol yöntemlerinin etkili olmadığı görülmektedir (Mair, Wood & Davis, 1978). Bir bilişim sistemini tasarlamak ve kullanıma sokmak konvansiyonel sistemlere göre çok daha zordur ve daha fazla zaman almaktadır. Manuel sistemlerde bağımsız olarak yapılan muhasebe rutin işlemleri bilişim sistemlerinde tek bir EBİ yordamına indirilmektedir. Hatırda tutulması gereken diğer çok önemli bir fark muhasebe işlemlerinin bilgi işlemin yapıldığı departmanda yapılmasıdır. Veri medyalarına depolanan dosyaların içeriği kağıda dökülünceye kadar okunamaz. İşlemin kontrol edilmesi ve sis-

temin çeşitli bölümlerini uygulanması sorumluluğu genellikle bir çok kişi tarafından paylaşılmaktadır. İşletim sistemleri (Aydın, E.D., 1988 s. 50) ve diğer denetleyici yazılım (kontrol sistemi) hemen hemen tamamen bilgisayar satıcıları veya uzman işletmeler tarafından sağlanmaktadır. Dolayısıyla bu sistemler kullanıcıların kontrolu dışında bulunmaktadır. Burada ciddi olan nokta işletme sistemlerinde hataların farkına varılmadan meydana gelebileceğidir. Güvenilir bir kontrol bulunmamaktadır. Bazı gelişmiş bilişim sistemleri gerçek zamanda (Aydın, E.D., 1989 s. 30-31) çalışır (toplu işleme (Aydın, E.D., 1989 s. 20-21) karşı olarak). Bu da bilgilerin derhal ve sürekli olarak işlendiği anlamına gelmektedir(Şekil3).



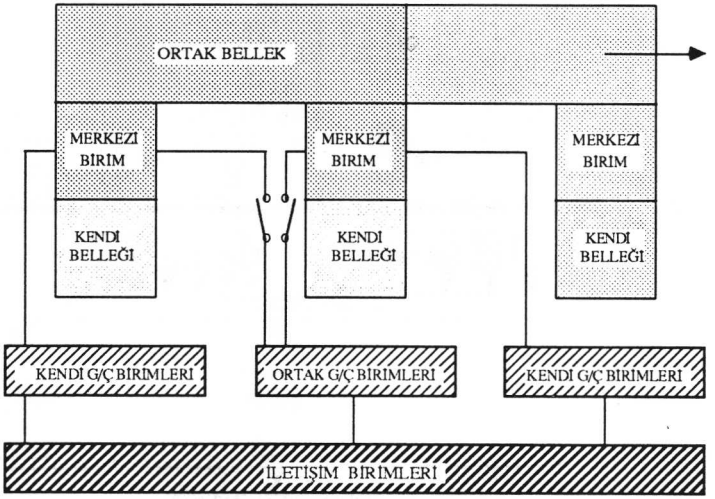
Şekil 3 - İşlemlerin toplu ve gerçek zamanda yapılması

Gerçek zaman sistemleri genellikle çok yönlü işlem yaparlar. Çok yaygın olan bir uygulamada GERÇEK ZAMAN olarak tanımlanan bir terminal aracılığı ile doğrudan, bir bilgisayar sistemi belleğinde saklı belirli program ve bilgi kaynaklarına erişme olanağına sahiptir. Cevaplar daima güncelleştirilmiş bilgiler halinde kaynakta hazırdır. Sisteme gönderilen soru biçimindeki verile doğrudan işleme alınır.

Bir başka anlatımla kullanıcı sorular sorar ve bilgisayar da bunların cevaplarını anında alır. Burada kullanıcı ile sistem arasında bir diyalog söz konusu olduğundan buna ETKİLEŞİM sistem adı verilmektedir. Bilgisayarda saklı program ve bilgi kay-

naklarına birden fazla kullanıcı veri ve komutlar göndererek erişebilir. Bu komutlar yardımıyla başlatılan programlar verileri sırasıyla işleme alır ve sonuç cevaplar halinde kullanıcılara ulaştırılır. Gerçek zamanlı sistemler banka işlerinde, otel ve seyahat rezervasyonlarında, stok yönetiminde vb. kullanılır.

Bir başka uygulama türü olan, SAKLAMA ve GERİ ALMA olarak tanımlanan etkileşimli bir sistemde kullanıcı gönderdiği komutlar yardımıyla bilgisayar sisteminde daha önce saklanmış olan bilgilere erişerek bunları geri alabilir. Veri bankaları, kitaplıklar ve sağlık kuruluşları bu sistemden yararlanırlar. Yani, bilgiler birbirleriyle ilgisi olmayan programlarda aynı anda işlenir (Şekil 4). Bu da kontrolu daha dagüçleştirir.

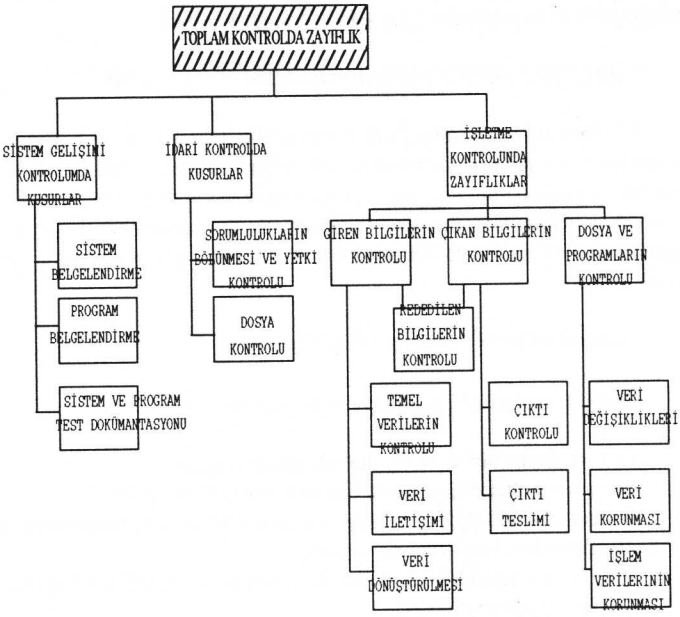


Şekil 4 - Karşılıklı olarak birbirleriyle ilgisi olmayan programlarla bilgilerin çok yönlü işlenmesi

Bilişim sistemine adapte edilebilecek etkin kontrol yöntemlerinin olmaması kasıtlı hareketlerin yapılması riskini arttırmaktadır (Şekil 5).

2.3.2.3. Bir başka kriminojenik unsur bilgisayarların kullanılması ile ilgili anonimitedir. Manuel sistemlerde görevlilerin makbuz imzalaması gerekmektedir. Çok terminalli bilgisayar esaslı sistemlerde ise, yetkililerin kontrollarına rağmen anonimite korunmaktadır. Gerek kurban (mağdur) gerekse kazanılan obje anonimdir. Suçlu kimin malını aldığını bilmemektedir ve kurban (mağdur) ile temas kurmamaktadır. Suçlu açısından kullanılan sadece rakkamlardır ve asıl kurban (mağdur) belirli

bir kişi değil, bilgisayardır. Elde edilen nesnenin anonim olmasının büyük bir psikolojik önlemleri alır. Bugün, veri medyaları üzerine kaydedilmiş sinyaller şeklinde büyük miktarlarda nakit ödeme emirleri üzerinde yapılacak girişimlere karşı özel bir tedbir alınmadan nakledilmektedir.



Şekil 5 - Verilerin kontrol yapısının zayıflığı

2.3.3. Bilişimle ilgili suçların işlenmesi sistemin nasıl fonksiyon gördüğü konusunda bilgiye ve genellikle bilgi işlem konusunda ileri düzeyde eğitime gerek duyar. Bilgi faktörü bir yanda sisteme müdahale edebilecek bilgiye sahip olan kişilerin az sayıda olması bakımından koruyucu bir etkiye sahiptir. Diğer yanda ise, bilgi iki açıdan bir suç oluşturma faktörü olarak kabul edilebilir. Bilişim hakkındaki bilgisini suç oluşturan amaçlar için kullanmaya niyetli olan bir kişi kendi yetenekleri ile diğer görevlilerin yetenekleri arasındaki boşluktan dolayı yakalanma riskinin az olduğunu bilmektedir. Dolayısıyla, Bilişim suçlarını işleyen kişilerin birçoğunun Bilişim sisteminde çalışan kişiler olması bir rastlantı değildir. Bu yetenekleri olmayan ve bilişim suçu işlemeyi planlayan kişiler dahi, Bilişim sisteminde çalışan personel ile danışıklı olarak hareket etmek zorundadırlar.

Gelecekteki eğilimler ile ilgili olarak bilişim bilgisinin geniş çapta yayılması beklenebilir. Bilişimin ilk günlerinde çok nadir bilinen bilgiler bugün ülkemizde binlerce kişi tarafından bilinmektedir. Bazı tahminlere göre (Örn. Sendrow 1980), gelecek 25 yıl içerisinde bilişim yetenekleri bugünkü okuma yazma yeteneği kadar yaygın bir hale gelecektir. Ancak bu büyük bir sonuç getirecektir. Kişisel bilgisayarların ve ev bilgisayarlarının yayılması aynı yönde etki gösterebilir.

3. BİLİŞİM SUÇU: TERMİNOLOJİSİ VE TANIMI

3.1. Hukuki ve kriminolojik kavram bilişim suçu ile ne kastedildiği ve bu ifadenin hangi yasaklanmış eylemleri kapsadığı konusunda belirsizlik mevcuttur. Ancak bir kavramı tanımlamaya çalışmadan önce, tanımın türü ve kullanımı hakkında açıklık getirilmelidir. Hizmet edeceği amaca göre tanımı belirlemek için çeşitli değişkenler kullanılmaktadır. Burada kullanılan bilişim suçu tanımları iki ayrı düzeyde irdelenebilir:

- Bilişim sistemlerine karşı işlenen suçlar

- Bilişim sistemleri ile işlenen suçlar/suç failleri

3.1.1. Hukuki bir kavram olarak bilişim suçları

Aşağıdaki haller bilişim suçu olarak kabul edilmektedir:

- İzinsiz olarak bilgisayara dayalı kişisel dosyanın açılması veya tutulması (sınır dokunulmazlığa karşı işlenen suçlar),
- Bilgi hırsızlığına karşı koruma ile ilgili kanunların ihlal edilmesi,
- Kişisel bilgiler verilmesi,
- Bilgi tecavüzü. Yani, EBİ kayıtlarına yasadışı yollarla erişilmesi veya bu kayıtların yasal olmayan şekilde değiştirilmesi, silinmesi veya bu tür kayıtların girilmesi veyahut bilgi tecavüzü için hazırlık yapılması.

Bilişim sistemleri alanındaki muazzam gelişmenin yol açtığı bütün cezalandırılabilir türdeki bilişim sistemlerinin kötü kullanımlarının (özellikle ülkemizdeki) mevcut kanunlar altında cezalandırılıp cezalandırılmadığı şüphelidir.

Mevcut durumun pratikte çeşitli sonuçları bulunmaktadır. Bunlardan en önemlileri arasında bilişim sistemlerinin çeşitli şekillerdeki kötü kullanımına karşı yeterli yasal korumanın mevcut olmamasıdır.

Bilişim sistemlerinin kötüye kullanılması ile ilgili muhtemel bütün yolları kapsayan hukuki bir tanımlamanın yapılabilmesi zordur.

ABD'deki çeşitli eyaletlerde bilgisayarla ilgili suçları üç ana başlık altında toplayan yönetmelikler bulunmaktadır: Fikir haklarına karşı tecavüzler (programlar dahil verileri ifade etmektedir), bilgisayar donanımına ve gereçlerine karşı işlenen suçlar ve bilgisayar kullanıcılarına karşı işlenen suçlar. **Bilişim sistemleriyle İlgili Suçlar Kanunu** diğer eyaletlerin yanısıra Florida, Colorado, Rhode Island, Michigan, New Mexico ve Arizona gibi eyaletlerde yürürlükte bulunmaktadır. Bu yönetmelikler diğer eyaletlerde tartışılmaktadır (Kanunların Uygulanmasına Yardım İdaresi, Birleşik Devletler Adalet Bakanlığı, 1979).

3.1.2. Her halukarda kanunen suç eylemleri olarak kabul edilip edilmemelerine bakılmaksızın bilgisayarların mevcut kötüye kullanım şekillerini temsil eden gerçek tablodan kriminolojik bir ortam oluşmaktadır. Suçun tanımlaması sadece ceza kanunlarının düzenlemesi altında bulunan eylemleri kapsamaktadır.

Bilişim suçu gibi kollektif bir kriminolojik kavramın herhangi bir uygulama fonksiyonuna hizmet edip edemeyeceği sorusuna cevap vermek üzere aşağıda bilişimle ilgili suçların mahiyeti ile ilgili bir tanımlama verilmiştir.

3.2. Kavramlar ve tanımlar

Bilişim suçunun tanımı ile ilgili görüşlerde farklılıklar bulunmaktadır. Bazı tebliğlerde bilişim suçu bir tür ekonomik suç olarak tanımlanmaktadır. Herbert Edelherz . (1977) bu konuda "Computer white-collar crime" (beyaz yakalı-bilgisayar suçları) deyimini kullanmaktadır. Yazara göre, bilişim sistemleri teknolojisindeki hızlı gelişme, siparişlerin yerine getirilmesi, para kayıtlarının tutulması, borçlandırma, gönderme, faturalama, muhasebe, transfer, uzlaştırma, depolama, ücret ödemeleri, krediler, tescil vs. ile ilgili manuel işlemlerde değişiklik getirmiştir. Manuel işlemlerin yerini otomatik bilgi işlem almıştır. Dolayısıyla bilgisayarlar bu yordamları ve "beyaz yakalı suçlarının" çevresini devralmıştır.

Edelhertz'e göre, ekonomik suçlarda "işlemin" suç niyetini gizlemek için daima araç olarak kullanılan "kağıt" üzerinde hile yapılması söz konusudur. Bilgi işlemde bilgiler elektronik semboller halinde manyetik ortamda saklandığından bu tür hilelerin yapılabilmesi fırsatını arttırmaktadır. Bir bilgisayarın büyük miktarlardaki nakit parayı transfer etmesi birkaç saniyeden fazla sürmez ve programda bu konu ile ilgili esas komutlar herhangi bir kalıcı iz bırakmadan "silinebilir". Bilgisayar kullanımıyla suçlu yakalanma riski fazla olmadan büyük miktarlarda parayı zimmetine geçirebilir.

Edelhertz bir bankanın nakit bölümü sorumlusunun üç yıl içerisinde milyonlarca Doları aktif olmayan hesaplardan kendi hesabına nasıl geçirebileceğini göstermektedir. İşlenen suç New York polisi tarafından haftada 30.000 Dolar'a varan bahisler düzenleyen bir bahisçinin yılda 11.000 Dolar maaşla bir bankada çalıştığı tesadüfen ortaya çıkınca anlaşılmıştır.

August Bequai (1978) Bilgisayar suçuyla ilgili bir tanım bulunmadığını öne sürmektedir. Onun tanımına göre "bilişim suçu", "beyaz yakalı suçu" adı verilen daha büyük bir suç eyleminin bir bölümünü oluşturmaktadır (Bilişim Suçları, 1973). Bu tanım beyaz yakalı suçu olarak sınıflandırılamayacak ve her halukarda bilişim suçları toplu kavramına atfedilecek belirli yasadışı kavramları kapsamamaktadır. Bu durum bilişim sistemlerine karşı işlenen çeşitli şiddet suçları için geçerlidir.

Rainer A. H. von zur Mühlen "Computerkriminalitaet" deyimini ifade etmektedir. Bilgisayarın (bilişim sisteminin) kendisi suçlu olamayacağından " Bilişim suçluluğu" haklı olarak eleştirilmektedir. Ancak, von zur Mühlen bu deyimi, bu olguyu kısa ve öz tanımlamasından dolayı genel olarak kabul edildiğini ifade etmektedir.

Von zur Mühlen, "Computerkriminalitaet" deyimi ile bilgisayarlara (bilişim sistemlerine) yöneltilen veya bilgisayarların araç olarak kullanıldıkları her türlü suç eylemini kastetmektedir (1975). Bu terim suçun çeşitli hukuki tanımlarını da kapsamaktadır. Bu suçlardaki ortak elemanlar araç ve hedeftir. Von zur Mühlen "suç eylemleri" olarak cezalandırılamayacak ancak mahiyetleri ve karakterleri dolayısıyla suç sayılması gereken eylemleri ifade etmektedir.

Sieber de von zur Mühlen ile aynı Almanca terimi, yani "Computerkriminalitaet"i kullanmaktadır. Ancak von zur Mühlen'in tanımını gerçeği yansıtmaktan uzak bulmaktadır. Von zur Mühlen'in tanımı boş (içinde bilgi bulunmayan) bir manyetik bandın çalınması gibi bilişim sistemleri ile rastlantısal yasaklanmış eylemleri de kapsamaktadır. Sieber ayrıca bu terimin tanımına bütün bilişim sistemlerine özgü suçların dahil edilmemesi gerektiğini düşünmektedir. Sieber'in düşüncesine göre. "Computerkriminalitaet" terimi altında sadece bilişim sistemleri ile ilgili mülkiyet suçları sınıflandırılmalıdır. Sieber ayrıca bu terimi aşağıda belirtilen şekilde daha kesin olarak tanımlamaktadır. "Computerkriminalitaet" bilgisayar verilerinin kasıtlı olarak değiştirildiği (bilgisayarda hile yapılması), tahrip edilmesi (Bilgisayar sabotajı), yetki dışı kullanılması veya yararlanılması (Bilgisayar casusluğu) ve bilgi işlem donanımı ile bilikte kullanıldığı (zaman hırsızlığı) mülkiyet suçlarını kapsar (Sieber 1980). Sieber'in tanımının von zur Mühlen'in tanımına nazaran daha iyi formüle edildiği ve sınırlarının belirlendiği kabul edilmekteyse de Sieber'de bilişim suçunu sadece mülkiyete karşı işlenen suçlar ile sınırlandırmaktadır.

Donn B. Parker'a göre, "beyaz yakalı suçu"nun bilişim suçuna belirli yönlerden benzerliği bulunmaktadır. Ancak bilişim sistemlerinin giderek daha fazla kullanılması ve bilişim alanındaki hızlı teknolojik gelişmeler bilişim suçunun fenomenolojisinde bir değişiklik meydana gelmesiyle sonuçlanmış ve bu şekilde beyaz yakalı suçu ile bilişim suçu arasındaki farklılaşma giderek artan şekilde doğrulanmıştır. Bilişim suçu gerek klasik gerek ekonomik suçlarla ilişkili suçların çeşitli hukuki tanımlama-

larını kapsayabilir. Parker bu konuda üç terim kullanmaktadır: Bilişim sistemlerinin kötüye kullanılması, Bilişim suçu ve bilişim sistemleri ile ilgili suçlar. Bu terimler Parker tarafından aşağıda belirtilen şekilde tanımlanmaktadır:

" **Bilişim sistemlerinin (bilgisayarın) kötüye kullanılması"** bir veya birkaç failin bilişim sistemleri kanalıyla yaptığı veya tekrar yapabileceği ve bir veya birkaç mağdurun zarara uğradığı veya uğrayacağı kasıtlı eylemlerdir (Parker D. B., 1980).

"Bilişim suçu" bilişim sistemlerinin yasadışı kullanımlarını tanımlamak için kullanılan ortak bir terimdir. Ancak, suçun işlenmesinde bilişim sistemlerinin doğrudan kullanımını kastetmektedir (Parker, D. B., 1980).

"Bilişim sistemleri ile ilgili suç" başarıyla uygulanabilmesi için bilgisayar teknolojisi ile ilgili bilgilerin gerekli olduğu herhangi bir yasadışı eylemi geniş anlamda ifade eder (Parker D. B., 1980).

Parker'a göre, "bilişim sistemleriyle ilgili suç" terimi sanayi ve ticaret alanlarına karşı işlenen suçlar, beyaz yakalı suçları veya ekonomik suçlarla kısıtlanamaz. Bu terim aynı zamanda kritik işlemlerin doğruluğunu ve etkinliğini kontrol eden bilgisayar kullanılarak bilişim sistemlerine ve verilerine karşı yapılan şiddet suçlarını veya insanların hayatını tehlikeye atan suçları da kapsayabilir.

Avusturalya'daki Caulfield Teknoloji Enstitüsü bünyesindeki Bilişim Sistemlerinin Kötüye Kullanılması Araştırma Bürosu, bilişim sistemleriyle ilgili hırsızlık, zimmete geçirme, sahtekarlık vs.;

- Giren ve/veya çıkan bilgilerin yetkisizce kullanılması,
- Terminaller vasıtasıyla bilişim sistemine yetki olmadan girilmesi,
- Uygulama programlarının yetki dışı uygulanması veya kullanılması,
- EBİ sistemine karşı işlenen suçlar, donanımın, dosyaların veya çıkan bilgilerin çalınması,
- Bilgisayar sistem donanımına karşı sabotaj,
- Verilerin yetki dışı durdurulması gibi olayları tanımlayan "bilişim sisteminin kötüye kullanılması" terimini kullanmaktadır (Fitzgerald 1980).

Yukarıda yer alan tanımlamalara dayanarak bilişim suçları ile ilgili ortak ve genel kabul görmüş bir tanımlama bulunmadığı söylenebilir. Bilişim sistemlerinin kötüye kullanılması, bilişim suçu, bilişim sistemleriyle ilgili suçlar gibi çeşitli terimler kullanılmaktadır. Bu terimlerden her birinin çeşitli eksikleri vardır. Kriminoloji açısından "bilişim suçu" terimi bu tanımın esas aldığı en önemli iki değişkeni, yani suçu ve bilişim sistemini tanımlamakta ve **suçun** bir **bilişim sistemi** ile ilişkili olduğunu ifade etmektedir.

Burada bilişim suçu geniş kapsamlı bir kriminolojik terim olarak kullanılmaktadır. Bu kollektif isim sahtekarlık, hırsızlık, zimmete geçirme, bilişim sistemi tecavüzü, hasar, şantaj ve yaşama ve sağlığa karşı suçlar gibi ortak paydaşı bilişim sistemi olan suçların çeşitli hukuki sınıflandırmalarını kapsamaktadır. Dolayısıyla bilişim suçu terimi bilişim sistemleriyle ilgili olmak kaydıyla her tür suç tipini kapsayabilir.

Bazı yazarlar tarafından "bilgisayarla ilgili suç" teriminin eş anlamlısı olan "bilişim suçu" kullanılmaktadır. Ancak, "bilişim suçu" sadece verilerle ilgili olmayıp bilgisayarın çeşitli kısımlarıyla ilgili belirli suç eylemlerine uygun değildir.

Bu olgunun daha kesin tanımlanabilmesi için ve bilişim suçunun yeni bir kriminolojik unsur olup olmadığı sorusuna cevap bulabilmek amacıyla herşeyden önce bilişim suçunun fenomenolojisinin bölümünü oluşturan ve aynı zamanda fırsat yapısını yaratan faktörler incelenmelidir.

3.3. Bazı Ana Hatlar:

- Kamu dosyalarındaki bilgilere erişme ve genel olarak bilgi hürriyeti sorunları.
- Halkın ve uzmanların öğretimi ve eğitimi.
- Belirli ağırlık verme ve devlet desteği sorunlarında araştırma ve geliştirme.
- Bilişim teknolojisinin gelecekteki gelişmesi ile ilgili araştırmalar, ileriye dönük tahminler.
- Bilişim sistemlerinin sosyal etkisinin incelenmesi.
- Bilişim alanında özel "ulusal projelerin" uygulamaya konulması. Bilişim sistemlerinin daha yaygın şekilde kullanılmasının desteklenmesi.
- Bilişim ürün ve hizmetlerinin edinilmesi, özellikle, uzman bir kuruluş araçılığıyla koordineli devlet alımları ile ilgili sorunlar.
- Bilgisayar/iletişim tesislerinin geliştirilmesi. Bilgisayarlar ile iletişim araçarı arasındaki etkileşiminin incelenmesi, uzmanlaşmış bilgi şebekesinin yaratılması.
- Sistem tasarımı yöntemleri, genelleştirilmiş yazılım paketleri ve güvenlik ile ilgili standardizasyon sorunları.
- Çeşitli ulusal yazılım ve donanım işletmelerinin desteklenmesi, bilgisayar pazarındaki ulusal çabaların koordine edilmesi, yerli üretimi için çaba sarfedilmesi.
- Bilgisayar alanındaki uzmanlığı temsil eden danışmanlık kuruluşlarının meydana getirilmesi.
- Merkezileştirme, merkezden uzaklaştırma, gelişmenin bölgeselleştirilmesi, diğer hususların yanısıra, güvenlik ve organizasyon açısından kamu bilişim sistemlerinin gelişiminin ve işletilmesinin bölgelere yayılması. Kamu bilişim ile ilgili farklı organizasyon modelleri.
- Bilgilerin işlenmesi ve kullanımının koordine edilmesi, özellikle, sosyal planlama ve istatistik açısından "bilgi bankaları/havuzları"nın yaratılması ve topla-

nan bilgilerin kullanılması.

- Örneğin bilişim sistemlerinin bütçelendirilmesi ile ilgili olarak metodoloji alanında koordinasyon sağlanması.
- Fiyatlandırma politikaları ve bilgisayar ve iletişim hizmetlerinin ücretleri.

4. BİLİŞİM SUÇLARININ FENOMENOJİK UNSURLARI/FAKTÖRLERİ

4.1. Yeni Fenomenolojik Unsurları/Faktörleri

Aşağıda yer alan altı unsurun bilişim suçunun esasını oluşturduğu kabul edilebilir:

- Suçun işlendiği alan/yer,
- Modi operandi ,
- Netice,
- (Zaman) Ani suç/mütemati suç,
- (Mekan) Mesafe suçu,
- Fail (Şekil 6).

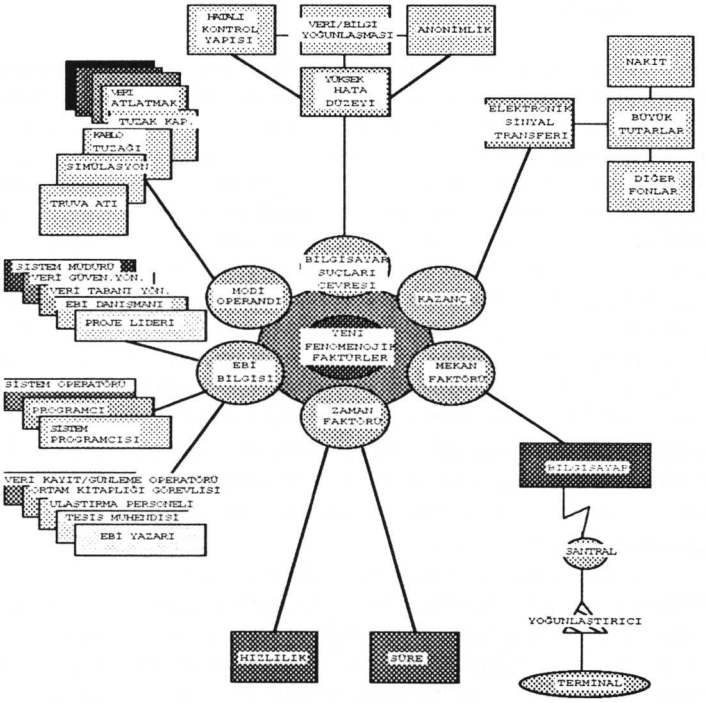
4.1.1. Suçun işlendiği yan/yer birçok bilişim suçu türünün çevresi bakımından bunlarla ekonomik suçların diğer türlerinin çevresi arasında bir benzerlik bulunmaktadır. Ekonomik suçun işlendiği yan/yer genellikle masa, dokümanlar, yazı malzemesi, muhtemelen bir hesap makinesi ve kazanılacak nesne yani paradır. Ancak, manuel sistemlerde fırsat yapısı bilgisayar sistemlerinin fırsat yapısına göre değişiklik göstermektedir. Eski manuel sistemlerde suç eylemlerinin ortaya çıkarılması güç olsa bile, fonksiyonu tesbit etmesinin yanısıra koruyucu etkisi de olan bir kontrol ve denetleme sistemi bulunmaktaydı. Ayrıca, tutulan defterlerdeki tahrifatların ortaya çıkarılması da çok daha kolaydı. İşlemler genellikle en az iki kişi tarafından yapıldığında sosyal kontrol daha iyi fonksiyon görmekteydi. Dokümanlar ve defter tutma işlemi genellikle çeşitli yerlere dağıtılmıştı. Dolayısıyla bir seferde büyük miktarlar üzerinde oynamak daha güçtü. Büyük meblağlar ile yolsuzluk yapmak için fail belgeler üzerinde sürekli tahrifat yapmak zorundaydı ve dolayısıyla bu da yakalanma riskini arttırmaktaydı. Dahili kontrol ile ilgili temel esas bir işlemin veya işlem türünün başından sonuna kadar tek bir kişi tarafından yapılmaması ve bir departman veya personel tarafından yapılan işin mümkünse bir başkası tarafından bağımsız olarak denetlenmesidir.

Bilgisayar teknolojisine geçişle birlikte suçlu için yeni bir çevre yaratılmıştır. EBİ'ye geçişin önemli nedenlerinden biri faaliyetlerin otomasyonu ile işlem güvenliğinin geniş ölçüde arttırılmasıdır (teknik işlemler fonksiyonu, malların, hastane yataklarının vs. mevcudiyeti, fatura ve ödeneklerin tahsilk edilmesi veya ödenmesi). Ancak, modern Bilişim sistemlerinin, örneğin; suç eylemlerine karşı hassaslık açısından belirli zayıf noktaları bulunmaktadır.

Büyük miktarlarda bilgi tek bir noktada toplanmaktadır. Bilginin büyük bir kısmı birkaç veri tabanında/bankasında yoğunlaşmaktadır. Tek bir hizmet bürosu birçok şirket için bilgi toplayabilir ve işleyebilir. Veritabanları, veri ortamları manyetik bantlar, diskler ve disketler v.b. den oluşmaktadır. Billişim sistemleri kritik üretim süreçlerinin kontrol edilmesinde kullanıldığı gibi; sağlık hizmetlerinde hastaların, hayatı ve sağlığı açısından büyük önem taşıyan büyük miktarlardaki bilgiler de bilgisayarlaştırılmıştır (Polli 1980).

Şekil 6 - Bilişim suçlarının fenomenolojik unsurları

Bilgilerin tek noktada büyük oranda yoğunlaştırılması ve çoğrafi açıdan çeşitli yerlere dağılmış bilgisayar kullanıcılarından alınan veya bunlara aktarılan bilgiler suç uygulamaları için yeni çevreler oluşturmaktadır. Bu yeni çevreler bilişim merkezleri, terminaller, iletişim araçları (telefon, faks, teleks), disk, disket, manyetik bant, kaset vs. şeklinde bilgi taşıyıcılardır.



Teknolojinin ileri düzeyde gelişmiş olmasına rağmen EBİ kullanımı bilgile-

rin ulaştığı veya dosyalandığı ve kullanıldığı noktalarda çeşitli işlemler yapılmasını gerektirmektedir. Ayrıca, bilgisayarda yapılan işlemlerin bir ara kademesi bulunmaktadır. O da çeşitli kontrollar ve kayıt ve bunu takip eden bilgi işlemin çeşitli şekillerini içermektedir. Bilgilerin işlendiği çeşitli noktalar arasında bir ulaştırma söz konusudur. Bilgisayarda da çeşitli kategorilerdeki personel, yani merkeze veya merkezden yapılan aktarmalardan sorumlu olan, bilgileri işlenmeden önce veya işlendikten sonra alan ve veren, bilgi sağlayan kişiler ile arşivlenmiş bilgilerden sorumlu olan bilgisayar operatörleri, programcılar ve diğerleri bu bilgiler ile doğrudan veya dolaylı olarak temas etmektedirler.

Bilişim sistemlerinin yoğun bir yapısı vardır. Bütün hatalar ve eksiklikler saptanıncaya kadar bir sistemin uzunca bir süre kullanılması gerekmektedir. Sistemin geliştirilmesi ve değiştirilmesi ile ilgili sürekli talepler nedeniyle de yeni kusurlar ortaya çıkmaktadır. Yani donanımlar ve yeni programlar devreye sokulmakta ve gerek yordamlar gerekse programlar sık sık değiştirilmektedir. Bütün zayıf noktaların saptandığı ve bilindiği bir istikrar durumunun elde edilmesi zordur.

"Bilgisayar hataları"na ilginç bir örnek ABD Senatosu Resmi İşler Komitesi huzurunda delil sunan ABD Adalet Bakanlığı temsilcisi Richard L. Thorhburgh tarafından bildirilmiştir. Sağlık, Eğitim ve Refah Bakanlığı yetkililerinin verdiği bilgiye göre, Sosyal Güvenlik İdaresi'nin bilgisayara geçmesinden sonraki 27 ay zarfında isimsiz 620 milyon Dolar tutarında haksız ödenekler ödenmiştir (ABD Senatosu Resmi İşler Komitesi, 1977).

Bilgisayar ve iletişim şebekelerinde hiçkimsenin doğrudan gözlem yapabilme ihtimali bulunmayan belirli suç eylemleri yapılabilir.

4.1.2. Modi operandi (Bilişim suçluluğunun maddi unsuru) hareket, Yeni modi operandi bilgisayar çevresine uygulanan otomatik yordamların kullanılmasına bağlıdır. Bilişim sistemleri olmadan hesapların yuvarlatılması adı verilen işlemle büyük meblağlarda sahtekarlık yapılması mümkün olmaz. Yuvarlatma sahtekarlığı aşağıda belirtilen rutin işlemlere dayanır. Bankalar mevduat için belirli bir faiz oranı tesbit ettiklerinde ondalık hanesi genellikle ikiden fazla olmaktadır. Bu meblağlar hesap sahibine alacak kaydedilemediğinden faiz hesabını yapan program fazla ondalık haneler tarafından temsil edilen meblağ müteakip hesaba eklenmektedir. Bu aktarma son hesaba kadar bu şekilde devam eder. Modus operandi fazla ondalık hanelerin temsil ettiği kuruşların bir sonraki hesaba aktarılması ve dolayısıyla suçlunun emrinde olan bir birikim hesabına aktarılmasına dayanır. Bir bilgisayar bir ay içerisinde bunun gibi birkaç milyon işlem yaptığından, toplamların daha önceki ile aynı olması dolayısıyla yakalanma riski olmaksızın oldukça büyük miktarlar toplanabilir. Buna "sa-

lam" tekniği adı verilmektedir. Değişik bilişim suçu şekillerine ait modi operandi'yi gösterecek yeni bir özel dil yaratılmıştır.

Bilgi aldatmacası, truva atı, salam tekniği, süper darbe, kapan kapakları, lojik bombaları, asenkronize saldırı, leşçilik, veri sızdırma, yankesicilik, taklit, tel salma, simülasyon, modelleme gibi ifadeler bilişim suçu işlenmesi ile ilgili teknik ve taktik yöntemleri çoğunluğunu belirtmektedir. Bunlardan bazıları aşağıda ele alınmıştır.

Bilgi aldatmacası verilerde yetkisiz şekilde kasıtlı olarak hile yapılması veya değiştirilmesini ifade eder. Veriler bunları şifrelenmesi, dosyalanması, ulaştırılması, kontrolu, ve bilgisayara girilmek üzere dönüştürülmesi amacıyla verilere erişimle imkanı olan personel tarafından değiştirilebilir. Bu işlem belgelerin tahrif edilmesi, veri ortamlarının (manyetik bant, disk veya disket) özel olarak hazırlanmış materyel ile değiştirilmesi, kartlara ek karekter kaydı ya da bazı kayıtların iptali veya manuel kontroldan kaçınılması süretiyle yapılabilir.

Truva atı bu tekniğin tarihteki Truva Atı efsanesine benzeyen yönleri bulunmaktadır. Bilgisayar programları ile ilgili olarak, sistem kitaplığındaki geçerli bir programın planlanan suçun işlenmesine yarayacak değiştirilmiş bir komut sırası içerdiğini ifade eder. Normalde program amaçlanan şekilde çalışır. Ancak program fail tarafından çağırıldığı zaman (bir bilgisayar programını veya alt programını harekete geçiren eylem) program şekil değiştirir. Yani, birkaç mikrosaniye içinde programdan çıkarılan değiştirilmiş talimatları araya girer.

"Truva atı"nın klasik örneği çeşitli yayınlarda açıklanmıştır. Bu olay birkaç yıl önce bir Amerikan Üniversitesinde meydana gelmiştir. Sistem mühendislerinden biri işletim sisteminde hata ararken raslantı eseri olarak daha önce hiç görmediği bir komut dizisi saptamıştır. Mühendis bu diziyi dikkatle inceledikten sonra sisteme bağlı olan birçok terminalden birinin sistem operatörü konsolu haline getirilebileceğini ve bu terminali kullanan kişinin bilgisayardaki bütün bilgilere ulaşarak bu bilgiler üzerinde sınırsız şekilde oynayabileceğini saptamıştır (Parker D. B., 1976).

Superzapping Superzapping bir master anahtar ile kıyaslanabilecek bir kullanma programıdır. Superzap programları çeşitli işletme hatalarının ortaya çıkması halinde acil durumlarda kullanılır. Bilgisayar durdurulur ya da normal kurtarma veya yeniden çalıştırma işlemleri ile giderilemeyen bir duruma girer. Sisteme konulmuş olan bütün güvenlik engellerini ve koruma önlemlerini aşabilmek için bilgisayarın işletmesinde meydana gelen belirli kusurları süratle düzeltmek amacıyla superzap sistemi kullanılır. Ancak aynı program suç işlemek amacıyla da kullanılabilir. Super-

zap programı suçlu tarafından kullanıldığı zaman tehlikeli bir alet haline gelebilir. Superzap programını usulüne uygun olarak kullanan bir New Jersey bankası bilgisayar merkezi başkanı herhangi bir kontrol söz konusu olmaksızın belirli meblağların başka hesaplara kolaylıkla aktarılabildiğini keşfetmiştir. Superzap programını kullanarak veri dosyalarında herhangi bir iz bırakmaksızın 128.000 Dolar'ı haksız olarak almıştır (ABD Adalet Bakanlığı Kanun İcra Dairesi, 1979).

Bu örnekler bilgisayar suçunun fenomenolojisi ile ilgili yeni elemanları göstermektedir. Bilgisayar teknolojisi bilgileri bir araya toplaması, muazzam işlem hızı ve programlardaki değişikliklerin saptanmasındaki güçlükler nedeniyle yeni suç yöntemlerinin kullanılmasına imkan sağlamaktadır.

4.1.3. Netice, Klasik hedef para ve diğer şeylerdir. Parayı ve diğer nesneleri haksız olarak edinmek için bunların fiziksel olarak sahibinden yasadışı işlem yapan kişinin zilyetine aktarılması gerekir. Büyük banka soygunları daima titizlikle planlanan soygundan sonra banknotlarla dolu torbaları taşıyan kişiler tarafından yapılmaktadır. Genellikle küçük meblağlar ile ilgili olarak kullanılan yol çek sahtekarlığıdır. Bilgisayar çağında bu hedef şekil değiştirmiştir. Para, buna sahip olan kişinin ödeme kabiliyeti ile ilgili bilgiden başka birşey olmadığı için banknotlar bir başka bilgi şekli ile, yani elektronik sinyaller ile değiştirilebilir. Bilgisayarlar, veri taşıyıcıları ve veri iletişimi ile para yerine elektronik sinyaller şeklinde veriler nakledilir. Bunlar tutarlar ile ilgili bilgilerin merkezi olarak modern medyalara kaydedilmesi ve kısa bir süre içerisinde coğrafi olara birbirlerinden uzak yerlere aktarılması suretiyle büyük miktarlar halinde toplanabilir. Elektronik sinyallerin banknotların yerini alması suç eylemlerine karşı alınacak koruma tedbirlerini önemli ölçüde azaltmıştır. Elektronik sinyaller halindeki paraya karşı olan davranış nakit paraya karşı olan davranıştan temel olarak farklıdır. Banknot kullanan kişi bunları dikkatle sayar. Kasada saklanan para alarm sistemine bağlı etkili kilitler ile korunur. Nakit paranın taşınmasında özel tedbirler alınır. Diğer yanda, elektronik sinyaller şeklindeki para hemen hemen büyük bir kayıtsızlıkla işlem görmektedir. bilgisayara geçişin kontrol ve güvenlik ile ilgili tüm sorunların üstesinden geleceği zannedilmiştir. Ancak, esas belgeler üzerindeki kontrol dahi büyük oranda azalmıştır. Mair ve ark. (1978) manuel sistemlerle kıyaslandığında EBİ sistemlerindeki kontrolun 10:1 oranında azaldığını belirtmektedirler. Fırsat yapısı yasalara uyma aleyhine değişmiş bulunmaktadır. Banknot şeklindeki paraya karşı olan geleneksel davranış elektronik sinyaller halindeki para söz konusu olduğunda değişime uğramıştır. Bilgisayar sistemlerinde muazzam miktarlarda bilgi toplanmasının ve işlem yapılmasının diğer bir sonucu da bunların klasik suçlara nazaran bilişim suçlarına çok daha açık durumda bulunmalarıdır.

Her bilişim ile ilgili suçtaki ortalama zarar geleneksel ekonomik suçlardaki zararlardan daha fazladır. ABD'de bilgisayar aracılığı ile zimmete geçirme ve sahte-

karlık olaylarının her olayda ortalama 617.000.- Dolar zarara yol açtığı, buna mukabil geleneksel ekonomik suçların ortalamasının 104.000.- Dolar olduğu hesaplanmıştır (Parker 1976). Bunun açıklaması şöyledir. Bilgi ve işlemlerin yoğunlaşmasının yanısıra, bilgisayar sistemlerinin mahiyeti ve şekli 100 Dolar ile 1 milyon Dolar'ın yakalanma risklerinin aynı olması sonucunu doğurmaktadır.

4.1.4. (Zaman) Ani suç/mütemati suç, bilişim suçunu geleneksel yasadışı eylemlerden ayıran yeni unsurlardan/faktörlerden biri de süredir. Deneyimler suçun işlenmesinde zamanın önemli bir risk faktörü olduğunu göstermektedir. Bir suçlu bir dizi suç planladığı taktirde bunların her biri için gereken zamanı hesaplayacaktır. Dolayısıyla geleneksel suçta zaman suça niyetlenen bazı kişileri engelleyen bir unsur olabilir. Suçun işlendiği süre içerisinde bunun tesbit edilmesi, alarm sisteminin devreye girmesi tehlikesi büyüktür.

Klasik suçlarda zaman dakika ve saat ile ölçülür. Bilişim suçlarında ise zaman faktörünün yeni bir boyutu bulunmaktadır. Bilgi işlem saniye ve saniyenin bölümleri gibi zaman kavramlarını kullanmaktadır. Bazı bilişim suçlarında 0.003 san., yani 3 milisaniye (bir saniyenin binde üçü) yeterli olmaktadır. Milisaniye, mikrosaniye, nanosaniye gibi yeni zaman boyutları hakkında fikir sahibi olabilmek için aşağıda yer alan kıyaslama yapılır. Bir nanosaniye ile saniye arasındaki zaman ilişkisi 1 saniye ile 30 yıl arasındaki ilişki gibidir.

Bilişim suçuna özgü diğer bir zaman kavramı da suç eyleminin süresidir. Üç genellikle uzun zaman alır (uzun suç dizisi). 15 bilişim suçu vakası ile ilgili bir raporda suç eylemleri 1.3 ila 6 yıl, ortalama olarak 3 yıl sürmüştür (Allen 1977). Dolayısıyla zaman faktörü yakalanma riskini büyük oranda azaltmıştır.

4.1.5. (Mekan) Mesafe suçu, Klasik suç şekillerinde suçlu genellikle suçun işlendiği yerde bulunmaktadır. Bir sahtekarlığın faili kurbanı/mağduru ile herhangi bir şekilde temas halinde bulunmalıdır. Ekonomik suçlarda da fail sahtekarlık yapılacak belge ile temas etmekten kaçınamaz. Dolayısıyla klasik suç eyleminin uzaktan işlenmesi istisnaen mümkün değildir.

Yeni iletişim sistemleri ile etkileşim halinde bulunan bilgisayarlar bu alanda da yeni imkanlar yaratmışlardır. Bilgisayar teknolojisi ile iletişim arasında giderek daha yakından kurulan bağlantı sayesinde bilgisayarlar arasında ya da bilgisayar ile kullanıcısı arasındaki coğrafi uzaklıklar kalkmıştır. Dolayısıyla, bilişim sistemi içerisinde bir suçun sınırsız bir uzaklıktan işlenmesi mümkündür. İstanbul'a yerleştirilmiş olan bir bilgisayar kanalıyla örneğin 1000 kilometre öteden suç işlenebilir. Halen bazı uluslararası şebekeler işletilmekte olduğundan (örneğin bankalar) suç eylemi ihtimalinin ulusal sınırları da aştığı söylenebilir. Bu da özellikle usul hukuku açısından yeni sorunları ortaya çıkarır ve yeni ulusal ve uluslararası alanda yeni düzenlemeleri

gerektirir.

4.1.6. Fail İnsanlar neden suç işler? Hepsinin suça eğilimi mi var yoksa, bu durum sadece belirli zihinsel veya fiziksel niteliklere sahip olanlar için mi geçerli? Olayın etyolojisi iki soru etrafında toplanmaktadır. Bu sorulara cevap verebilmek için makro faktörlerin yanısıra farklı suç türlerinin fenomenolojisi ile suç faillerini incelemek gerekir.

Bilişim suçları alanında failin tipolojisi ve davranışları ile ilgili bazı araştırmalar yapılmıştır. Bilişim suçları şimdiye kadar bilgisayar merkezleri ve kullanıcıları üzerinde yoğunlaşmıştır. F.W. Dennis (1979) bilgisayar ilişkili sahtekarlığın yapılması için suçlunun bilgisayar sistemi hakkında bilgi sahibi olması gerektiğini belirtmektedir. ABD'de bilgisayarı kötüye kullanabilecek yani suç niyeti ile veriler üzerinde işlem yapabilecek eğitim düzeyine sahip yaklaşık iki milyon insan olduğu tahmin edilmektedir (Türkiye'de yaklaşık 10.000 kişi bilgisayar eğitiminden geçmiştir). Dennis açıklamasını 200 vakanın analizine dayandırmaktadır.

Hemen hemen bütün Bilişim suçlularının herhangi bir suç kaydı olmayan itibarlı kişiler olduğu bilinmektedir. Birçok olayda bunların bilişim suçları ilk suçları olarak kayda geçmiştir. Bu suç bazen diğer insanlarla danışıklı olarak işlenmiştir. Parker, Stanford Araştırma Enstitüsü'nde kaydedilen 669 bilgisayar ilişkili suçun yüzde 50'sinin başkaları ile danışıklı olarak işlendiğini saptamıştır (bilişim suçu, 1979). Suçlular genellikle yüksek gelir düzeyinde olan kişiler olmakla birlikte suça iten nedenler esas itibariyle ekonomik mahiyettedir. Bunun nedeni faillerin genellikle gelirlerinin sağladığından daha yüksek bir standartta yaşamalarıdır.

Yasadışı uygulamalar bakımından önemli olan bir başka unsur bulunmaktadır. Bilgisayar bunu kullanmak üzere eğitilmiş insanlar için entellektüel bir meydan okuma aracı oluşturmaktadır. Bir bilişim sisteminin yenilmesi örneğin öğrenciler için bir oyun olarak kabul edilmektedir. Bunlar yetkisi olmayan kişilerin bilgilere ulaşmasının veya bunları kullanmasının yasak olduğunu bilmektedirler. Ancak, öğrenciler bilginin kendisini değil sistemi yenmekle ilgilendiklerini iddia etmektedirler. Ancak bu yolla kritik durumlarda bilgisayarı yetkileri dışında kullanabilecekleri belirli bir deneyim kazanmaktadırlar. Öğrenciler halihazırda bilgisayar sistemine girebilmek ve yakalanmadan bilgiler üzerinde oynamak için yordamlar denemişlerdir. Bilişim suçunda yer alan zeka oyunu suç eylemini kolaylaştırabilir ve ahlaki direnci zayıflatabilir.

San Francisco'da 55 kişinin katıldığı bir seminerde Donn B. Parker bilgisayarın kötüye kullanılması ile bir anket sunmuştur. Ankete katılan programcılar ve veri tabanı yöneticileri bilgisayarın çeşitli kötüye kullanılma şekilleri ile ilgili 12 soruya

cevap vermişlerdir. "Patronunuz için yazdığınız bir programı izinsiz olarak kullanması için bir başkasına verdiniz mi?" "Yazılı bir anlaşma olmaksızın diğer programcılar ile program değiş tokuşu yaptınız mı?"

Bu gibi eylemlere karşı olan davranışları değerlendirebilmek için dört alternatif cevap bulunmaktaydı: "OK", "ahlak dışı", "şerefsizlik", "yasadışı". Sorularda yer alan uygulamalar yasadışı olarak kabul edilmekle birlikte oniki sorudan altısına katılanların %25-30'u tarafından "OK" cevabı verilmiştir. Verilen cevaplar katılanların %15 ila 18'inin programları veya bilgisayar zamanını yukarıda sorulduğu gibi doğru olmayan amaçlar için kullanmışlardı. 193 bilişim suçu vakası üzerinde yapılan bir incelemede 482 kişi yer almış, bunlardan %94'ü bilgisayar eğitimi görmüş, %6'sı ise bilgisayar eğitimi görmemiştir (Parker D. B., 1976).

Bilişim suçu bilgisayar alanında çalışan birçok kişi tarafından toplum düzenine aykırı bir davranış olarak tanımlanmakta ancak yasaların ihlal edilmesi olarak tanımlanmamaktadır. Bu durum kısmen belirli kasıtlı hareketlere ve bilişim sistemlerinin kötüye kullanılmasına karşı katı cezai müeyyidelerin bulunmamasına bağlı olabilir.

Potansiyel suçlular bilişim uzmanları grubuna dahil olan, yani, bilgisayar teknolojisini ve bilgi işlemi kendilerini kontrol edenlerden, patronlarından ve denetçilerden çok daha iyi bilen ve yüksek düzeyde entellektüel eylem yapabilme kabiliyetinde olan kişilerdir. Bu da bilişim suçunun ele alınması ve sınırlandırılması açısından hukuk sistemine ve uygulamalarına yeni bir durum getirmektedir.

YARARLANAN/YARARLI KAYNAKLAR

Allen, B.; ***The biggest computer frauds: Lessons for CPAS****, The journal of Accountancy, 1977.*

American Bar Association (ABA), Criminal Justica Section, Task Force on Computer Crime.; ***American Bar Association Report on Computer Crime****. Washington, D.C.: ABA, June, 1984.*

American Institute of Certified Public Accountants.; ***American Institute of Certified Public Accountants (AICPA) Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries****. New York: AICPA, 1984.*

ADV und Recht.; ***Einfuhrung in die Rechtsinformatik und das Recht der I nformationsverarbetung****. Hrsg. W. Steinmüller. Berlin: J. Schweitzer 1976.*

Artandi, S.; ***An Introduction to Computers in Information Science****. 2. ed. Metuchen: The Scarecrow Press 1972.*

Aydın, E.D.; ***Bilişim, Genel Sistemler ve Sibernetik Terimleri Sözlüğü****, Mistaş A.Ş., İstanbul, 1984.*

Aydın, E.D.; ***Bilgisayar Nedir?****, Mikro-Tip A.Ş., İstanbul, 1988.*

Aydın, E.D.; ***Tele İşlem ve Veri İletişimi****, EDA Bilişim Ltd., İstanbul, 1989.*

Aydın, E.D.; ***Bilgi Bilimi ve Kitle İletişimi****, Aydın Özel Eğitim Yayıncılık, İstanbul, 1991.*

Aydın, E.D.; ***Veri Tabanı - Data Base****, İstanbul, Evrim Basın Yayın Dağıtım, Eylül 1990.*

Baker, D.; ***An Agenda for the National Commission on Electronic Fund Transfers****. In: Bank Administration, Vol. LI (1975, Dec.) 19.*

Beer, S.; ***Cybernetics and Management. London****: The English Universities Press 1965.*

Bequai, A.; ***Computer Crime****, p 207. Lexington Books, 1978.*

Bigelow, R., Nycum S.; ***Your Computer and the Law****. Englewood Cliffs: Prentice-Hall 1975.*

Bing, J., and Harvold, T.; ***Legal Decisions and Information Systems****, Universitetforlaget, Oslo, 1977.*

Bloom Becker, Jay.; ***Computer Crime, Computer Security, Computer Ethics****. Los Angles: National Center for Computer Crime Data, 1986.*

_____ ***The Computer Crime Law Reporter****, with 1988 Update. Los Angles: National Center for Computer Crime Data, 1988.*

_____. ***Introduction to Computer Crime****, 2nd ed. Los Angles: National Center for Computer Cire Data, 1988.*

_____. ***The Spread of Computer Crime.*** *Los Angles: National Center for Computer Law Advisor, May, 1984.*

_____. ***Commitment to Security****. Los Angles: National Center for Computer Crime Data and RGE Associates, March, 1989.*

Caldwell, M.; ***Jurisprudence in Interdisciplinary Environments****. In: Jurimetrics Journal, Vol. 8 (1968) No. 3, 1*

Cherry, C.; ***On Human Communication****. 2. ed. Cambridge: The M.I.T. Press 1966.*

Committee on Goverment Operations, United States Senate, ***Problems associated with computer technology in federal programs and private industry****, Computer abuses, Washington, 1976.*

Committee on Government Operations, United States Senate, ***Computer in security federal programs****, Washington, 1977.*

Committee on Government Operations, United States Senate, ***Staff study of computer in federal programs****, Washington, 1977.*

Communication Sciences and Law*: Reflections from The Jurimetrics Conference. Ed. L. Allen, M. Caldwell. New York...: Bobbs-Merrill 1965.*

Computers, Society and Law*: The Role of Legal Education. (Proceedings of the AFIPS/Standford Conference June 25-27, 1973). Ed. J. Leininger and B. Gilchrist. Montvale: AFIPS Press 1973.*

Cowan, Th.; ***Decision Theory in Law, Science and Technology****. In: Communication Sciences and Law. Ed. L. Allen, M. Caldwell. New York.: Bobbs-Merrill*

1965.

Danielsson, A., Törnebohm, H.; ***On Complex Systems with Human Components.*** *Stockholm: Försvarets Forskningsanstalt (FOA P rapport C 8212-10).*

Data Processing Management Association (DPMA). ***Data Processing Management Association Model Computer Crime Act.*** *Park Ridge, IL: DPMA, 1987.*

_____. ***Data Processing Management Associaton Principles for Computer Crime.*** *Park Ridge, IL: DPMA, 1987.*

Dennis, F.W.; ***The Computer Criminal, Security world.*** *p 26, September 1979.*

Dopping, O.: ***Kort och brett om ADB,*** *Lund, 1972.*

Edelhartz, H.; ***The investigation of white collar crime,*** *Washinton 1977.*

Federal Financial Institutions Examination Council (FFIEC). ***EDP Examination Handbook.*** *Washington, D.C.: FFIEC, 1988.*

Fiedler, H., von Berg, M.; ***Stichworte zur RechtsinformatikAusbildung an den juristischen Fakultaetan.*** *In: Datenverarbeitung im Recht, Vol. 2 (1973), No. 2/3, 231.*

Fiedler, H.; ***Grundproblemen der juristischen Informatik.*** *In: Datenverarbetung im Recht, Vol. 3 (1974), No. 3/4, 198.*

Fiedler, H.; ***Forschungsaufgaben der juristischen Informatik.*** *In: EDV und Recht. Möglichkeiten und Problemen. A. Kaufman. Berlin: J. Schweitzer 1973 (EDV und Recht. Band 6).*

Fitzgerald, K. J.; ***A Study in computer abuse,*** *Caulfield, 1979.*

Fitzgerald, K. J.; ***EDP losses and prevention,*** *Caulfield Institute of Technology, Caulfield, 1980.*

Göranzon, B.: ***Perspektiv paa datasystemutveckling,*** *Lund, 1978.*

Haft, F., ***Elekronische Datenverarbetung im Recht.*** *Berlin: J Schweitzer 1970. (EDV und Recht. Band 1).*

Informatica e Dritto. Bibliografia Internazionale. *Rivista trimestriale Florence: Istituto per la documentzione giuridica, Consiglio nazionale ricerche .*

Kerimov, D.; ***Future Applications of Cybernectics to Jurisprudence in the U.S.S.R.*** *In: Modern Uses of Logic in Law (M.U.L.L.), Dec. 1963, 153.*

Knapp, V.; ***O vozmozjnosti ispolsovanija kibernetitjeskich metodov v prave (On the Possibilities of Using Cybernetic Methods in the law).*** *Moskva: Progress 1965.*

Kolveit, James M.;" Audits vs. Director's Examinations" ***Illinois Banker,*** *March, 1986.*

Law Enforcement Assistance Admistration, US Dept. of Justice, ***"Computer crime",*** *Criminal Justice Resource Manual, 1979.*

_____. ***Legal Aspects of Computerized Information Systems. Report by a Panel on Legal Aspects of Information Systems (COSATI).*** *In: The Honey well Computer Journal, Vol. (1973), No. 1.*

Loevinger., L.; ***Jurimetrics: The Next Step Forward.*** *In: Minnesota Law review,*

Vol. 33 (1949), 455 (also published in Jurimetrics Journal, Vol. 12 (1971), 1,3).

Loevinger., L.; ***Law and Science as Rival Systems.*** *In: Jurimetrics Journal, Vol. 8 (1966), No. 2, 63.*

Losano, M.; ***Giuscibernetica. Macchine e modelli cibernetici nel diritto.*** *Torino: Piccola Biblioteca Einaudi 1969.*

Luhmann, N.; ***Verfassungsmaessige Auswirkungen der elektronischen Datenverarbeitung.*** *In: Öffentliche Verwaltung und Datenverarbeitung, Vol. 2 (1972), No. 2, 44.*

Mühlen, Rainer A.H.; von zur ***Probleme der strafrechtlichen Erfassung von Sonderfaellen der Computerkriminalitaet*** *Betribswirtschaftliche Forschung und Praxis.*

Mühlen, Rainer A.H.; von zur ***Computer-Kriminalitaet - Kehrseite des Fortschrittes,*** *archiv für Kriminologie Vol 157.*

Novotny, E.J.; ***Restrictions on the transnational flow of corporate information,*** *New challenges for the auditing profession, the EDP Auditor, 1979.*

Novotny, E.J.; ***Tarnsborder data flows and international law: A framework for policy-oriented inquiry,*** *Stanford Journal of International Law. Vol 16,1980.*

Novotny, E.J.; ***The security of transborder data flows: Computer-communication protection at the international level,*** *Remarks before thee National Conference on Computer-related Crime, Washington, 1980.*

Parker, D.B.; ***Rules of ethics in information processing,*** *Communications of the Association for Computing Machining, 1968.*

Parker, D.B.; ***Crime by computer,*** *USA, 1968.*

Parker, D.B., ***Computer abuse research update,*** *Computer/Law Journal, Vol II, No. 2, 1980*

Parker, D.B.; ***Manager's Guide to Computer Security.*** *Reston, VA: reston Publishing Co., 1981.*

President's Council on Integrity and Efficiency Prevention Committee. ***Computers: Crimes, Clues and Controls-A Management Guide*** *Washington, D.C.: 1986.*

Reisinger, L.; ***Strukturtheorie des Recht und EDV.*** *In: Dataverarbetung im Recht, Vol. 2 (1973), No. 4. 271.*

Ross Ashby, W.; ***An Introduction to Cybernetics.*** *London: Methuen 1 1971.*

Polli, G.T.; ***Confidentiality and computerized patient information,*** *Security World, July, 1980.*

Seipel, P.; ***Om anvaendaning av automatisk databehandlings teknik inom juridiken.*** *I: Svensk Juristtidning, Vol. 55 (1970b), 257 (Part I), 722 (Part 11).*

Seipel, P.; ***Traevetenskapliga perspektiv på juridiken.*** *I: Mål och metoder för forsking inom civilraetten. Stockholm: Statens råd för samhaellsforskning 1974.*

Sendrow, M.; ***Impact of rapidly changing computer technology on computer cri-***

me, *National Conference on Computer-related Crime, Longsdon Drive, Oct. 20-22, Washington, 1981.*

Sieber, U.; ***Competerkriminalitaet und Strafrecht 2. auflage,*** *Heyman, Köln, 1980.*

Smith, A.; ***Comminication in Law: What does Communication Theory have to after Law Teachers and Law Researchers?*** *In: Jurimetrics Journal Vol. 10, (1969), No. 1, 20.*

Stadler, G.; ***Elektronische Datenverarbeitung und Kybernetik in der Gesetzgebung.*** *In: Datenverarbeitung im Recht, Vol. 2 (1973), No.1,1.*

Vanyo, J.; ***The Legal System: Can It Be Analyzed to Suit the Scientist?*** *In: Jurimetrics Journal, Vol. 14 (1973), No. 2, 100.*

Vrecion, V.; ***Zur Anwendungsmöglichkeit der Informationstheoire im Bereich des Rechts.*** *In: Datenverarbeitung im Rech, Vol. 2 (1973), No. 1, 76.*

Weinberg, G.; ***An Introduction to General Systems Thinking.*** *New York...: Wiley 1975.*

Weyers, H.L.; ***Etwas Kybernetik im Privatrecht.*** *In: Funktionswandel der Privatrechtsinstitutionen. Festschrift für Ludwig Reiser zum 70. Geburtstag. Hrsg. F. Baur... Tubingen: Mohr 1974.*

Wold, Geoffery H.:"Are You Redy for ATMs?" ***Independent Banker,*** *Vol. 36, No. 4, April, 1986.*

_____. *"Before Purchasing a Microcomputer."* ***Indepentend Banker,*** *Vol. 36, No. 7, July, 1986, &pp, 42-44.*

_____. *"Biometrics: Fingerprints, Signatures and Keystrokes."* ***Financial Operation,*** *Winter, 1988, pp. Vol. 3, No. 4, July, 1987, pp. 31-32.*

_____. *"Blocing Computer Crime."* ***Independent Banker,*** *Vol. 37, No. 2, February, 1987, pp. 42-44.*

_____. *"How to Prepare Disaster Recovery Plan."* ***Financial Manager's*** *Statement. Vol. 9, No. 4, July, 1987, pp. 31-32.*

_____. *"Planning for EDP Needs."* ***Independent Banker,*** *Vol. 3, No. 7, July, 1985, pp. 18-19.*

_____. *"Preparing for Disaster and Planning for Recovery."* ***Independent Banker,*** *Vol. 36, No. 10, 1986, pp. 42-44.*

_____. *"Revisiting Data Processing Alternatives."* ***Financial Manager's*** *Statement. Vol. 10, No. 2 March, 1988, pp. 76-78.*

_____. *"Say the Secret Word."* ***Financial Operations,*** *Vol. 2, No. 4, Winter 1987-88, pp. 14-16.*

_____. *"When Disaster Strikes."* ***Credit Union Management,*** *Vol. 11, No. 4, pp. 22-24.*

_____. *"Words of Caution on Electronic Speadsheets."* ***Independent Banker,*** *Vol. 36, No. 1, 1986, pp. 16-18.*

Wold, Geoffrey H., and Robert F. Shriver; ***Disaster Recovery Compliance made Easy: Step-by-Step Guidefor Preparing, Evaluating and Testing a Savings***

Institution's Emergency Plan. *Chicago; U.S. League of Savings Institutions, 1988.*

_____. ***Disaster Recovery for Banks: A Comprehensive Program for Today's Refilatory Climate.*** *Rolling Meadows, IL: Bank Administration Institute, 1988.*

U.S. Department of Justice-Federal Bureau of Investigation, Bank Crime Statistics, Federally Insured Financial Institutions, January, 1988-December 31, 1988, Washington, D.C.