

Ülkemizde Bilişim Suçları Ve Mücadele Yöntemleri

Giriş:

Gelişen teknolojiler akıl almaz bir hızla ilerleyerek insan hayatını her geçen gün biraz daha kolaylaştırmaktadır. Bilgisayar ve iletişim teknolojilerindeki gelişmeler günümüzde insanlık tarihi açısından çok önemli bir devrim olarak kabul edilmekte hatta sanayi devrimi ile mukayese edilmektedir. Eğitimden ticarete, devlet sektöründen özel sektöre, eğlenceden alış-verişe kadar bir çok alanda klasikleşmiş anlayışları değiştirmiş ve insanlara yeni bir anlayış yeni bir hayat tarzı kazandırmıştır. Bununla birlikte insanın bulunduğu her yerde suç rastlanıldığı gibi bu alanda da yeni suç tipleri ortaya çıkmış ve suçlular da teknolojinin getirdiği yenilik ve kolaylıkları kullanmaya başlamıştır. Günümüzde bilgisayar kavramı sadece hayatımızı kolaylaştıran bir devrim olmaktan çıkmış suç kavramı ile birlikte anılan bir araç haline de gelmiştir.

Bu tür suçlar özellikle dijital ortamdaki değerlere yapılan saldırılardır ve genellikle bankalardaki finans kayıtları, hastane kayıtları, askeri bilgiler v.b. bu saldırılara maruz kalma potansiyeli taşımaktadır. Bilgisayar üzerinden daha ucuz ve kolay suç işleme olanağı ileride bu suç tipleri ile daha çok karşılaşacağımız ve bildiğimiz klasik suç tiplerinin; hırsızlık, soygun, terörizm, sabotaj, kaçakçılık ve bir çoğunun dijital ortamda yerini alacağı anlamına gelmektedir. Hatta ülkeler arasındaki sanayi, teknoloji ve strateji casusluğu dijital ortamda yapılmakta ve ülkeler bundan dolayı büyük zararlara uğratılabilmektedir. Bununla birlikte banka hırsızları artık klasik yöntemler yerine iletişim sistemlerini kullanarak bankalardaki hesap kayıtlarını rahatça değiştirilebilmektedirler. Ayrıca İnternet üzerinde oluşturulan sistemler ile kumar oynatılabilmekte, pornografik ve hatta devlet aleyhine karşı yasadışı yayınlar yapılabilmektedir.

Bilişim Suçlarının Kapsamı, Tanımlamaları ve Sınıflandırılması:

Bu suçlarda teknolojinin kullanılması kaçınılmazdır. Bir bilgisayar, internet uzayı, bir kredi kartı, elektronik bir cihaz veya cep telefonu ile de bu suçlar işlenebilmektedir. Bu yüzden bilgisayar suçlarının kapsamı çok geniştir. Tanımlamalar da bu yüzden hep değişik olmuştur. En basit tabiriyle bilgisayar suçları olarak tanımlayabildiğimiz gibi; Siber Suçlar, Dijital suçlar, İnternet Suçları, Bilişim Suçları, İleri Teknoloji Suçları vs. tanımlamaları ile de karşılaşmaktayız. Diğer ülkelerde yapılan tanımlarda ise; Computer Crimes, Cyber Crimes, IT Crimes (Information Technologies – Bilgi Teknolojileri), Crime of Networks vb. Aslında tüm bunlar ile bu suçların bir kısmı tanımlanması yapılmaktadır. Ancak Türkçe'mize Bilişim Teknolojileri Suçları olarak geçen IT Crime (Information Technologies) bu suçların alanı açısından tanım olarak daha iyi uymaktadır. Bu yüzden daha kısa ve yalın bir ifade ile "Bilişim Suçları" olarak kullanılması daha uygun olacaktır.

Bilişim Suçları kapsamına giren suçların tanımlanması ve sınıflandırılmasının yapılması daha sonra yapılacak çalışmalara hazırlık teşkil edecek ve her bir suç tipi daha rahat anlaşılabilir olacaktır. Burada suç tipleri arasındaki farkı oluşturan esas etken "suçun işlenmesindeki amaç" olmalıdır. Bu tür suçlar hangi yöntemle işleniyor olsa da, hangi amaca hizmet ettiğine bakmak önemlidir. Örneğin; bir bilgisayar sistemine girmek için bir çok yöntem bulunabilir; bir virüs veya trojan kullanarak veya sistemin açık kapıları zorlanarak giriş yapılabilir. Ancak burada amacın "sisteme girme" eylemi olduğuna dikkat etmek önemlidir. Burada kullanılan yöntemler ancak suçun ağırlaştırıcı sebeplerini oluşturabilir. Mesela bir sisteme girerken başka sistemlere de sızmış olması gibi. Aşağıda tanımlanması yapılan suç tipleri gerek Avrupa Birliği, gerek Avrupa Konseyi ve gerekse diğer Avrupa ülkelerince yapılan tanımlamaların ülkemize uyarlanmış halidir. Benzer tanımlamalarla İngilizce tabirleri ile karşılaşmak mümkündür. "Unauthorized Acces, Computer Sabotage, Computer Fraud" gibi. Bu suç tiplerine bakacak olursak;

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme

Anayasamızda belirtilen *Özel Hayatın Gizliliği* maddesine aykırı olarak teknolojik dinlemelerin yapıldığına güncel olarak karşılaşmaktayız. Günümüzde daha modern bir yapıya ulaşan iletişim kavramı artık bilgisayarlar üzerinden yapılmakta ve hatta kişilere ait önemli bilgiler bu ortamda iletilmektedir. Kişilerin, bankaların, hastanelerin, hatta güvenlik ve istihbarat birimlerini tutmuş olduğu bilgiler bilgisayarlarda saklanmaktadır. Bu bilgilere ulaşmakta yine bilgisayar teknolojileri kullanılarak yapılmaktadır. İşte bu noktada gizlilik gerektiren bilgilere yetkilisi haricinde yapılan erişimler bu suç tipine girmektedir. Erişim haricinde haberleşme amacıyla kurulu iki bilgisayar sisteminin iletişiminin dinlenmesi de aynı şekilde değerlendirilmektedir. İletişimin dinlenmesi; sadece bilgisayar başındaki iki kişinin birbiri ile görüşmesi olarak düşünülmemelidir. Birbirine bilgi gönderen ve uyum içinde çalışan bilgisayarların network içinde göndermiş oldukları bilgilerin dinlenmesi de dinleme olarak değerlendirilmelidir.

2. Bilgisayar Sabotajı

Bilgisayar Sabotajı yetkisiz erişimden ikinci safhası olarak değerlendirilebilir. Çünkü; Yetkisiz erişimde bulunan birisi sadece pasif bir davranışta bulunup özel hayatın gizliliğini bozmuş olur. Ancak Bilgisayar Sabotajı erişimden sonra elde ettiği bilgilerin silinmesini ve değiştirilmesini içerir. Bu suç tipi iki şekilde karşımıza çıkmaktadır. Birincisi; yine bilgisayar teknolojileri kullanılarak erişilen bilgilerin silinmesi, yok edilmesi ve değiştirilmesidir. İkincisi ise bilgisayar teknolojileri kullanılmadan direk olarak bilgilerin tutulduğu bilgisayarı ve/veya bilgisayarları fiziksel olarak zarara uğratmaktır. Burada önemli olan mala karşı değil de, bilgisayarın içindeki bilgilere karşı yapılmış bir hareket olarak algılamak önemlidir. Çünkü bu bilgiler bilgisayar kendisinden daha değerli olabilir.

3. Bilgisayar Yoluyla Dolandırıcılık

Klasik olarak bildiğimiz ve karşılaştığımız dolandırıcılık suçunun bilgisayar ve iletişim ortamları üzerinden yapılıyor olmasıdır. Bilgisayar Yoluyla Dolandırıcılık en çok kredi kartlarının kullanımıyla yapılmaktadır. Bunun için üretilmiş birçok "Cart Generator" programı bulunmaktadır. Bunlar sayesinde internet üzerinden alışveriş yapılırken, istenilen kredi kartı şirketi için mantıksal olarak olası kredi kartı bilgileri üretilmekte ve bu olaydan kredi kartı sahibinin haberi bile olmamaktadır. Bununla beraber yine finans bilgilerinin tutulduğu programlarda yapılan değişiklikler ile istenilen kişinin hesabına istenildiği kadar para aktarılması yapılabilmektedir.

4. Bilgisayar Yoluyla Sahtecilik

Yine klasik olarak bilinen sahtecilik suçunun, yüksek teknoloji ürünü cihazlar kullanılarak yapılmasıdır. Bilgisayar Suçlarının tanımı içerisinde bu suçlara bakıldığında diğer sahtecilik suçlarından ayırt edebilmek için Bilgisayar Yoluyla Sahteciliği ayrı olarak ele almak gerekmektedir. Çünkü; bilgisayar kullanımı ile üretilmiş sahte para suçunda, olay yerinde delil niteliği teşkil edecek bilgilerin bulunması çok zordur ve bu delillerin toplanması ve soruşturulması teknik bir olay olarak karşımıza çıkmaktadır.

5. Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

Fikir ve Sanat Eserleri Kanununda eser olarak kabul edilen bilgisayar yazılımlarının lisans haklarına aykırı olarak kullanılmasıdır. Bilgisayar yazılımları satın alınırken üzerinde gelen lisans sözleşmesine göre bir yazılımın bir adet kopyası ancak satın alan şahıs tarafından yapılacağı ve bu yazılımın başka bir kişi tarafından kopyalanmayacağı ve kiralanmayacağı belirtilmektedir. Bir çok yazılım şirketinin yazılım korsanlığına karşı hukuki işlemlerini yürüten BSA'nın (Business Software Alliance) verdiği rakamlara göre ülkemizde lisanssız yazılım kullanımının %80'lerin üzerinde olduğu belirtilmektedir.

6. Yasadışı Yayınlar

Yasadışı yayınlar karşımıza üç şekilde çıkmaktadır. Bunlardan birincisi; vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli internet sayfalarıdır. Özellikle terör örgütleri tarafından hazırlanan bu sayfalarda Türkiye içerisinde yayınlamadıkları bölücü fikirlerini internet ortamında çok rahat teşhir edebilmektedirler. Bununla birlikte; *halkın ar ve haya duygularını incitecek şekilde genel ahlaka aykırı* pornografik görüntüler içeren internet sayfaları da yayınlana bilmektedir. Yurtdışındaki diğer ülkelerde genel itibarıyla çocuk pornografisi üzerine yoğunlaşmış ve ona göre çalışmalar yapılmıştır. Ülkemizde ise; çocuk veya büyük pornografisi şeklinde bir ayırım yapılmadığından bütün pornografik yayınlar yasaklanmış durumdadır. İnternet sayfaları ile işlenebilecek diğer bir suç türü ise; bir kişiye karşı yapılan hakaret ve sövme suçunudur.

Teknolojinin ilerlemesi ile birlikte birçok yeni suç tipinin çıkması muhtemeldir. Dijital Sertifikalar oluşturularak kurumların ve kişilerin doğrulanma yöntemleri gün geçtikçe yaygınlaşmakta ve ileride dijital ortamdaki şahısların taklidi yapılarak işledikleri suçları başkaları yapıyormuş gibi gösterilebilme ihtimali çok yüksektir. Bununla birlikte bu dijital sertifikaların verileceği dijital noterlerinde hangi kurumlar olacağı üzerinde düşünülmesi gereken bir konudur.

Hukuki açıdan bakıldığında adı geçen suç tiplerini iki şekilde kategorize edebiliriz. Aşağıdaki tabloda da gösterildiği şekliyle birincisi; geleneksel suçların bilgisayar yolu ile işlenmesi, diğeri ise yeni teknolojiler ile birlikte ortaya çıkan suç tipleridir.

Hukuki Olarak	Suç Tipi	Kanundaki Yeri
Geleneksel Suçların Bilgisayar Yoluyla İşlenmesi	Bilgisayar Yoluyla Dolandırıcılık	TCK 503-507 : Dolandırıcılık ve İflas
	Bilgisayar Yoluyla Sahtecilik	TCK 316-368 : Sahtecilik Suçları
	Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı	5846'nolu Fikir ve Sanat Eserleri Kanunu (FSEK)
	Yasadışı Yayınlar	<ul style="list-style-type: none"> ■TCK 125-200 : Devletin Şahsiyetine karşı cürümler ■TCK 480-490 : Hakaret ve Sövme Cürümleri ■TCK 426-427 : Halkın ar ve haya duygularını inciten veya cinsi arzuları tahrik eden ve istismar eder nitelikte genel ahlaka aykırı: ve diğer anlatım araç ve gereçleri
Teknolojinin İlerlemesi ile Ortaya Çıkan Suç Tipleri	Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme	TCK 525 a,b,c ve d "Bilişim Alanında Suçlar Babı"
	Bilgisayar Sabotajı	

Tabloda da görüldüğü gibi her suç tipinin hukukumuzda karşılığı bulunmaktadır. Teknolojinin ilerlemesi ile ortaya çıkan suçların hukukumuzdaki karşılığı 1991 yılında TCK'a eklenen 525-a,b,c,d maddeleri ile yapılmıştır. Şu an üzerinde çalışılan ve meclise sunulması planlanan yeni Türk Ceza Kanunu Ön Yasa Tasarısı ile de; gelişen teknolojiye ayak uyduracak ve oluşan yeni suç tiplerini de kapsayacak şekilde düzenlemesi düşünülmektedir. Ancak teknolojinin hızla ilerlemesiyle birlikte suçlarda hızla ilerleyecek ve yeni suç tipleri ile karşılaşılacaktır. Suçların teknik olarak engellenmesinin mümkün olmayacağı bu noktada; teknolojik suçlarla mücadelede hukukun tartışılmaz üstünlüğü ortaya çıkmaktadır. Bu yüzden en iyi çözüm hukuki bazda yapılacak değişimlerdir.

Ayrıca bu suçlardan bazıları *takibi şikayete bağlı suçlar* olup mağdur olanların bizzat şikayette bulunmaları gerekmektedir. Ancak; Türkiye'de bakıldığında buradaki mağdurların bu konuda nasıl bir müracaatta bulunacaklarını ve hangi kanunlarla korunduklarını bilemediklerinden kendi yöntemleri ile mağduriyetlerini giderme cihetine gitmektedirler. Bunlar ise; genel itibarıyla "sen benim bilgilerimi sildin bende seninkileri silerim" türünden davranışlar olmaktadır.

Yaşanan Problemler ve Çözüm Yöntemleri:

Görüldüğü üzere suç tipleri tanımlanmış ve bu suç tiplerinin kanunlarımızda karşılığı bulunmaktadır. Ancak istatistiklerden de anlaşılacağı gibi, bu suçlarla mücadele de yeterli

başarının sağlanmadığı görülecektir. Mücadelede yaşanan problemler ve problemlerin çözüm yöntemleri aşağıda açıklanmıştır.

1. Elde Edilen Delillerin Hukuki Durumu

Suçların bulunmasında en etkili yöntem delillerin toplanmasıdır. Toplanan her delil soruşturma süresince polise ışık tutacak ve mahkeme aşamasında önemli sonuçlar ortaya koyacaktır. Bilgisayar suçlarında delil niteliği teşkil eden bilgiler ise; yine bilgisayar ortamında tutulmuş olan kayıtların olacağı da aşikardır. Bu kayıtların delil niteliği teşkil edebilmesi için sağlam ve değiştirilemez bir yapıya sahip olması gerekmektedir. Ancak bilgisayarın kullanıcısı tarafından belirlenen yöntemlerle kaydedilen bilgiler yine bilgisayarın kullanıcısı tarafından değiştirilebilir ihtimali taşımaktadır. Böyle olunca sağlam bir delil olmaktan çıkmaktadır. Kanunlarımızda faks çıktıları dahi delil olarak nitelendirilmediği göz önünde bulundurulacak olursa, bilgisayar kayıtlarının ne kadar delil teşkil edip etmeyeceği gözükecektir. Bilişim Suçlarında delil niteliği olan sadece bu kayıtlı bilgiler olduğundan dijital delillerin hukuki durumu tartışılması en önemli konulardan biri olmalıdır.

2. Delillerin Elde Edilmesi

Ülkemizde dijital kayıtların delil niteliğinin düzenlenmiş olduğunu varsayacak olursak, bu sefer delillerin elde edilmesi problemi karşımıza çıkmaktadır. İnternet'e bağlanmak için ya bulunduğunuz kurumun bilgisayar ağına bağlı olmanız, ya bir İnternet Servis Sağlayıcıdan hizmet almanız veya bir İnternet Kafeye gitmeniz gerekmektedir. Tabi bilgisayar üzerinden bir suç işlemeniz içinde bu yerlerden servis olarak internete bağlanmanız gerekir. Böyle olunca suçu işleyen kişiye ait bilgiler sadece buralardan bulunabilir. Ancak ülkemizdeki İnternet Servis Sağlayıcıları ve özellikle de İnternet Kafeler düzenli kayıt tutma işleminin masraflı olmasından dolayı bu sistemleri kurmamaktadırlar. Bu yüzden emniyet tarafından takip edilen bir soruşturma da kayıtların elde edilmesi aşamasında problem yaşamaktadır. Bu da; suçların yaygınlaşmasında önemli bir rol oynamaktadır. Bu yüzden bu türden internet servisi veren yerlere en kısa zamanda devlet tarafından belli standartların getirilmesi ve bu konuda sorumluluklar verilmesi gerekmektedir.

3. Uluslararası Polis İşbirliği

Ülkemizde gerek delillerin hukuki niteliği, gerekse de İnternet Servis Sağlayıcılardan delillerin elde edilmesi konusunda her türlü düzenleme yapılmış olsa da, uluslararası polis işbirliğine gidilmeden sağlıklı bir sonuç elde edilmesi afaki kalacaktır. Çünkü; özellikle internet üzerinde işlenen suçlarda birden fazla geçiş noktası bulunabilmektedir. Bu noktalarda genelde birden fazla ülke üzerinde bulunabilmektedir. Böyle olunca bir olayın soruşturmasında olayın yurt dışındaki bir servis sağlayıcı üzerinden yapıldığı bulunursa ilgili ülke polis teşkilatı ile irtibata geçip gerekli bilgilerin elde edilebilmesi gerekmektedir. Aksi takdirde olayın soruşturması bir noktadan sonra kesilecektir. Bu amaçla ülkelerin bu konuda aralarında ikili polis işbirliğine gitmelidir.

4. Uluslararası Suçun Tanımlanması

Şu ana kadar sayılan tüm problemler halledilmiş olsa da, eğer soruşturmadaki bir suç diğer ülkede suç niteliği teşkil etmiyorsa o ülkeden gerekli bilgiler alınamayacaktır. Bu amaçla İnterpol, Avrupa Birliği ve Avrupa Konseyinde uluslararası suçun tanımının yapılmasına dair çalışmalar bulunmaktadır. Ülkemizde de bu çalışmalar özenle takip edilmeli ve kanunlarımızdaki eksiklikler giderilmeye çalışılmalıdır.

Bilişim Suçları olgusu teknolojiyi kullanan ve kullanacak bütün ülkelerin ortak problemi haline gelmiş ve özellikle A.B.D ve Avrupa ülkelerinde bu alandaki hukuki ve idari yapılanmaların düzenlenmesi için birçok çalışmalar başlatılmıştır. Bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde milli sınırları aşmış, bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmıştır. Teknolojik gelişmeler ile globalleşen dünyamızda; tüm ülkelerin işbirliği ile bu tip suçlara karşı mücadele etme gereği ortaya çıkmıştır.

SONUÇ

Gerçek hayatta güncel olarak rastladığımız suç tiplerini artık dijital ortamda da sıkça görmekteyiz. Pornografik ve yasadışı yayınlar, kredi kartı dolandırıcılığı, telif hakları ile korunan bilgisayar yazılımlarının kopyalanması v.b. suç tipleri İnternet ve özellikle bilgisayarlar üzerinde aktüel olarak işlenmektedir. Ayrıca yüksek teknoloji suçları bilinen suç tiplerinden farklılık arz etmektedir. Bu yüzden bu tip suçlara polisler ve suçun soruşturulması esnasında görevli olan herkes daha farklı yaklaşmalıdır. Çünkü elektronik cihazlar, bilgisayarlar ve diğer yüksek teknoloji ürünleri kullanılarak daha kolay ve ucuz suç işlenebilmektedir. Bu da; ileride bu suçlar ile daha çok karşılaşacağımız anlamına gelmektedir. Bu yüzden Türkiye'nin Bilişim Suçları üzerine ciddi olarak eğilmesi gerekmektedir.