

*Semih DOKURER
Komiser
Emniyet Genel Müdürlüğü
Bilgi İşlem Daire Başkanlığı
Bilişim Suçları Araştırma Büro Amirliği
Bursa Paneli*

ÜLKEMİZDE YAŞANAN BİLİŞİM SUÇLARI VE GELİŞTİRİLEN MÜCADELE TEKNİKLERİ

GİRİŞ

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 hayat tarzı kazandırmıştır. Teknolojik alanda gerçekleştirilen gelişmelerden dolayı iletişim, hukuk, sanat, ticaret ve hemen hemen her türlü alanda radikal değişimler oluşmuştur. Teknolojinin efektif olarak kullanılmaya başlandığı günümüzde atık bilgi teknolojilerinin ortaya çıkaracağı yenilik ve değişimlere kendimizi hazırlamamız da dolaylı olarak şart haline gelmiştir.

Hazırlanmamız gereken en önemli şeylerden biride; suçların teknoloji kullanılarak işleniyor olmasıdır. Artık günümüzde teknolojik olarak işlenen bir çok yeni suç tipi ortaya çıkmış ve suçlular da teknolojinin getirdiği yenilik ve kolaylıkları kullanmaya başlamıştır. Böyle olunca; 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.

Bu amaçla; Emniyet Genel Müdürlüğünde 1998 yılında kurulan *Bilgi Suçları ve Bilgisayar Güvenliği Kurulu* kurulmuştur. Bilgisayar suçları üzerinde daha da yoğunlaşılması amacıyla Kurul tarafından oluşturulan *Bilişim Suçları Çalışma Grubu* ile de çalışmalara hız kazandırılmıştır. Emniyet güçleri olarak Bilişim Suçları konusunda ileride daha çok karşılaşacağımız vakalara hazırlıklı olabilmek için; yapılan çalışmaların başında Bilişim Suçlarının kapsamı, bu kapsam içerisine giren Suç Tiplerinin tanımlaması ve sınıflandırmaları yapılmıştır. Bu çalışmalar ise;

Bilişim Suçlarının Tanımı ve Kapsamı

Bu konuda karşımıza bir çok tanım çıkmaktadır; Bilgisayar suçları, Dijital suçlar, İnternet suçları, Siber Suçlar, Yüksek Teknoloji Suçları v.b. Diğer ülkelerde yapılan tanımlarda ise; Computer Crimes, IT Crimes(Information Technologies), Crime of Networks v.b. Aslında tüm bunlar ile bu suçların bir kısmı tanımlanması yapılmaktadır. Çünkü bu suçlar bir bilgisayar ile yapılabildiği gibi bir bilgisayar ağı veya internet ortamında da olabilmekte, bunun için elektronik bir devre veya ufak bir kredi kartı bile kullanılabilir. "Bilişim" tabiri ise; bilgisayar ve bilgisayar teknolojileri ile iletişim teknolojilerini kapsadığından Kurul tarafından "*Bilişim Suçları*" başlığı altında ele alınmıştır. Bu yüzden bilişim suçlarını incelerken suçun tüm bu sistemlerin kullanılarak işlenebiliyor olması göz önünde bulundurulmalıdır. Çünkü Bilişim Suçları tahkikat altına alındığında çok teknik bir ekip tarafından incelenmesi ve soruşturmaların ona göre yapılması gerekmektedir.

Bilişim Suçlarının Sınıflandırılması

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 lazımdır. 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 lazımdır. Burada kullanılan yöntemler ancak suçun ağırlaştırıcı sebeplerini oluşturabilir. Mesela bir sisteme girerken başka sistemlere de sızmış olması gibi. Bu suç tiplerine bakacak olursak;

1. Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim

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 bulunmaktadır. Kişilerin, bankaların, hastanelerin, hatta güvenlik ve istihbarat birimlerini tutmuş olduğu bilgiler bilgisayarlarda saklanmaktadır. Bu bilgilere ulaşmakta yine bilgisayar teknolojileri kullanılarak yapılmaktadır.

2. Bilgisayar Sabotajı

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 lazımdır. 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 suçudur.

7. Diğer Suç Tipleri

Yukarıda bahsedilen suç tipleri kapsamına alamadığımız fakat teknolojinin gelişimiyle karşımıza çıkan suçlarda bulunmaktadır. Bunlardan en önemlisi ise; Bilgisayar ağları üzerinde sahte kişilik oluşturma ve kişilik taklidi. Öyle ki; çoğu zaman karşılaşılan "Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim" suçlarında genellikle kullanılan yöntemlerden biride budur. 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. Bunla birlikte bu dijital sertifikaların verileceği dijital noterlerinde hangi kurumlar olacağı üzerinde düşünülmesi gereken bir konudur.

Bunun gibi, teknolojinin ilerlemesi ile birlikte birçok yeni suç tipinin çıkması muhtemeldir. Bahsedilen suç tiplerine dikkat edildiğinde iki şekilde kategorize edebiliriz. Bunlardan birincisi; geleneksel suçların bilgisayar yolu ile işlenmesi diğeri ise yeni teknolojiler ile birlikte ortaya çıkan suç tipleridir. Bu suçların mağdurlarını en aza

indirmek için kanunlarımızda bu konuda yeterli düzeyde tanımlamaların yapılması gerekmektedir. Polis güçleri; kamu düzeni ve güvenliğinin sağlanmasının yanında, insanların temel hak ve hürriyetlerinden en iyi biçimde ve eksiksiz yararlanmasını temin etmekte görevlidir. Ancak bu konuda görevleri kanunlarla sınırlandırılmış bulunan Emniyet güçlerinin daha verimli çalışabilmesi için kanunlarda radikal değişimlerin yapılması gerekmektedir.

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 çihetine gitmektedirler. Bunlar ise; genel itibarıyla “sen benim bilgilerimi sildin bende seninkileri silerim” türünden davranışlar olmaktadır.

Diğer taraftan bazı suç tipleri ise; *kamu suçu* niteliği teşkil etmekte olup emniyet mensupları resen olarak müdahale etme yetkisine sahiptirler. Bu nedenle Emniyet Genel Müdürlüğü olarak yapmış olduğumuz çalışmaların devamında; Emniyet Teşkilatının nasıl bir yapılanmaya gitmesi gerektiği üzerinde durulmuştur. Bu noktada Emniyet Genel Müdürlüğü; bünyesinde kurulan Bilgisayar Suçları ve Bilgi Güvenliği Kurulu olarak çalışmalar yapılmaktadır. Bilgi İşlem Dairesi Başkanlığının koordinesi altında; Asayiş, Güvenlik, İnterpol, İstihbarat, Kaçakçılık ve Organize Suçlar, Kriminal Polis Laboratuvarları ve Terörle Mücadele ve Harekat Dairesi Başkanlıklarından yetkili personellerce kurulmuş bulunan Bilgi Güvenliği ve Bilgisayar Suçları Kurulu ile her daire başkanlığı kendi hizmetleri doğrultusunda Bilişim Suçları ile ilgilenmektedir. Daire başkanlıklarının görevleri ise şu şekildedir;

BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI

1. Bilişim teknolojilerini takip ederek, bilişim suçları alanındaki gelişmeleri araştırmak, tanımlarını yapmak ve ilgili daire başkanlıklarına bildirmek,
2. Yerli ve yabancı kurumlarla (Üniversite, Diğer ülkelerin polis teşkilatları, sivil örgütler) irtibata geçerek bilişim suçlarını incelemek ve ortak çalışmalar yapmak.
3. Bilgisayar Suçları ve Bilgi Güvenliği kurulunun çalışmalarını organize etmek,
4. Bilişim Suçları konusunda uzman personele gelişen teknolojiler hakkında bilgilendirici kurslar açmak; ile görevlidir.

İTERPOL DAİRESİ BAŞKANLIĞI

1. Bilişim suçları ile ilgili olarak uluslararası kuruluşlar ve Polis teşkilatlarıyla gerekli koordinasyonu yapmak,
2. İnterpol ve diğer uluslararası kurumlardaki konu hakkında gelişmeleri takip etmek ve ilgili daire başkanlıklarını bilgilendirmek,ile görevlidir.

KAÇAKÇILIK VE ORGANİZE SUÇLAR DAİRESİ BAŞKANLIĞI

1. Kanunsuz olarak bilgisayar yazılımlarının kopyalanmasının ve satışının takibi ve denetlenmesi,
2. Bilgisayar yoluyla dolandırıcılık ve sahtecilik suçlarının takibi ,ile görevlidir.

ASAYİŞ DAİRESİ BAŞKANLIĞI

1. Olay yeri incelemelerindeki delil toplamada bilgisayar ve ileri teknoloji ürünleri konusunda daha duyarlı olunması ve bu konuda uzman personel yetiştirilmesi, uzman personel olmadığı yerlerde bilgi işlem şubelerinden yardımcı personel alınması,
2. Yapılan uygulamalarda şüpheli kişilerin üzerinden çıkan ileri teknoloji ürünlerinin (databank,disket,CD) incelenmek üzere ilgili birime gönderilmesi ve bu konularda duyarlı olunması,
3. İnternet kafelerin denetlenmesi: Her ne kadar bu tür yerlerin açılması belediyeden alınan ruhsatlar ile olsa da İnternet vasıtasıyla pornografik yayınlar yapılabileceği gibi yine İnternet kullanılarak iç hukukumuzda aykırı eylemlerin yapılması muhtemeldir bu konularda da İnternet Kafelerin belli zamanlar içinde denetlenmesi gerekmektedir,

KRİMİNAL POLİS LABORATUVARLARI DAİRESİ BAŞKANLIĞI

1. Veri depolama medyalarının içerdiği suç delillerini (gizli dosyaları, silinmiş dosyaları, şifreleri, korumalı dosyaları) araştırmak, incelemek ve görüş bildirmek,
2. Veri depolamada kullanılan medyaların bırakabileceği fiziki izleri incelemek ve görüş bildirmek,ile görevlidir.

GÜVENLİK DAİRESİ BAŞKANLIĞI

İnternet ve dijital ortamda yayınlanan dergi, gazete ve benzeri yayınları incelemek, ile görevlidir.

TERÖRLE MÜCADELE DAİRESİ BAŞKANLIĞI

İnternet ortamındaki terör içerikli yasadışı sayfaları kendi yönetmelikleri gereği takip etmek ile görevlidir.

İSTİHARAT DAİRESİ BAŞKANLIĞI

İnternet ortamında yapılan faaliyetleri kendi istihbari yönetmelikleri gereği takip etmek ile görevlidir.

YAŞANAN PROBLEMLER

1. Elde Edilen Delillerin Kanuni Durumu

Suçluların 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 kayıtlardır. 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 değiştirilebilme ihtimali taşımaktadır. Böyle olunca sağlam bir delil olmaktan çıkmaktadır. Bilişim Suçlarında delil niteliği olan sadece bu kayıtlı bilgiler olduğundan bunların hukuki durumu tartışılmalıdır.

2. İnternet Servis Sağlayıcıları ve İnternet Kafelerin Sorumlulukları

Delillerin durumu nasıl önem taşımakta ise, bu kayıtları tutan kişiler veya kurumlarda büyük önem taşımaktadır. Çünkü bunların kayıtların tutulmasındaki standartlar kendileri tarafından belirlenmektedir. 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 alarak internet'e bağlanmanız gerekir. Böyle olunca suçu işleyen kişiye ait bilgiler buralarda otomatik olarak tutulur. Ancak her zaman için buradaki tüm bilgiler sistemi yöneten kişi tarafından ya silinebilme yada değiştirilebilme ihtimali taşımaktadır. Bu da suçun soruşturulmasında görevli emniyet güçlerinin suçluyu bulmada önemli rol oynayan delillere erişmesinde sakınca olmaktadır. İnternet Servis sağlayıcıları ve İnternet bağlantısı olan kurumlarda maliyeti nedeniyle bir kaç gün tutulan kayıtlar zaten esas amacı internet sağlamak olmayan ve umuma açık yerler statüsünde bulunan İnternet Kafelerde hiç bir şekilde tutulmamaktadır. 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.

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. Böyle olunca suça müdahale edecek polis güçleri ve suçun tahkikatında görevli savcı hakim ve avukatlarda yeterli teknoloji ile donatılmalı ve gerekli bilgi birikimine sahip olmalıdırlar.