

BİRİNCİ BÖLÜM .....	2
BİLİŞİM SUÇLARI ve HUKUK .....	2
GİRİŞ .....	2
MEVCUT HUKUKUMUZ VE BİLİŞİM SUÇLARI .....	3
A) Özel Hukuk Ve Bilişim Suçları .....	3
B) Kamu Hukuku Ve Bilişim Suçları .....	3
C) CEZA YARGILAMASI AÇISINDAN BAKIŞ .....	6
D) YETKİLİ MAHKEME AÇISINDAN BAKIŞ .....	7
İNTERNET KAFELER .....	7
ADALET BAKANLIĞININ KONU İLE İLGİLİ GÖRÜŞLERİ .....	9
SONUÇ: .....	9
İKİNCİ BÖLÜM .....	11
BİLİŞİM SUÇLARI SINIFLANDIRILMASI .....	11
1.Bilgisayar Sistemlerine Ve Servislerine Yetkisiz Erişim .....	11
1.1 Yetkisiz Erişim .....	11
1.2 Yetkisiz Dinleme .....	11
1.3. Hesap İhlali .....	11
2 Bilgisayar Sabotajı .....	12
2.1. Mantıksal Bilgisayar Sabotajı .....	12
2.2. Fiziksel Bilgisayar Sabotajı .....	12
3. Bilgisayar Yoluyla Dolandırıcılık .....	12
3.1. Banka Kartı Dolandırıcılığı .....	12
3.2 Girdi/Çıktı/Program Hileleri .....	12
3.3. İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma .....	13
4. Bilgisayar Yoluyla Sahtecilik .....	13
5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı .....	13
5.1. Lisans Sözleşmesine Aykırı Kullanma .....	13
5.2. Lisans Haklarına Aykırı Çoğaltma .....	13
5.3. Lisans Haklarına Aykırı Kiralama .....	14
6. Diğer .....	14
6.1. Kişisel Verilerin Suiistimali .....	14
6.2. Sahte Kişilik Oluşturma ve Kişilik Taklidi .....	14
6.3. Yasadışı Yayınlar .....	14
ÜÇÜNCÜ BÖLÜM .....	15
DiĞER ÜLKELERDE BİLİŞİM SUÇLARI ALANINDAKİ HUKUKİ VE İDARİ YAPILANMA .....	15
Giriş .....	15
Amerika Birleşik Devletleri: .....	16
Fransa: .....	16
İrlanda: .....	17
Hollanda .....	17
İspanya .....	18
İsrail .....	18
İsveç .....	18
İsviçre .....	18
Norveç .....	19
İtalya .....	19
Kanada .....	20
Yeni Zelanda .....	20
Hindistan .....	20
Malezya .....	21
Pakistan .....	21
Rusya .....	21
Singapur .....	22
DÖRDÜNCÜ BÖLÜM .....	23
EMNİYET TEŞKİLATI İÇERİSİNDEKİ İDARİ YAPILANMA .....	23
Giriş .....	23
1) İnternet ve Bilişim Suçları Araştırma ve Koordinasyon Merkezi Şube Müdürlüğü .....	24
2) Merkez Teşkilatındaki Yapılanma .....	24
3) Taşra Teşkilatındaki Yapılanma .....	24
Karşılaşılan Problemler Ve İhtiyaçlar .....	25
ŞEMA-1 .....	26

# BİRİNCİ BÖLÜM

## BİLİŞİM SUÇLARI ve HUKUK

### GİRİŞ

Gelişen teknolojiler hayatın her alanına akıl almaz bir hızla girerek 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 alanda olduğu gibi bu alanda da yeni suç tipleri ortaya çıkmış ve suçlularda 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 noktada bilişim suçu kavramı ortaya çıkmıştır. Bilişim suçları olgusu teknolojiyi kullanan ve kullanacak bütün ülkelerin ortak problemi haline gelmiştir. Bilişim teknolojilerindeki gelişmeler bilgisayar ağları sayesinde milli sınırları aşmıştır. Bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmaktadır. Bilişim suçları ile ideal bir mücadele, teknolojik gelişmeler ile globalleşen dünyada bu tip suçlara karşı dünya çapında bir işbirliği ile mümkündür. Dijital ortamın getirmiş olduğu bütün imkanları dünya devletleri suçla mücadelede kullanmadıkça bu alandaki suç tipleri ile mücadele başarılı olmak mümkün değildir.

Bilişim suçları teknolojik gelişmelere açık ülkelere öncelikli problem olarak kabul edilmiş ve bu alanda gerekli çalışmalar başlatılmıştır. Özellikle A.B.D ve Avrupa ülkeleri bu alandaki gerekli hukuki altyapılarını tamamlayarak gerekli idari yapılanmalarını düzenlemişlerdir. Mevcut kanunlarında düzenleme yapan ülkelerin hukuklarını incelediğimizde iki farklı yaklaşım ortaya çıkmaktadır. Birincisi Bilişim Suçlarını ayrı bir konu olarak değerlendirip Dijital ortamda işlenen suçlar için ayrı düzenlemeler yapmaktadırlar. İkincisi ise bu alanda işlenen suçların diğer suçlardan farklı olmadığı ve sadece mevcut kanunlarında dijital ortamı ifade eden düzenlemelerin yeterli olacağı görüşüdür. İki görüşünde kendine göre haklılık payı bulunmakla birlikte karma bir yaklaşım en sağlıklı olacaktır.

Bilişim suçlarını kısaca Bilgisayar ve iletişim teknolojileri kullanılarak işlenen suçlardır diye tanımlayabiliriz. Bu noktada iki farklı suç tipi karşımıza çıkmaktadır. Birincisi mevcut hukukumuzda tanımlanmış olup dijital ortamlarda ve bilgisayar teknolojileri kullanılarak işlenen suçlardır. Bu suçlara hakaret, dolandırıcılık, devlet aleyhine yürütülen faaliyetler vs yi örnek verebiliriz. İkincisi Mevcut hukuklarda düzenlenmemiş dijital ortamların varlığı ile ortaya çıkan suç tipleridir. Bu suç tiplerine örnek olarak Bilgisayar sistemlerine izinsiz girişleri verebiliriz.

Bir çok kişinin düşündüğü gibi ülkemizde bu alanda düzenlemeler yapılmamış değildir. Her ne kadar ideal manada bir düzenleme yapılmış bulunmamakla birlikte hukukumuzun bu alanda ki suçlarla mücadele etmek için yeterli olduğu söylenebilir. TCK unun 525. maddesi Bilişim alanında işlenen suçları düzenlemektedir.

## MEVCUT HUKUKUMUZ VE BİLİŞİM SUÇLARI

### A) Özel Hukuk Ve Bilişim Suçları

Hukuk sistemimiz incelendiğinde Bilişim alanında işlenen suçlar bakımından yetersiz olduğu anlaşılmakla beraber, ihtiyaca cevap verecek kadar, çözüm getirecek hükümleri bulunduğu da görülmektedir. Bunlar daha çok özel hukuk alanındadır. Bu ikinci kategori hükümler, demetinin de İnternet ile ilgili sorunlara amaca uygun çözüm getirecek surette tatbiki, hiç şüphesiz yine zaman alacak ve ciddi yorum tartışmalarına yol açacaktır. Ama yine de mevzuatımızın bu alanda tamamen yetersiz olduğu ve dolayısıyla İnternet ile ilgili çeşitli faaliyet ve uygulamaların başı boş kaldığı düşüncesi veya endişesi uyanmamalıdır.

İnternet'in sùjeleri arasındaki özel hukuk ilişkileri taraflar arasında yapılan sözleşmeye dayanmaktadır ve bu sözleşmelerin hukuki niteliđi, hüküm ve sonuçları İnternet hukukunun belli başlı konuları arasındadır.

### B) Kamu Hukuku Ve Bilişim Suçları

Yapılan incelemeler ortaya koymuştur ki, mevzuat özellikle kamu hukuku alanında yeni bir konu olmasından kaynaklanan sebeplerle belirsizlikler arz etmektedir.

İnternet'in asıl niteliđi ve karakteristiđini belirleyen özellikler dikkate alındığı zaman, kamu hukuku alanında getirilecek kurallara egemen olacak ilkelerin çok büyük bir titizlikle tespit edilmesi gerekmektedir. İnternet, niteliđi- hatta doğası ve varlık sebebi- icabı, serbest ve açık bir iletişim ortamıdır. Soruna bu açıdan bakıldığı zaman İnternet' in basit bir olay veya olađan bir teknik gelişme olarak ele alınmaması; fakat çađa damgasını vuran olađanüstü bir oluşum niteliđinde görülmesi gerektiđini söyleyebiliriz. Gerçekten, bilginin doğması, yayılması ve paylaşılması ve dolayısıyla tüm toplumlarda bilgi düzeyinin yükselmesi bakımından matbaanın icadı ne sağlamış ise, günümüzde de İnternet aynı ortamı sağlamakta ve hatta mukayese edildiğinde, çok daha ileri ve olađanüstü geniş kapsamlı sonuçlar yaratılmasına zemin hazırlamaktadır.

Hedef İnternet'in hukuk alt yapısının, kamu hukuku alanında da kısıtlayıcı olmaktan ziyade düzenleyici, istikamet verici ve hatta teşvik edici hükümler ile kurulmasıdır. İnternet ve Dijital alanda yapılacak kanuni düzenlemeler bu alanı sınırlamak ve kontrol altına almaktan ziyade kişi hak ve sorumluluklarını belirlemek ve koruma altına almak içindir. Kuşkusuz, bu hassasiyet içinde dahi, suç teşkil edecek veya kamu düzenini ihlal edici davranışların engellenmesini sağlayacak esaslara yer verilmesi bir zorunluluk olarak karşımıza çıkmaktadır. Ancak İnternet ortamındaki özgürlüklerin getireceđi faydalar değerlendirilerek, olanaklar ölçüsünde kısıtlayıcı hükümlere ve daha da önemlisi, kısıtlamayı teşvik edici ilkelere yer vermekten kaçınılması gereklidir.

### Bilişim Suçları ve Mevzuatımız:

Esasen bilgisayarla işlenen fiiller, temelde sahtecilik, dolandırıcılık, hırsızlık, karşılıksız yararlanma, ızzar ve benzeri suçlarda düzenlenen eylemlere benzerlik arz etmekteyse de, işin içine bilgisayar boyutu girince bunlar daha çok genişlik kazanmakta ve bu suçları işleniş şekli deđişmektedir. Bu sebeple, mevcut ceza hükümlerine bilgisayar boyutu eklenmeden bu eylemleri karşılayabilmek pek mümkün olmamaktadır. Örneđin; dolandırıcılık suçu kişilerin aldatılması marifetiyle mülkiyete ilişkin menfaatlerin ihlalini cezalandıran bir suçtur ve bilgisayara yani makineye yönelik gerçekleştirilen bir takım hileli ve aldatici hareketlere dolandırıcılık denilebilmesi oldukça zordur. Yine, sahtekarlık suçu

için özel veya resmi bir varakanın tahrifi, hırsızlık suçu için menkul bir malın sahibinin rızası hilafına alınması gerekirken, yerine göre dijital ortamda elektronik değer olan bir akımın silinmesi veya değiştirilmesi yahut kopyalanması elde edilmesinin ne derece hırsızlık veya sahtecilik yahut ızzar suçuna vücut vereceği tartışmaya açıktır. Bu gibi sebeplerle, bilgisayar suçlarının ceza kanunları ile karşılanabilmesi için kanun koyucular mevzuatlarında yeni bir takım düzenlemeler yapmaktadır.

Mukayeseli hukukta bilgisayarla ilgili suçların düzenlenmesinde, temelde iki sistemin izlendiği görülmektedir. Buna göre, ya bu hususta yeni ve özel bir düzenleme meydana getirilmekte ya da mevcut hükümlerde değişikliğe gidilmektedir.

Dünyadaki gelişmelere paralel olarak Türkiye’de de bilgisayar kullanımı, olumlu ve olumsuz yönleriyle yaygınlaşmaktadır. Bu teknolojik gelişme karşısında Türk Kanun Koyucusu, bir yandan mevzuatta kendini hissettiren ihtiyaçları karşılayabilmek, bir yandan tavsiye kararlarına uyum sağlayabilmek amacıyla hukuki alanda bazı düzenlemeler yapma ihtiyacını hissetmiştir. Gerçekten, kanun koyucu bilgisayar suçlarına ilişkin ilki 1991 yılında, 3756 s.k’la TCK.’nun ikinci kitabına bazı bilgisayar suçlarını öngören “Bilişim Alanında Suçlar” başlıklı 11. babı ilave etmiştir. Bunu takiben 1995 yılında, bilgisayar programlarının “eser” sayılacağını belirleyen bir değişiklik yapılmış ve bilgisayar programlarına karşı gerçekleştirilen bir takım eylemler de yaptırım altına alınmıştır.

3756 S.K.la TCK. nun 2. Kitabına 11.babı olarak ilave olunan “Bilişim Alanında Suçlar”, 525a, 525b, 525c ve 525d maddeleri olmak üzere dört maddeden oluşmaktadır. 525d maddesi hariç, 525a, b ve c maddelerinde feri cezalar yer almaktadır. 525a, b ve c maddesinde “bilgileri otomatik olarak işleme tabi tutmuş bir sistemden bahsetmek suretiyle bilgisayarlar kast edilmektedir. 525a/1 ve 2, 525b/1 maddelerinde bilgisayar, suçun konusunu oluşturmakta, 525b/2 ve 525c maddelerinde ise suçta araç vazifesini görmektedir.

TCK. Md 525 a/1’ de, Bilgileri otomatik işleme tabi tutmuş bir sistemden “programları, verileri veya diğer herhangi bir unsuru hukuka aykırı olarak ele geçirmek” yaptırım altına alınmak suretiyle “Bilgisayar sistemlerinde bulunan programlar ve bilgiler” hukuki olarak koruma altına alınmıştır.

TCK md.535 a/2’ de, “Bir programı, verileri veya diğer herhangi bir unsuru başkasına zarar vermek üzere kullanmak, nakletmek veya çoğaltmak” eylemleri yaptırım altına alınmaktadır.

TCK md.525 b/1’ de, “Başkasına zarar vermek veya kendisine veya başkasına yarar sağlamak maksadıyla, bilgileri otomatik işleme tabi tutmuş bir sistemi veya verileri veya diğer herhangi bir unsuru kısmen veya tamamen tahrip eden veya değiştiren veya silen veya sistemin işlemesine engel olan veya yanlış biçimde işlemesini sağlayan” kimselerin fiilleri yaptırım altına alınmak suretiyle bilgisayar ve sistemlerine veya bunlardaki veri, program ve diğer unsurlara karşı gerçekleştirilen ızzar eylemleri yaptırım altına alınmaktadır.

TCK. Md.525 b/2’ de, “ Bilgisayar kullanmak suretiyle kendisini veya başkasını lehine hukuka aykırı yarar sağlamak” suç olarak düzenlenmektedir.

TCK. Md.525 c’de ise, “ Hukuk alanında delil olarak kullanılmak maksadıyla sahte bir belgeyi oluşturmak için bilgileri otomatik olarak işleme tabi tutan bir sisteme , verileri veya diğer unsurları yerleştiren veya var olan verileri veya diğer unsurları tahrif eden kimsenin fiili yaptırım altına alınmaktadır. Madde de ayrıca, “tahrif edilmiş olanları bilerek kullananlara ... hapis cezası verilir” demek suretiyle de yukarıdaki suça ilaveten sahtecilik mahsulü bir belgenin bu niteliği bilinerek kullanılması da ayrıca kullanma suçu olarak düzenlenmektedir.

Ceza Hukukumuz açısından bir eylemin suç teşkil edebilmesi için tipe uygunluk, hukuka aykırılık ve kusurluluk unsurlarının bir arada olması gerekir. Esasen Ceza Hukukumuzda bir çok suç türü için işleniş şekli çok sıkı şekil şartları bağlanmamıştır. Bir

suçun işlenmesinde İnternet aracı olarak kullanılmışsa ve bu suçun işleniş şekli özel bir şarta bağlanmamışsa faillerin tespit edilmesi ve delillendirilmesi durumunda cezai müeyyideler uygulanabilecektir. Hakaret, sövme, müstehcen yayın, suçların övülmesi, suça tahrik, adli teşkilatın işleyişine tecavüz, devletin güvenliğine karşı suçlar, devlet memurlarına hakaret, yalan haber yaymak gibi ceza kanunlarında veya basın-yayın ile ilgili mevzuatta yer almış pek çok suç çeşidinin İnternet yoluyla işlenmesi durumunda da bu fiilleri yapanlar cezalandırılabilir. Ancak Ceza Hukuku doktrininde bu konu henüz tam olarak irdelenmemiştir.

Bilgisayar sistemleri kullanılarak yapılan dolandırıcılık, sahtekarlık, ızzar ve benzeri suçlar TCK'nde gerek klasik kanunlarınızla gerekse bilişim suçlarını düzenleyen TCK'nun 525. maddesiyle faillerinin tespiti halinde cezalandırılabilir.

Bilgisayar ve bilgisayar ağları, bir taraftan klasikleşmiş suç çeşitlerinin gerçekleştirilmesine elverişli bir ortam oluşturduğu gibi, bir taraftan da gerçekleştirilmesine olanak verdiği bazı eylemler dolayısıyla yeni suçları da yaratan bir faaliyet alanı olarak ortaya çıkmaktadır. Bu çerçevede gerekli hukuki alt yapı gözden geçirilerek gerekli düzenlemelerin yapılması kaçınılmazdır.

Bu alandaki en çarpıcı örnekler müstehcen yayınlar ve İnternet üzerinden oynan kumar oyunlarıdır ve mevcut yayınların İnternet'e aktarılmasıdır.

Müstehcen ve pornografik yayınların İnternet üzerinden işlenmesi durumunda da tipe uygunluk, hukuka aykırılık ve kusurluluk unsurlarının bir arada olması nedeniyle faillerin tespit edilmesi halinde TCK'na göre cezalandırılabilir. Zira TCK'nun 426. maddesinde "Halkın ar ve haya duygularını inciten veya cinsi arzularını tahrip ve istismar eden nitelikte genel ahlaka aykırı; her nevi kitap, gazete, risale, mecmua, varaka, makale, ilan, resim, tasvir, plak, afiş, pankart, televizyon ve teyp bantları, fotoğraf, sinema ve projeksiyon filmleri veya diğer anlatım araç ve gereçleri ile...bu fiilleri icra edenler tedarik edenler, tedarik edileceğini ilan edenler ve ilan ettirenler 2 milyon liradan 10 milyon liraya kadar ağır para cezası ile cezalandırılır." denmektedir.

İnternet üzerinden interaktif olarak kumara izin veren ülkelerde açılmış Web sayfaları üzerinden yapılan yayınlarda cezai müeyyide uygulanmamaktadır. TCK'nun 567. maddesinde "her kim umuma mahsus ve umuma açık yerlerde kumar oynatır veya oynatmak için yer gösterirse....cezalandırılır." denmektedir. İnternet ortamı umuma mahsus ve umuma açık yer olarak kabul edilemeyeceğinden işlenen eylem tipe uygunluk açısından bire bir uymamaktadır. Bu nedenle de cezai müeyyide uygulanamayacaktır.

Elektronik iletişimin yayılması ile özellikle İnternet ve web sayfası yayını sureti ile insanlar arasında yeni bir iletişim türü ortaya çıkmıştır. Eskiden bir dergi, kitap yayıncısı tarafından çoğaltılıp alıcısına gönderilmekte iken, günümüzde alıcı, yayıncının web sitesine başvurmakta kendisi "kopya/ suret" çıkartarak bilgisayarına transfer etmektedir. İnternet üzerinde yayın yapan milyonlarca web sitesi bulunmaktadır. Bu web sitelerinin bazıları periyodik yayınlar (elektronik gazete gibi.) Bazıları ise periyodik olarak güncellenen yayınlardır. İnternet üzerindeki bu tür yayınları Basın Kanunu açısından değerlendirdiğimizde Basın Kanununda dijital biçimde basılma, neşir tabiri yoktur. Bu nedenle çok kısa süre içinde web yayıncılığının niteliği üzerinde tartışmalar sonuçlarını vermeye başladıkça Basın Kanununun adından başlayarak ciddi değişiklikler geçirmesi beklenmektedir.

## **Cezada Sorumluluk**

Ceza hukukunda tartışılan konulardan birisi de İnternet aracılığı ile gerçekleştirilen eylemlerde ve İnternet eylemlerinde sorumluluğun kime ait olacağıdır. Bu konuda da henüz

belirgin bir düzenleme yapılmamıştır. İnternet hizmeti veren kuruluşun, işlenen suçtan haberdar olmasına rağmen yayın faaliyetine devam etmesi veya resmi mercilerin herhangi bir uyarısına rağmen eylemi sürdürmesi, kısaca iştirak kurullarının geçerli olabilmesi durumunda, bu kuruluşların da sorumluluğu yönüne gidilebilecektir. Hizmet veren kuruluşların sorumlulukları söz konusu olunca, ceza hukuku yönünden sorumlu kişilerin, kanuni düzenleme içerisinde belirlenmesi önemli bir gereklilik olarak ortaya çıkmaktadır.

Mukayeseli hukukta İnternet eylemlerini veya İnternet yoluyla işlenen fiilleri cezai yaptırıma bağlayan temel yaptırım olmamasına rağmen, bu konudaki tartışmaların henüz yeterince olgunlaşmadığı bilinen bir gerçektir.

Öte yandan Dünyada meydana gelen sosyal, siyasal ve ekonomik değişiklikler dolayısıyla eskiyen değerlere dayalı 765 sayılı Türk Ceza Kanununu çağa uydurmak amacıyla daha önceden hazırlanan “Türk Ceza Kanunu Ön Tasarısı” nı gözden geçirip gerekli değişiklikleri ve geliştirmeleri yapmak üzere, 21.12.1999 tarihinde bilim adamları ve uzman personelden oluşturulan komisyon, çalışmalarına devam etmektedir. Bu nedenle İnternet üzerinden işlenen suçlarla ilgili yasal düzenlemeler bu komisyon çalışmalarında değerlendirilmesi uygun olacaktır.

### **C) CEZA YARGILAMASI AÇISINDAN BAKIŞ**

Suç oluşturduğu iddia edilen eylemleri, devletin yasalarla, görevlendirdiği makamlar tarafından, yasalarla önceden belirlenmiş kurallar çerçevesinde, iddia-savunma-yargı üçlüsü içinde değerlendirmek, ceza yargılamasının en kalın çizgileri ile tanımlamasıdır.

Bu değerlendirmenin yapılması, devletin cezalandırma hakkının bir sonucudur. Aynı sonuç, yargılanan sanığın suçlu bulunması halinde, yasalarda öngörölmüş cezalarla cezalandırılmasıdır.

Bu tablo, Bilişim suçlarında (hem İnternet yolu ile işlenen suçlar ve hem de dar anlamda İnternet suçları) tümüyle geçerlik taşıyacaktır. Ceza yargılaması yasalarının ülkeselliği ilkesinin gereği olarak, Türk yasalarının egemen olduğu alanlar içinde bir suç işlendiğinde, ceza yargılaması mekanizması harekete geçecek ve sonuçlarını doğuracaktır. TCK incelendiğinde hem mülkîlik hem de şahsîlik ilkesi esas alınmaktadır. TCK Madde 3- (Kanunun Yer Bakımından Uygulanması): Türkiye’de suç işleyen kimse, Türk kanunlarına göre cezalandırılır ve bundan dolayı bir Türk hakkında yabancı memlekette hüküm verilmiş olsa bile Türkiye’de muhakeme olunur. Böyle bir fiilden dolayı Türkiye dışında hakkında hüküm verilmiş olan yabancı dahi Adliye Vekilinin talebi üzerine Türkiye’de muhakeme edilir. Madde 4-(Yabancı Memlekette Devlete Karşı İşlenen Suç): Bir Türk veya yabancı, yabancı memleketlerde Türkiye Devletinin şahsiyetine karşı bir cürümü veya bu Kanunun 316, 317, 318, 319, 320, 323, 324, 332, 333 üncü maddelerinde yazılı suçları işlerse, hakkında resen takibat yapılarak bu maddelerdeki cezalarla cezalandırılır. (1991/3756) Bunlar hakkında yabancı memleketlerde evvelce hüküm verilmiş olsa bile Adliye Vekilinin talebi üzerine Türkiye’de tekrar muhakeme olunur. Yabancı memleketlerde Türkiye namına memuriyet veya vazife deruhte etmiş olup da bu memuriyet veya vazifeden dolayı bir cürüm işleyen kimse hakkında Türkiye’de takibat yapılır. (1933/2275, 1987/3352, 1987/3354, 1991/3756) Madde 5- (Yabancı Memlekette Türk’ün İşlediği Suç): Bir Türk dördüncü maddede yazılı cürümlerden başka, Türk kanunlarına göre aşağı haddi üç seneden eksik olmayan şahsî hürriyeti bağlayıcı bir cezayı müstehzim cürümü yabancı memlekette işlediği ve kendisi Türkiye’de bulunduğu taktirde Türk kanunlarına göre cezalandırılır. Eğer cürümün aşağı haddi üç seneden az şahsî hürriyeti bağlayıcı bir cezayı müstehzim ise takibat icrası zarar gören şahsın veya yabancı Hükümetin şikayetine bağlıdır. Mağdur yabancı ise bu fiilin, işlendiği mahal kanunlarında da cezayı müstehzim olması şarttır.

(1936/3038, 1937/3112) Madde 6-(Yabancı Memlekette Yabancı'nın İşlediği Suç): Bir yabancı dördüncü maddede yazılı cürümlerden başka, Türk kanunlarına göre aşağı haddi bir seneden eksik olmayan şahsi hürriyeti bağlayıcı bir cezayı müstehzim cürümü yabancı memlekette Türkiye'nin veya bir Türk'ün zararına işlediği ve kendisi Türkiye'de bulunduğu takdirde Türk kanunları mucibince ceza görür. Ancak bu babda takibat icrası Adliye Vekilinin talebine veya zarar gören şahsın şikayetine bağlıdır. Eğer cürüm bir yabancı'nın zararına işlenmiş ise fail, Adliye Vekilinin talebi üzerine, aşağıdaki şartlar dairesinde cezalandırılır.

1-Türk kanunlarına göre şahsi hürriyeti bağlayıcı ve aşağı haddi üç seneden eksik olmayan cezayı müstehzim bir fiil olmak,

2-İadesi mücrimin muahedesi bulunmamak veyahut iade keyfiyeti, cürümün irtikap edildiği mahallin veya failin tebaasından bulunduğu Devletin Hükümeti tarafından kabul edilmemiş bulunmak.

Bir Türk veya yabancı, Türk Ceza Kanununun 8 inci babının 3 üncü faslındaki cürümleri yabancı memlekette işlerse resen takibat yapılarak o fasılda yazılı maddelerdeki cezalarla cezalandırılır. (1933/2275, 1936/3038)

## **D) YETKİLİ MAHKEME AÇISINDAN BAKIŞ**

Türk sistemi bugün için genel ilke olarak suçun işlendiği yerdeki mahkemelere yetki vermektedir. Bu yer bilinmediği hallerde, yargı yeri yedek kurallarla belirlenmektedir. Bu tür kurallara ihtiyaç olduğu da açıktır, çünkü ceza yargılamasında, fiili yargılayacak mahkeme bulunmadığı için yargılamayı yapamamak hiçbir şekilde söz konusu olamaz.

Türk sistemi, özellikle basın yolu ile işlenen suçlarda, birden çok yere yetki vermek ilkesini de benimsemektedir. Bu yerler, suçun işlendiği yer, mağdurun ikametgahı olarak değişebilmektedir.

İnternet vasıtası ile işlenen suçlar açısından olaya yaklaştığımızda, ilk belirleyeceğimiz sonuç, İnternet yolu ile suç teşkil eden eylemlerin yapılması ile, suç teşkil eden neticenin kendiliğinden doğmasıdır. Bu durumda, İnternet suçları yönünden suçun işlendiği yeri tespit güçlüğü yoktur. Bu nedenle, suçun işlendiği yere yargı yetkisi vermek uygun bir çözümdür. Bunun yanı sıra, özellikle kişileri hedef alan suçlarda, bu kişilerin ikametgahlarının bulunduğu yer mahkemesinde de yetki vermek yargıyı kolaylaştıracaktır.

Günümüzde suç işlemekte vasıta olarak İnternet ortamı kullanılmaktadır. Fakat, bunların büyük bir çoğunluğunun faaliyetlerini yurt dışında yaptığı bilinmektedir. Dolayısıyla failleri tespit ve yakalamak imkansız hale gelmektedir. Bu sorunun çözüm yolu, Uluslararası alanda yapılacak ve İnternet yolu ile işlenen suçların engellenmesine ve hatta faillerin iadesini düzenleyen bir anlaşma yapılmasıdır. Yurt içinde işlenen suçlarla ilgili olarak ise; esasen mevzuatımızdaki suç tanımlamaları bakımından önemli bir sorun olmamakla birlikte fail ve fiil arasındaki ilişkiyi kurma hususunda güçlükler vardır.

Bu konuda yapılması gereken temel çalışma, İnternet vasıtasıyla suç işleyen faillerin tespiti ve suç ile fail arasındaki illiyet bağına net bir şekilde ortaya koyabilecek teknolojik donanıma kavuşulmasıdır.

## **İNTERNET KAFELER**

Bilgisayar ve İnternet kullanımına paralel olarak ülkemiz iktisadi ve sosyal yapısına yeni bir sektör olarak giren ve sayıları hızla artan İnternet kafelerin açılması, denetlenmesi, küçük yaştaki çocukların buralara girip giremeyeceği gibi konularda, Bakanlığımıza intikal eden yazılı ve şifahi taleplerden uygulamada ciddi tereddütler olduğu ve bu tereddütlerin

giderilmesi, uygulamada yeknesaklığın sağlanması için bazı açıklamaların yapılması zorunlu görüldüğünden 01.03.2000 gün ve B.05.1.EGM.0.11.03.05.00054 sayılı genelge hazırlanmış olup;Bu genelge ile;

-Daha önce 02/12/1998 tarih ve 233 sayılı genelgemizle Belediyelerden aldıkları ruhsatla faaliyette bulunabilecekleri bildirilen İnternet kafelerin, 30/12/1999 tarih ve 23922 sayılı Resmi Gazetede yayımlanan 99/13681 karar sayılı “Açılması İzne Bağlı Yerlere Uygulanacak İşlemler Hakkında Yönetmelik”le, açılması Mahallin En Büyük Mülki Amirin iznine tabi yerler kapsamına alındığı,

-Müşterilere, içerisinde bulunan İnternet bağlantılı bilgisayarlar sayesinde uluslararası bilgi iletişim ağına erişim imkanı sağlayan ancak, içerideki bilgisayarlarla oyun oynanmasına müsaade edilmeyen İnternet kafelerin açılmasına izin verilirken bunlarda eğitim-öğretim kurumlarına 200 metre uzaklıkta bulunma zorunluluğu aranmayacağı, bu yerlerde İnternet bağlantılı bilgisayarlar dışında hiçbir şekilde 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun Ek 8 inci maddesinde belirtilen elektronik veya mekanik oyun alet ve makinaları bulundurulmayacağı, ayrıca bilgisayarlarla oyun oynatılmasına da müsaade edilmeyeceği,

-İnternet bağlantılı bilgisayarların yanı sıra 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun Ek 8 inci maddesinde belirtilen nitelikte elektronik veya mekanik oyun alet ve makinaları (atari, okey ve benzeri) bulundurulmak veya bilgisayarlarda oyun oynatılmak suretiyle, Yönetmeliğin 4 üncü maddesinde tanımı yapılan, oyun ve eğlence amacına yönelik “oyun yeri” gibi işletilmek istenen yerler için 200 metre uzaklık şartının aranacağı, bu yerlerin izin belgelerinde oyun yeri niteliğinde olduğu belirtileceği ve 18 yaşından küçüklerin girmesine müsaade edilmeyeceği, izinsiz olarak açılan bu tür yerler 2559 sayılı Polis Vazife ve Salahiyet Kanunu’nun 7. maddesinin ikinci fıkrasına göre kapatılacağı,

-Eğitim-öğretim kurumları, kütüphaneler, kamu kurumları, kamu kurumu niteliğindeki meslek kuruluşları, dernekler, sendikalar ve benzeri kuruluşlara ait ve yalnız kendi üyeleri veya personeline açık olan yerlerde kurulan İnternet kafelerin yönetmelik kapsamında mütalaa edilmeyeceği,

-Kumar, bahisler ve pornografik yayın içerikli siteler, Devletin ülkesi ve milleti ile bölünmez bütünlüğünü zedeleyici ve anayasal düzeni yıkma amacına yönelik kurulan sitelere yapılan yazılı tebligata rağmen bu tür web sitelerinin kullanımına müsaade edilen, Lisanssız ve bandrolsüz her türlü film, bilgisayar yazılımı, bilgisayar ortamında tutulan veri ve bilgisayar oyunlarına ait CD ve benzeri ekipmanların yasa dışı olarak kopyalanması, kiralanması veya kopyalanarak satılması, İnternet vasıtasıyla diğer bilgisayarlara veya bilgisayar ağlarına kasten zarar verilmesi veya izinsiz oyun yeri gibi işletilen İnternet kafeler hakkında öncelikle yazılı uyarılarda bulunulacağı, yazılı uyarılara rağmen bu siteleri açık tutan İnternet kafeler için, 2559 sayılı Polis Vazife Salahiyet Kanunu’nun 8 inci maddesine göre kapatma işlemi uygulanacağı,

-15 yaşından küçüklerin İnternet kafelere alınmasına müsaade edilmeyeceği, 18 yaşından küçüklerin, akşam belli bir saatten sonra yanında ailesi olmadan İnternet kafelere alınıp alınmayacağı hususu, küçüklerin korunmasına dair mevzuat hükümleri ile 5442 sayılı İl İdaresi Kanunu’nun 11/c veya 32/ç maddesi hükümlerinin esas alınarak Mülki Amirliklerce değerlendirileceği ve bu hususunda önceden işletmeciye tebliğ edileceği,

-İnternet kafelerin açılış ve kapanış saatlerinin ilgili Bakanlık, Kuruluş ve Valiliklere gönderilen 01.02.2000 gün ve 00029 sayılı genelge hükümlerine göre, kolluk amirliğinin görüşü de alınarak, mahallin en büyük amirinin onayı ile belediyelerce belirleneceği gibi çeşitli konularda düzenlemelere yer verilmiştir.

Bunların yanında İnternet kafelere giden küçük yaştaki çocukların velilerinden gelen taleplerle düzenlenen 15 yaş sınırının İnternet kafelerde yapılacak düzenlemelerle küçük

yaşta çocuklarında istifade edebileceği ortamlar haline getirilerek yaş sınırının kaldırılması veya daha aşağılara çekilmesi toplumsal olarak İnternet'ten istifade adına önemli bir adım olacaktır.

## **ADALET BAKANLIĞININ KONU İLE İLGİLİ GÖRÜŞLERİ**

Dünyada bilişim alanında yaşanan hızlı gelişmelerin insan yaşamını ve ilişkilerini değiştirip, etkilemesi sebebiyle yeni suç tipleri ve hak ihlallerinin gündeme gelmesi, yeni bir iletişim ve bilgi aracı olmasının yanı sıra, teknik yönü de ağır basan İnternet kanalıyla; Ülkemiz veya diğer ülkeler üzerinden ceza mevzuatımıza özü itibariyle aykırı fakat işleniş şekli, zamanı ve mahiyeti ile farklılık gösteren yayınların yapılması sebebiyle, ayrıca terör örgütlerinin propaganda amaçlı devlet aleyhine yayınları, kumar, bahis, pornografik yayın, fuhşa aracılık, bilgisayar sistemlerine ve hizmetlerine yetkisiz erişim, bilgisayar sabotajı bilgisayar yoluyla dolandırıcılık, sahtecilik, kanunla korunmuş yazılımın izinsiz kullanımı, yasadışı yayınlar, verilerin suiistimali gibi eylemlerle daha etkin olarak mücadele edilebilmesi için bilgisayar teknolojileri konusunda bu yeni oluşumun teknik ve hukuki yönden düzenlenmesi gerektiğinden İnternet üzerinden işlenen bu tip eylemlerin suç kapsamında değerlendirilip değerlendirilemeyeceği ile hukuki takip prosedürünün ne olacağı konusunda Adalet Bakanlığında 12.04.2000 gün ve B.05.1.EGM.0.11.20/090360 sayılı yazı ile görüş istenilmiş olup; Alınan 03.05.2000 gün ve B.03.0.KGM.0.00.00.01.430 sayılı cevabı yazıda İnternet'in gelişimine bugün için ülkeler düzeyinde yaklaşıldığında yapılan ilk tespitin İnternet'in ifade özgürlüğünün kullanıldığı bir alan olduğu, bu nedenle iletişim özgürlüğünden yararlanmak sureti ile İnternet'in yaygınlaştırılması ve kitle iletişiminin en üst düzeye çıkarılmasının temel amaç kabul edildiği, bu konuda yapılabilecek hukuki düzenlemelerde değişik menfaatleri dengelemenin bir zorunluluk olarak görüldüğü belirtilmektedir.

Dünyada meydana gelen sosyal, siyasal ve ekonomik değişiklikler dolayısıyla eskiyen değerlere dayalı 765 sayılı Türk Ceza Kanununu çağa uydurmak amacıyla daha önceden hazırlanan "Türk Ceza Kanunu Öntasarımı"ni gözden geçirip gerekli değişiklikleri ve geliştirmeleri yapmak üzere, 21.12.1999 tarihinde bilim adamları ve uzman personelden oluşturulan Komisyonun çalışmalarına devam ettiği ve bu konunun da bir bütünlük içinde Kanunlar Genel Müdürlüğünce Komisyon çalışmaları sırasında değerlendirilmesinin daha uygun olacağı ifade edilmiştir.

### **SONUÇ:**

İnternet üzerinden işlenen suçlarla ilgili cezai yaptırıma bağlayan temel bir yasa, İnternet'in bilgi ve iletişim aracı olması, çok hızlı gelişim göstermesi, teknolojik yönünün ağır basması ve tüm ülkeler arası bağlantıya sahip olması nedeniyle gerek hukukumuzda gerekse mukayeseli hukukta henüz bulunmamaktadır. Bu konuda genel eğilim demokratik bir toplumda serbest toplumsal fikir alış-verişini sağlayacağı toplumsal yarar, İnternette sansürün sağlayacağı toplumsal yarardan çok daha önemlidir. Bu nedenle müstehcen yayınlar ile şiddete dayalı yayınların önlenmesinde klasik basın hukuku düzenlemeleri ile önlenmesi genel kabul görmektedir. İnternet hizmeti veren kuruluşun sorumluluklarının ne şekilde olacağı ise mutlaka kanuni düzenleme ile belirlenmesi gerekmektedir.

Müstehcen ve pornografik yayınlara ilişkin olarak öngörülen cezai müeyyideler çok hafif para cezaları olduğundan caydırıcılık niteliği bulunmamaktadır. Ayrıca çocuk pornografisi içeren yayınlar için ise ayrı bir düzenleme mevcut olmadığından genel müstehcen ve pornografik yayınlara ilişkin cezai müeyyidelere tabii olmaktadır. Gelişmiş

ülkelerde bu alanda hürriyeti bağlayıcı cezalar verilerek düzenlenen çocuk pornografisi konusu bu tip suçların ülkemizde de yayılması göz önüne alınarak tekrar düzenlenmeli ve özel hükümler getirilmelidir. Bir diğer sorun da İnternet vasıtasıyla suç işleyen faillerin tespiti ve suç ile fail arasında illiyet bağıını net bir şekilde ortaya koyabilecek teknolojik donanım eksikliğidir. İnternet üzerinden işlenen suçlarla kapsamlı bir şekilde mücadele edilebilmesi için;

Yeni hazırlanan Türk Ceza Kanunu Ön Tasarısına İnternet üzerinden işlenen suçlarla ilgili düzenlemeler yapılmalı ve diğer müstehcen, pornografik ve özellikle de çocuk pornografisine ilişkin ceza müeyyideler caydırıcı bir yapıtıma bağlanmalıdır.

İnternet üzerinden yapılan yayınların Basın Kanununda yapılacak deęişikle açık bir şekilde bu kanuna dahil edilerek gerekli düzenlemeler yapılmalıdır.

İnternette veya dijital ortamda yer alan verilerin ve kişilere ilişkin özel bilgilerin deşifre edilmesi riskine karşı cezai önlem alınması ve özel hayatın korunması çerçevesinde tekrar kanuni düzenlemeler getirilmesi gerekmektedir.

İnternette yer alan faaliyetlerin takibi, tespiti ve yakalanması ancak uzmanlaşmış personel ve sürekli bir çalışma ile mümkün olacaktır. Her gün deęişen ve gelişen bilgisayar teknolojisinin gerisinde kalmamak için bilinen klasik polisliğin ötesinde teknik donanıma sahip gerek kolluk kuvvetlerinde gerekse adalet bakanlığı içinde konu hakkında uzman personelin istihdamı bugün için olmasa dahi yarının Türkiye'sinde bir zarurettir. Bu sebeple en kısa zamanda bu alandaki eğitim ve yapılanma çalışmaları başlatılmalıdır.

İnternet vasıtasıyla suç işleyen faillerin tespiti ve suç ile fail arasında illiyet bağıını net bir şekilde ortaya koyabilecek teknolojik donanım sağlanmalıdır. Bu konu gerekirse ISS lerin kurulmasına ilişkin yapılacak düzenlemelerle standart hale getirilmelidir. Bu sayılan konularla birlikte en önemli husus bu alandaki uluslararası düzenleme ve işbirliği eksikliğidir. Uluslararası alanda İnternet yolu ile işlenen suçların engellenmesini ve hatta faillerin iadesini düzenleyen bir uluslararası anlaşmanın yapılması gerekmektedir.

## İKİNCİ BÖLÜM

### BİLİŞİM SUÇLARI SINIFLANDIRILMASI

Bilişim alanındaki suç tiplerini incelerken İnterpol Genel Sekreterliğinin hazırlamış olduğu “İnterpol Computer Crime Manual” esas olmak üzere, Birleşmiş Milletlerin hazırlamış olduğunu “United Nations Manual on The Prevention and Control of Computer-Related Crime” kitapçığı ve Avustralya Polis Teşkilatının hazırlamış olduğu “Minimum Provisions for The Investigation of Computer Based Offences” kitapçıklarından istifade edilerek aşağıdaki suç tipleri belirlenmiştir. 11.06.1999 tarihinde hazırlanan BİLİŞİM SUÇLARI raporunda tanımlanmış olan suç tipleri mevcut kanunlar ve uygulamalar göz önüne alınarak yeniden düzenlenmiştir.

#### 1.Bilgisayar Sistemlerine Ve Servislerine Yetkisiz Erişim

##### 1.1 Yetkisiz Erişim

**Tanım:** Bir bilgisayar sistemine yada bilgisayar ağına yetkisi olmaksızın erişmektir.

**Açıklama:** Suçun hedefi bir bilgisayar sistemi yada ağıdır. “Erişim” sistemin bir kısmına yada bütününe ve programlara veya içerdiği verilere ulaşma anlamındadır. İletişim metodu önemli değildir. Bu bir kişi tarafından bir bilgisayara direkt olarak yakın bir yerden erişebileceği gibi, uzak bir mesafeden örneğin bir modem hattı yada başka bir bilgisayar sisteminden de olabilir.

##### 1.2 Yetkisiz Dinleme

**Tanım:** Bir bilgisayar veya ağ sistemine, sisteminden veya sistemi içinde yapılan iletişimin yetkisi olmaksızın teknik anlamda dinlenmesidir.

**Açıklama:** Suçun hedefi her türlü bilgisayar iletişimidir. Genellikle halka açık ya da özel telekomünikasyon sistemleri yoluyla yapılan veri transferinin teknik olarak takip edilmesi ve dinlenmesidir.

Teknik anlamda dinleme, iletişim içeriğinin izlenmesi, verilerin kapsamının ya direk olarak (bilgisayar sistemini kullanma yada erişme yoluyla) ya da dolaylı olarak (elektronik dinleme cihazlarının kullanma yoluyla) elde edilmesi ile ilgilidir.

Suçun oluşması için hareket yetkisiz ve niyet edilmiş olarak işlenmesi gerekir. Uygun yasal şartlar çerçevesinde soruşturma yetkililerinin yaptıkları bu kategoriye girmez.

##### 1.3. Hesap İhlali

**Tanım:** Herhangi bir ödeme yapmaktan kaçınma niyetiyle bir başkasının bilgisayar sistemlerinde bulunan hesabını kanunsuz olarak kullanmaktır

**Açıklama:** Bir kişinin, İnternet, telefon veya benzer bir sistemdeki hesabının kişinin rızası olmaksızın kanunsuz olarak kullanılmasıdır.

## **2 Bilgisayar Sabotajı**

### **2.1. Mantıksal Bilgisayar Sabotajı**

**Tanım** : Bir bilgisayar yada iletişim sisteminin fonksiyonlarını engellenme amacıyla bilgisayar verileri veya programlarının sisteme girilmesi, yüklenmesi, değiştirilmesi, silinmesi veya ele geçirilmesidir.

**Açıklama:** Bir bilgisayar yada iletişim sisteminin fonksiyonlarına zarar vermek amacı ile verilerin yada programların Zaman Bombası (Logic-Time Bomb), Truva Atları (Trojan Horses), Virüsler, Solucanlar (Worms) gibi yazılımlar kullanılarak değiştirilmesi, silinmesi, ele geçirilmesi yada çalışmaz hale getirilmesidir.

### **2.2. Fiziksel Bilgisayar Sabotajı**

**Tanım:** Bir bilgisayar yada iletişim sisteminin fonksiyonlarına zarar vermek amacı ile sisteme fiziksel yollarla zarar vermedir.

**Açıklama:** Bir bilgisayar yada iletişim sistemini oluşturan parçalara sistemin fonksiyonlarını yerine getirmemesi amacıyla fiziksel yollarla zarar verilmesidir.

## **3. Bilgisayar Yoluyla Dolandırıcılık**

**Tanım:** Bilgisayar ve iletişim teknolojileri kullanılarak verilerin alınması, girilmesi, değiştirilmesi ve silinmesi yoluyla kendisine veya başkasına yasadışı ekonomik menfaat temin etmek için mağdura zarar vermektir.

**Açıklama:** Suçlunun hedefi kendisine veya bir başkasına mali kazanç sağlamak yada mağdura ciddi kayıplar vermektir. Bilgisayar dolandırıcılığı suçları suçların modern bilgisayar teknolojileri ve ağ sistemlerinin avantajlarını değerlendirmeleri yoluyla klasik dolandırıcılık suçlarından farklılık gösterir.

### **3.1. Banka Kartı Dolandırıcılığı**

**Tanım:** Kartlı ödeme sistemleri kullanılarak yapılan dolandırıcılık ve hırsızlık suçlarıdır.

**Açıklama:** Kredi kartları, Bankamatik kartları ve benzeri kartlarla yapılan dolandırıcılık suçlarıdır. Kart ödeme sistemleri (ATM-Automated Teller Machine) genelde bankalar veya benzer finans kuruluşları tarafından kullanılırlar. Erişim genellikle bir kişi tanımlama numarası (PIN-Personel Identification Number) girişi gerektiren bir kart yada benzeri bir sistem ile yapılır. Dolandırıcılık bu kartların çalınması, çoğaltılması, kopyalanması yada iletişim hatlarının engellenmesi ve dinlenmesi yoluyla oluşur.

### **3.2 Girdi/Çıktı/Program Hileleri**

**Tanım:** Bilgisayar sistemine kasıtlı olarak yanlış veri girişi yapmak veya sistemden yanlış çıktı almak yada sistemdeki programların değiştirilmesi yoluyla yapılan dolandırıcılık ve hırsızlıktır.

**Açıklama:** Bir bilgisayar veritabanına yanlış veri girmek yaygın bir dolandırıcılık yoludur. Davalar araştırılırken sistem de kullanılan yazılım programları da içerecek şekilde tam bir teknik tanımlama yapılmasına ihtiyaç vardır.

### 3.3. İletişim Servislerini Haksız ve Yetkisiz Olarak Kullanma

**Tanım:** Kendisine veya başkasına ekonomik menfaat sağlamak amacıyla iletişim sistemlerindeki protokol ve prosedürlerin açıklarını kullanarak iletişim servislerini veya diğer bilgisayar sistemlerini hakkı olmadan kullanmak.

**Açıklama:** İletişim servislerinin değişik şekillerde kötü niyetli olarak kullanımı olarak tanımlanabilir.

## 4. Bilgisayar Yoluyla Sahtecilik

**Tanım:** Kendisine ve başkasına yasa dışı ekonomik menfaat temin etmek ve mağdura zarar vermek amacıyla; bilgisayar sistemlerini kullanarak sahte materyal (banknot, kredi kartı, senet vs.) oluşturmak veya dijital ortamda tutulan belgeler (formlar, raporlar vs.) üzerinde değişiklik yapmaktır.

**Açıklama:** Dijital ortamda tutulan dokümanlar üzerinde değişiklik yapmak bir tür sahteciliktir. Bilgisayarlarda tutulan dokümanlarda (İş akış programları, raporlar, personel bilgileri vs) sahtecilik amacıyla yapılan değişikliklerle kişiler kandırılabilir.

## 5. Bir Bilgisayar Yazılımının İzinsiz Kullanımı

**Tanım:** Kanunla korunmuş yazılımların izinsiz olarak çoğaltılmasını, yasadışı yöntemlerle elde edilen bilgisayar yazılımlarının satışını, kopyalanmasını, dağıtımını ve kullanımını ifade eder.

### 5.1. Lisans Sözleşmesine Aykırı Kullanma

**Tanım:** Tek bir bilgisayar için alınan yazılımın birden fazla bilgisayarda lisans haklarına aykırı olarak kullanılmasıdır.

**Açıklama:** Yazılım lisansları genellikle tek bir bilgisayarda kullanmak üzere tanzim edilir. Tek bir bilgisayar için alınan yazılımın lisans hakları çerçevesinde birden fazla bilgisayara kullanılmak üzere kopyalanması ve çalıştırılması yasaktır.

### 5.2. Lisans Haklarına Aykırı Çoğaltma

**Tanım:** Lisans sözleşmesi ile korunmuş bir yazılımın saklanmış olduğu medya ortamının başka bir medya ortamına kanunsuz olarak kopyalanmasıdır. Genel itibariyle ödemedi kaçınmak için daha önce satın alınmış veya yine lisans sözleşmesine aykırı olarak kopyalanmış yazılımın başka bir medya ortamına taşınmasıdır

**Açıklama:** Burada söz konusu yazılımı kopyalayan da kopyalatan da sözleşme ihlali yapmış sayılır. Bugün bir çok yerde satılan program, film ve oyun CD'leri bu şekildedir. Bu tür CD'lere bakıldığında üzerlerinde Kültür Bakanlığının bandrolü olmadığı ve yazılabilir CD'lere kayıt edildiği ve orijinal kutularında olmadığı görülmektedir.

### **5.3. Lisans Haklarına Aykırı Kiralama**

**Tanım:** Değişik medyalar üzerine kayıtlı oyun, film ve yazılımların lisans haklarına aykırı olarak kiralanmasıdır.

**Açıklama:** Oyun, program ve filmleri kiralamaya yönelik özel bir lisansı bulunmadan kiralanmasıdır. Daha çok film ve oyun CD'lerinin kiralanması olarak karşımıza çıkmaktadır.

## **6. Diğer**

### **6.1. Kişisel Verilerin Suiistimali**

**Tanım:** Ticari yada mesleki sırların, kişisel bilgilerin yada değerli diğer verilerin kendisine veya başkasına menfaat sağlamak yada zarar vermek amacıyla, bu bilgilerin kullanımı, satılması ve dağıtımıdır.

**Açıklama:** Banka, hastane, alışveriş merkezleri, devlet kurumları gibi kuruluşlarda tutulan her türlü kişisel bilginin kendisine yada başkasına menfaat sağlamak veya zarar vermek amacıyla kişilerin rızası dışında kullanılmasıdır.

### **6.2. Sahte Kişilik Oluşturma ve Kişilik Taklidi**

**Tanım:** Hile yoluyla kendisine veya bir başkasına menfaat sağlamak yada zarar vermek amacıyla gerçek kişilerin taklit edilmesi veya hayali kişilerin oluşturulmasıdır.

**Açıklama:** Bu metotta, gerçek kişilere ait bilgileri kullanarak o kişinin arkasına saklanılmakta ve o kişinin muhtemel bir suç durumunda sanık durumuna düşmesine neden olunmaktadır. Ayrıca kredi kartı numara oluşturucu programlar gibi araçlar kullanılarak elde edilecek gerçek bilgilerin hayali kişiler oluşturulmasında kullanılmasıyla menfaat sağlanılmakta ve zarar verilmektedir.

### **6.3. Yasadışı Yayınlar**

**Tanım:** Yasadışı unsurların yayınlanması ve dağıtılması maksadı ile bilgisayar sistem ve ağlarının kullanılmasıdır.

**Açıklama:** Kanun tarafından yasaklanmış her türlü materyalin, Web Sayfaları, BBS'ler, elektronik postalar, haber grupları ve her türlü veri saklanabilecek optik medyalar gibi dijital kayıt yapan sistemler vasıtasıyla saklanması dağıtılması ve yayınlanmasıdır.

## ÜÇÜNÇÜ BÖLÜM

### DİĞER ÜLKELERDE BİLİŞİM SUÇLARI ALANINDAKİ HUKUKİ VE İDARİ YAPILANMA

#### Giriş

Yeni teknolojilerin geleneksel suçları işlemede kullanılması yeni olan bir kavram değildir. Teknolojik gelişmeler, suç işleyen kişilere yasadışı işler yapmada yeni yollar tanımaktadır. Bilişim suçları da yeni teknolojilerin suç işlemede kullanılmasıdır. Bilgisayar ve iletişim teknolojilerindeki gelişmeler geleneksel suçların işlenmesinde yeni bir araç olmasının yanında yeni suç tiplerinin de çıkmasına sebep olmuştur. Her şeye rağmen şu da göz ardı edilmemelidir ki polis teşkilatları da yeni teknolojileri takip ettikçe ve kullanmaya başladıkça suçla mücadelede ve vatandaş memnuniyeti ve emniyetinde ciddi mesafeler kat etmiştir.

Bugün en karmaşık suç tipleri bilgisayar teknolojileri kullanılarak işlenen suçlardır. Özellikle İnternet'in uluslararası bir bilgisayar ağı olması nedeni ile suç ve suçlu ile mücadele de bir çok zorluklar ortaya çıkmaktadır. Teknolojiyi kullanan suçlular veya ileri teknolojiye hakim olup suç işlemeye meyilli insanlar için İnternet bulunmaz bir ortam oluşturmaktadır. İnternet ve ileri teknoloji ürünü aletler kullanılarak işlenen suçlarda en büyük problem bu insanların kimliklerini tespit etmektir. İnternet'in büyüyerek herkesin ilgisini çektiği günümüzde İnternet üzerinde işlenen ve işlenecek suçlarla mücadele bütün polis teşkilatlarının öncelikli gündemi haline gelmektedir. Teknolojik gelişmelerin ülke sınırları ile sınırlandırılmadığı günümüzde bu tür suçlarla mücadele içinde uluslararası boyutta işbirliği ve çalışmalar kaçınılmaz hale gelmiştir. Suçluların teknolojik gelişmeleri kullanarak kazandıkları hızı polis teşkilatları da yapacakları işbirliği ve geliştirecekleri yeni çalışma sistemleri ile bir an önce kazanmalıdırlar. Bu tip suçlarla mücadelede ulusal düzenlemeler ve yapılanma çok önemlidir ama uluslararası koordinasyon ve işbirliği her zamankinden daha fazla ihtiyaç duyulan hayati bir konu haline gelmiştir.

2000 yılı Şubat ayında Amerika Birleşik Devletleri'nin önemli İnternet siteleri yapılan saldırılar ile hizmet dışı kalmış, bu saldırılar neticesinde (Denial of Service) Yahoo, CNN, E-Bay ve bunun gibi pek çok site hizmet veremez hale gelmiştir. Yine bir kaç ay sonra "I Love You" ve "New Love" virüs saldırıları ile dünya üzerindeki pek çok şirketin bilgisayar sistemlerinde ciddi zararlar meydana gelmiştir. Bununla birlikte yaklaşık 30 tane bilgisayar virüsünün ortaya çıktığı günümüzde bilgisayar sistemleri zarar görmekte ve firmalar milyonlarca dolar zarar etmektedir. Devlet ve özel kuruluşların vatandaşlara ve müşterilerine daha iyi ve hızlı hizmet verebilmek için her geçen gün daha fazla kullanmaya başladıkları bilgisayar sistemlerini düşünürsek karşılaşılan tehlikenin ne kadar önemli olduğunu anlamakta zorlanılmayacaktır.

"The Computer Security Institute" ve FBI tarafından yapılan bir araştırmada "Bilgisayar Suçları ve Güvenliği" anketine katılan sadece 273 organizasyonun toplam 265.589.940 \$ (iki yüz altmış beş milyon beş yüz seksen dokuz bin dokuz yüz kırk dolar) mali kayıpları olduğu tespit edilmiştir. Bunu bilgisayar kullanan şirketlerin dünya çapında ne kadar olduğunu düşünürsek ve yaklaşık üç yüz milyon İnternet'e bağlı bilgisayar olduğunu da değerlendirirsek her sene bilgisayar sistemlerine verilen zararlar sonucu milyarlarca dolar zarar edildiği görülecektir.

Bilgi çağına girdiğimiz şu dönemde, bilgi teknolojileri günlük iş ve sosyal hayatımızın her alanına girmiş durumdadır. Bu durum kanun uygulayıcı kuvvetler açısından yeni problemler doğurmaktadır. Yukarıda da bahsedildiği gibi geleneksel suçların ileri

teknolojinin yardımı ile daha farklı yollardan işlenmesi kanun uygulayıcı kuvvetlerin işini zorlaştırmakta ancak, yine ileri teknolojiler sayesinde kanun uygulayıcı kuvvetler siber suçluların takibini ve yakalamasını gerçekleştirmektedir. Tabii geleneksel suçların yeni yollarla işlenmesi beraberinde yeni suç tiplerinin belirlenmesi ihtiyacını doğurmuş ve ülkelerin bu alanda kanuni düzenlemeler yapmasını gerekli kılmıştır. Aşağıda İnterpol vasıtası ile ulusal mevzuatlarına ulaştığımız ülkelerin hukuki durumları görülmektedir.

### **Amerika Birleşik Devletleri:**

Amerika Birleşik Devletleri'nde teknolojik suçlar ve siber terörizmle mücadele eden pek çok kuruluş ve bu kuruluşlara ait özel birimler bulunmaktadır. Bunlardan bazıları şunlardır. FBI National Infrastructure Protection Center, Information Technology Association of America, Trap and Trace Center Authority ile Carnegie Mellon's Emergency Response Team ile bazı üniversiteler bünyesinde kurulan birimler bunların en önemlileridir.

ABD yönetimi, bu suçlarla mücadelenin gerekliliğini anlayarak Temmuz 1996 yılında "Commission of Critical Infrastructure Protection" adı A.B.D başkanına bağlı bir komisyon oluşturmuştur. Bu komisyon, elektronik haberleşme ve bilgisayar ağlarının ABD açısından hayati önem taşıdığını, söz konusu ağların dış saldırılara karşı açık olduğunu, öte yandan, kamu ve özel sektörün mevcut tehditleri ciddiye almadığını belirtmiş ve bu ağların korunması için önlemler alınmasının gerekliliğini savunmuştur. Söz konusu komisyon, suçun takip edilmesi ve araştırılması ile önceden alınacak önlemler konusunda yöntemler tespit etmiştir. Bu komisyon bu alanda çalışma yapan ilk ulusal grup olmuştur.

Bununla birlikte, bir çok kamu kurumu ve kuruluşu bu suçlarla mücadele etmede bazı birimler oluşturmuşlardır. Örneğin, CIA, "Information Warfare Center" adında ve 1000 kişilik bir personelle 24 saat hizmet veren bir birim oluşturmuştur.

FBI ise bilgisayar sistemlerine girme ve benzeri suçları takip etmek amacıyla "National Infrastructure Protection Center" ve "Computer Crime Squad"ı oluşturmuştur.

Yine Adalet Bakanlığı bünyesinde oluşturulan "Computer Crime and Intellectual Property Section" bu alanda çalışmalar yapmakta, gerekli eğitim faaliyetlerinde bulunmakta ve diğer birimlere destek vermektedir.

ABD'de bu suçlarla mücadelede kullanılan kanunların bazıları şunlardır.

- 18 U.S.C. § 1029. Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers
- 18 U.S.C. § 1362. Communication Lines, Stations, or Systems
- 18 U.S.C. § 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited
- 18 U.S.C. § 2701. Unlawful Access to Stored Communications
- 18 U.S.C. § 2702. Disclosure of Contents
- 18 U.S.C. § 2703. Requirements for Governmental Access

Görüldüğü üzere ABD'de mevzuat alanında bu suçlarla ilgili gerekli önlemler alınmış, bunun yanında kanun uygulayıcı kuvvetlerin bu suçlarla mücadeledeki hak ve sorumlulukların da gerekli düzenlemeler yapmıştır.

### **Fransa:**

Fransa da 1998 yılında yeni teknolojiler kullanılarak işlenen suçların maliyeti 14 milyar FF düzeyine ulaşmış, 1999 yılında ise bu konuda polis ve jandarma makamlarına 3815 olay aksettirilmiştir. Bunların 2450 adedi İnternet kullanılarak işlenen suçlardır. Kalan 1336 adedi ise telekomünikasyon sistemlerinin kullanımına aittir.

Bu alandaki Fransız Danıştay'ının 1998 yılında İnternet konulu yayınladığı raporda, mevcut mevzuatın bilgisayar ortamında işlenen suçlarla mücadeleyi de kapsayacak şekilde geliştirilmesinin yeterli olacağını belirtmiştir. Ancak, bazı özel konularda yeni hukuki çerçevelerin belirlenmesi ihtiyacı doğmuştur. 17 Mart 1999 tarihinde şifreleme sistemi kullanımına ilişkin mevzuatta değişiklikler yapılmıştır. Yine 29 şubat 2000 tarihinde elektronik imzaların hukuki değer taşımasına ilişkin bir kanun kabul edilmiştir.

Teknolojik suçlarla mücadele amacıyla devletin birden fazla kurumunda özel birimler kurulmuştur.

- Başbakan'a bağlı Milli Savunma Genel Sekreterliği (SGDN) bünyesinde kurulan Haberleşme Sistemleri Güvenliği Merkez Birimi (DCSSI)

- Haberleşme Teknolojisi kullanılarak yapılan dolandırıcılıkların soruşturulması birimi (SEFTI)

- Bilgisayar ortamında işlenen suçların bastırılması birimi (BCRCI)

- Jandarma Genel Komutanlığı Seç Araştırmaları Enstitüsü (IRCGN)

- Fransız İstihbarat Örgütü (DST)

- İletişim ve Enformasyon ve Teknolojilerinin Kullanımı Suretiyle İşlenen Suçlarla Mücadele Bürosu

## **İrlanda:**

İrlanda şu anda ülkede yatırım yapan ABD firmalarının da etkisiyle bilgisayar üretimi/satışı, program yazılımı ve enformasyon teknolojisine yatırım açısından AB'nin en önde gelen ülkesi konumundadır.

İrlanda'da bilgisayar suçları ile mücadele etmek amacıyla 1991 yılında "The Computer Crime Unit" kurulmuş ve bu tür suçlarla mücadelede yetkili kılınmıştır. Temelde spesifik olarak bilgisayar suçları ile ilgili kanunlar olmasa da, 1991 yılında yasalaşan "Criminal Damage Act" bu tür suçlarla ilgili geniş tanımlamalar yapmaktadır. 1991 yılında çıkarılan bu yasa dört temel suç ortaya koymaktadır.

- Mülkiyete zarar verme (bilgisayarlar ve veriler dahil)

- Mülkiyete zarar vermek amacıyla tehdit etmek

- Bilgisayara yetkisiz giriş

- Bilgisayarlara zarar vermek niyetiyle sahip olunan her şey (ör: virüsler)

"Criminal Damage Act" haricindeki diğer kanunlar aşağıda sıralanmıştır.

1. The Copyright Act 1963

2. The Criminal Evidence Act 1992

3. The Data Protection Act 1988

4. The Postal and Telecommunications Services Act 1983

5. The Child Trafficking and Pornography Act 1998

## **Hollanda**

1993 tarihli Computer Crime Act yasalaşmadan önce Hollanda polisi bilgisayar suçları ile mücadele etmek amacıyla özel bir birim kurmuştur. Üç pilot bölgede yapılan başarılı uygulamalardan sonra bölgeler arası bir bilgisayar suçları ile mücadele birimi kurulmuştur. Bilgisayar suçları birimleri Adalet Bakanlığına bağlı kriminal laboratuvarları, Information Technology and Crime Department of the National Criminal Intelligence Division ve Detective's Training Collage ile birlikte çok yakın çalışmalar yapmaktadır.

Konunun uzmanları, siber suçlarla ilgili olarak takip edilen yöntemin, diğer suçların işlenişleriyle aynı olduğunu, kapsamlı bir uluslararası antlaşmanın olmaması ve suçun hangi

ülkeden işlendiğinin tespit edilmesindeki güçlükler nedeniyle, uluslararası alanda mücadele güç olmakla beraber, tespit edilen suçlarla ilgili işbirliğinin adli yardımlaşma çerçevesinde gerçekleştirildiğini ifade etmektedirler.

## **İspanya**

İspanya’da siber suçlara ilişkin mevzuat Ceza Kanunu ile ilgili maddelerden ibarettir. Söz konusu suçlarla mücadelede şirketler, firmalar ve şahıslar tarafından alınan tedbirler ise bu amaçla hazırlanmış koruma amaçlı yazılımlardan öteye gitmemektedir.

İspanyol Hükümeti yasalardaki düzenlemelere ilaveten, İçişleri Bakanlığı, Emniyet Genel Müdürlüğü bünyesinde bir birim oluşturmuştur. Enformasyon Teknolojilerindeki Suçları Araştırma Birimi adı altında faaliyet gösteren emniyet görevlileri teknoloji, iletişim, telekomünikasyon ve çocuk pornografisi alanlarında işlenen suçları ve ortaya çıkan şikayetleri takip etmektedir. Sadece Madrid’de bulunan merkez büronun yanında bu sene içinde ülke çapında değişik yerlerde de yeni bürolar açılması planlanmaktadır.

## **İsrail**

İsrail Emniyet Müdürlüğü, bilgisayar üzerinden işlenen suçlar konusuyla 1996 yılından itibaren ilgilenmeye başlamıştır. Bu yılın başında, Sahtekarlık bünyesinde Bilgisayar Suçları Bölümü kurulmuştur. Anılan bölümdeki görevliler, esasen polis olup bilgisayar konusunda eğitimden geçirilmişlerdir. Bu birim, 1995 yılında yürürlüğe giren Bilgisayar Yasası ve polis soruşturma ve tutuklama kanunu çerçevesinde görev yapmaktadır. Gerekliğinde diğer polis birimlerince yürütülen soruşturmalara yardımcı olmaktadır.

Bilgisayar üzerinden işlenen suçlara karşı polis tarafından teknik önlemler alınması söz konusu değildir. Bu alanda diğer devlet kuruluşları ve özel şirketlere yardımcı olunmamaktadır. Söz konusu kuruluşlar kendi imkanları ile korunma sistemlerini oluşturmakta ve işletmektedirler.

İsrail hükümeti, bilgisayar suçları ile mücadele konusunda başta ABD olmak üzere, birçok Avrupa ülkesiyle işbirliği anlaşması imzalanmış bulunmaktadır.

## **İsveç**

Konuya ilişkin olarak İsveç’te mevcut yasal düzenlemeler ceza kanunu içerisinde bulunan “bilgi hırsızlığı” ve “bilgi sistemlerini ihlal etme/bilgisayarlara yasadışı giriş ya da verileri kötüye kullanma” şeklinde tanımlanabilecek suçlara ilişkin hükümlerdir.

İsveç’te bütün devlet kuruluşları bilgisayar güvenliği konusunda kendi önlemlerini almaktadır. Bununla beraber, 1999 yılında hükümet “Ulusal Posta ve Telekomünikasyon Ajansı”na konuyla ilgili ihtiyaçları tespit ve analiz etme talimatı vermiştir. Konu hakkında polisiye birimleri bulunup merkezi bir ekip bu tür suçları bütün ülkede takip etmekte ve mücadele etmektedir.

## **İsviçre**

İsviçre’de siber terörizm ve teknolojik suçlarla mücadeleye ilişkin, “federal ceza yasası” ve “haksız rekabet yasası” adında federal iki yasa mevcuttur. “Federal ceza yasası” yasal olmayan yollardan teknolojik bilgi edinme, bilgi çalma ve bilgileri bozma gibi

suçların cezalandırılmasını içermekte, “haksız rekabet yasası” ise, ticari amaçlı bilgisayar suçlarını içermektedir.

Federal ceza yasasının 143. maddesi kayıt altına alınmış veya elektronik ortamda iletişime konu olan verilerin hırsızlığına ilişkin suçun 5 yıl ve daha fazla süre için hapisle cezalandırılmasını öngörmektedir.

Aynı yasanın 143. maddesi ise, bir bilgisayar sistemine teknik yollar kullanılarak girilmesi suretiyle yapılacak veri hırsızlığının, şikayet üzerine, hapis veya para cezası ile cezalandırılmasını öngörmektedir.

Söz konusu yasanın 147. maddesine göre, bir bilgisayarın yasadışı biçimde eksik ve yanlış veriler kullanılarak etkilenmesi yoluyla sahtecilik amaçlı kullanılması ve bu sayede başkalarına maddi zarar verilmesi durumunda en fazla 5 yıl en az 3 ay hapis cezası verilmesi, suçlunun bu eylemi mesleğini icra ederken yaptığı belirlendiğinde ise 10 yıldan fazla ve 3 aydan az olmamak üzere hapis cezası verilmesi öngörülmektedir.

## **Norveç**

Norveç’te işlenen bilgisayar suçları ile ilgilenen makam Norveç Adalet Bakanlığına bağlı Polis Teşkilatı içinde özel olarak oluşturulan OKOKRIM “Ekonomik ve Çevre Suçları Araştırma ve Soruşturma Milli Otoriter” birimidir. OKOKRIM’in bilgisayar suçları birimi, bilgisayar mühendisleri, dedektifler ve savcılardan oluşan multidisipliner bir merkezdir. 1993’den bu yana faaliyette olan birim, çeşitli türdeki siber saldırıların tespiti, soruşturulması ve ortaya çıkarılması, dijital korsanlık gibi konularda büyük tecrübeye sahiptir.

## **İtalya**

Bilgisayar suçları konusunda en son yasal düzenleme 23 Aralık 1993 tarihinde 547 sayılı kanun ile yapılmıştır.

İtalya’da bilgisayar suçları ile mücadele için 30 Mart 1998 tarihinde Emniyet Genel Müdürlüğü bünyesinde kurulmuş olan Posta ve İletişim Güvenliği Daire Başkanlığı bulunmaktadır. Başkanlık bünyesinde Personel/Lojistik ve Teknik olmak üzere iki bölüm mevcuttur. Taşrada ise 20 ilde doğrudan başkanlığa bağlı olarak görev yapan ofisler bulunmaktadır. Operasyonel işlevi olan teknik bölüm bünyesinde oluşturulan bir çalışma grubunda mühendisler, bilişim teknisyenleri ve örgütlü suç, terörizm, çocuk pornografisi vb. Konularda uzmanlaşmış dedektifler görev yapmaktadır.

Bilgisayar üzerinden işlenen suçlar konusunda, ceza yasasında tarif edilen suç teşkil eden eylemler özet olarak aşağıdadır:

- Yazılımları kısmen veya tamamen tahrip eden, değiştiren, bilgi veya iletişim sistemlerinin doğru çalışmasını engelleyen programlarla saldırıda bulunmak (1 milyon lirt-500\$- kadar para cezası)
- Kamu yararına kullanılan tesislerin, bilgi sistemlerinin, veri, bilgi ve yazılımlarının içeriklerini tahrip etmek ve çalışmasını kesintiye uğratmak (1 yıldan 4 yıla kadar hapis)
- Bilgi veya iletişim sistemlerine fiziki olarak veya yazılım aracılığıyla yetkisiz olarak girmek, bilgi almak, alınan bilgileri yaymak, kayıtlar üzerinde tahribat yapmak veya sisteme maksatlı olarak yeni bilgiler ilave etmek ( 3 yıla kadar hapis ve 10 milyon lirt –5000\$-kadar para cezası)
- Her türlü iletişimin engellenmesi, mahremiyetinin, ihlal edilmesi, bu amaçla çeşitli cihaz ve sistemlerin kurularak enformatik ve telematik haberleşmenin kesintiye uğratılması, araya girilmesi veya iletişimin içeriğinin değiştirilmesi,

•Gizli dokümanların içeriğinin açıklanması, gizli kalması gereken kamu veya özel dokümanların içeriğinin yasadışı olarak ele geçirilmesi ve açıklanması (3 yıla kadar hapis ve 2 milyon liraya kadar para cezası)

Bu suçlarla mücadele için Posta ve İletişim Güvenliği Daire Başkanlığı bünyesinde oluşturulan grup, sürekli olarak İnternet üzerinde çalışmakta ve ilgili kanunlarda tarif edilen herhangi bir suç unsuruna rastladıklarında çeşitli yöntemlerle suçlular tespit edilerek, suç ve suçlular adli makamlara intikal ettirilmektedir. Dijital Ortamda işlenen her türlü suç bu grubun görev alanına girmektedir.

## **Kanada**

Kanada’da ABD’den farklı olarak, siber terörist saldırılara veya network sabotajlarına karşı önlemler almakla sorumlu bir hükümet kuruluşu olan FEDCERT (Federal computer emergency response team) benzeri bir özel birim bulunmamaktadır. Esasen, Kanada enformasyon ağırlıklı bir sisteme sahip olup da bilgisayar olaylarına karşı uluslararası koalisyon durumundaki FIRST (Forum For Incident Response Teams)’e üye olmayan ender ülkelerden biridir. Bununla birlikte, Kanada’da CANCERT (Canadian Computer Emergency Response Team) adı altında benzer işleve sahip bir özel sektör kuruluşu bulunmaktadır. Ayrıca her federal bakanlık ve kuruluşun da ayrı ayrı enformasyon teknolojisi güvenliği politikası ve yöntemleri mevcuttur.

Kanada’da siber terörizm ve benzeri teknolojik suçlar halen mevcut ceza kanunu kapsamında işlem görmektedir. Ceza kanununun 1985 yılından itibaren yapılan değişikliklerle bu tür faaliyetler de suç kapsamına alınmıştır. Ceza kanununun 342. maddesi uyarınca hakkı olmadan ve sahtekarlık yoluyla elektromanyetik, akustik, mekanik veya başka bir cihaz yoluyla bir bilgisayar sistemini dolaylı veya doğrudan kesintiye uğratan herkes cezai müeyyideyi gerektiren bir suçun faili durumundadır.

## **Yeni Zelanda**

Teknolojik suçlarla ilgili olarak, 1961 tarihli ceza yasasının yetersizliğinin görülmesi üzerine hazırlanan “Crimes Involving Computers” başlıklı yasa değişikliği tasarısı parlamentoya sevk edilmiş ve yıl sonunda onaylanması beklenmektedir. Bununla birlikte bilgisayar suçlarına yönelik polisiye birimler oluşturulmuştur.

## **Hindistan**

Siber terörizm ve benzeri teknolojik suçlarla mücadele hususunda Hindistan Bilgi ve Teknoloji Bakanlığı tarafından yapılan çalışmalarda üç aşamalı bir yaklaşım izlenmiştir. Birinci aşamada, bu tür suçların önlenmesini teminen alınması gerekli fiziki tedbirler belirlenmiş ve kullanıcıların istifadesi için güvenlik rehberi hizmeti verilmeye başlanmıştır. İkinci aşamada, başta savunma, dışişleri, içişleri bakanlıkları olmak üzere, hassas bilgilere ve teknolojilere sahip bakanlık ve kuruluşları, siber terörizm ve teknolojik suçların yaratabileceği tehlikeler ve bunlara karşı alınacak tedbirler hakkında bilgilendirme çalışmaları başlatılmış ve müteakip aşamada oluşturulacak yasal çerçeve için söz konusu kurulların destek ve deneyimlerine başvurulmuştur. Son aşama yasal çerçevenin hazırlanmasıdır. Bu amaçla aralık 1999’da parlamentoya sunulan yasa tasarısı bahse konu suçların önlenmesi ve bu suçları yasal bir çerçeveye oturtmayı ve devletin bu alandaki kontrol zafiyetini gidermeyi amaçlamaktadır. Siber ve teknolojik suçlarla ilgilenmek üzere Bilgi ve Teknoloji Bakanlığı bünyesinde özel bir grup tesis edilmiştir. Bilgisayar

mühendislerinden oluşan bu grup siber ve teknolojik güvenliğin artırılması çalışmalarını yürütmekte ve kamu kurum ve kuruluşlarının güvenlik programlarının oluşturulmasına yardım etmektedir.

## **Malezya**

Malezya'da siber suçlarla mücadele, Haberleşme, Multimedya ve Enerji Bakanlığı sorumluluk alanına girmektedir. Malezya'da teknolojik suçlara ilişkin kanunlar:

- Digital Signature Act
- Multimedia Convergence Act
- Computer Crime Act
- Telemedicine Development Act

Bu kanunlarda yer alan bilgisayar suçları da şöyledir:

- Bilgisayarlara izinsiz nüfuz etme, hasar verme
- Kullanıcı şifresi alışverişi
- Telif haklarının ihlali
- Marka sahteciliği
- Ticari sırları çalma
- Çocuklara yönelik istismar ve müstehcenlik
- İnternet dolandırıcılığı
- İnternet tacizi

İnternet'le tehdit, korku, panik, huzursuzluk yayma

Hükümet ve özel sektör siber suçları, engelleyici teknolojiler geliştirerek, güvenli iletişim için uluslararası iletişim ve bilgi teknolojileri standartlarını kullanarak, gizli elektronik işlemleri şifreli olarak ve güvenlik yazılımları kullanmak suretiyle engellemeye çalışmaktadır.

## **Pakistan**

Pakistan Bilim ve Teknoloji Bakanlığı, ilgili diğer kuruluşlarla işbirliği halinde siber terörizm ve benzeri teknolojik suçları da kapsayacak şekilde bilgisayarlarla ilgili bütün hususları içeren bir yasa oluşturulması üzerinde çalışmaktadır.

## **Rusya**

Rusya'da bilgisayar üzerinden işlenen suçlar konusunda iki yıl öncesine kadar bir düzenleme bulunmamaktaydı. Ancak, G-8 ülkelerinin 1997 yılında Washington'da yaptıkları Adalet ve İçişleri Bakanları toplantısında kabul edilen bildiri ile "Ulusal Temas Noktaları" oluşturulmasına karar verilmesi üzerine, İçişleri Bakanlığı bünyesinde bir temas noktası oluşturulmuştur. "R dairesi" olarak adlandırılan bu bölüm, ülke içindeki güvenlik ve yargı organları ile ve diğer ülkelerdeki karşıtları ile doğrudan temas halinde bulunmakta ve uzmanları 24 saat kesintisiz çalışma prensibi uygulamaktadır.

Rusya İçişleri Bakanlığı, İnternet üzerinden suç ve suçluların takibi için delillerin korunması amacıyla İnternet hizmeti sağlayan servislerle işbirliği yapmakta, İnternet firmalarına verilerini 6 ay saklama ve yargı makamlarının talebi olduğu takdirde söz konusu verileri ilgili makamlara sağlama zorunluluğu getirmektedir.

## Singapur

Singapur hükümeti, bilgisayar üzerinden işlenen suçlarla mücadele için “Computer Misuse Act” ile elektronik ticareti düzenlemek ve işlemleri hukuki zemine oturtmak için “Electronic Transaction Act” yasalarını çıkarmıştır. Singapur’da siber suçlarla aşağıda belirtilen kurumlar ve program aracılığıyla mücadele edilmektedir.

- Singapur Polis Gücü: Yasaların uygulanmasını sağlamaktadır.
- Infocommunications Development Agency’nin güvenlik Dairesi: siber suçlarla mücadele için gerekli politikaları oluşturmakta ve bu konuda ilgilileri yönlendirmektedir.
- Singapur Computer Emergency Response Team (SINGCERT) : Kamuoyunu siber saldırılar karşısında uyarmakta, gerekli önlemleri nasıl alabileceklerini bildirmekte, koruma programları tavsiye etmekte, networku önlem niteliğinde kontrol etmekte, saldırı denemeleri olup olmadığını araştırmakta ve siber saldırılardan korunma konusunda halkı ve ilgili kuruluşları bilgilendirmek için seminerler düzenlemektedir. SINGCERT, hükümet ile Singapur Ulusal Üniversitesi’nin işbirliği ile yürüttükleri bir programdır.

Siber suçlar computer misuse act de şu şekilde sınıflandırılmıştır:

- Yetkisiz olarak bir bilgisayara veya sisteme girmek
- Suça yardımcı olmak maksadıyla veya bu amaçla sisteme girmek
- Bilgisayarda saklı bilgileri yetkisiz değiştirmek, silmek
- Bilgisayar kullanımını önlemek ve işlemez hale getirmek
- Yetkisiz bir bilgisayar hizmetinden yararlanmak
- Şifreleri çalmak veya bunları açıklamak

Yukarda da görüldüğü gibi dünyanın bir çok yerinde ülkeler bilgisayar/bilişim suçları hakkında çalışmalar başlatmış bunlarla ilgili gerekli kanuni düzenlemeler yapmış ve bu suçlarla mücadele edecek özel birimler oluşturmuştur.

Ülkemizde Hukuki açıdan ideal bir yapı olmamakla birlikte mevcut kanunlar Dijital ortamda işlenen suçlarla mücadele için yeterlidir. Fakat Dijital ortamda işlenen suçlar kovuşturulurken uzmanlık gerektiren suçlar olduğu için bu alanda ülkemizde de özel birimlerin oluşturulması gerekmektedir. Şuan itibariyle her ne kadar Dijital ortamda işlenen suçlar Emniyet teşkilatı için bir sorun olarak görünmüyor olsa bile önümüzdeki yıllar İnternet ve elektronik ticaretin hızla geliştiği ülkemizde bu alanda da suç patlaması olacağı tahmin edilmektedir.

## DÖRDÜNCÜ BÖLÜM

### EMNİYET TEŞKİLATI İÇERİSİNDEKİ İDARİ YAPILANMA

#### Giriş

Yaklaşık iki seneden beri bilişim suçları konusunda yapmış olduğumuz çalışmalar, Emniyet teşkilatının şu anki yapılanmasının bilişim suçları konusundaki ihtiyaçlara cevap veremediği kanaatini ortaya çıkarmıştır. Bilişim suçları konusu şuan itibariyle herhangi bir daire başkanlığımızın tam olarak görev alanına girmemekle birlikte ilgi alanlarına göre Asayiş, Bilgi İşlem, Güvenlik, İnterpol, İstihbarat, Kaçakçılık, Organize Suçlarla Mücadele, Kriminal Polis Laboratuvarları ve Terörle Mücadele ve Harekat Daire Başkanlıkları konu ile ilgilidirler. İdeal manada önümüzdeki 5-10 yıl içerisinde belki de dijital suçların artmasıyla birlikte tek bir daire başkanlığı çatısı altında toplanması uygun olacaktır. Konunun hassasiyeti ve özel durumu nedeniyle yukarda bahsi geçen daire başkanlıklarının sürekli diyalog halinde olması hatta Bilgi İşlem Daire Başkanlığının veya Genel Müdürlüğümüz bünyesinde kurulacak direkt olarak Makama bağlı Bilişim Suçları Araştırma ve Koordinasyon Merkezi Şube Müdürlüğü tarafından belli aralıklarla bir araya getirilmesi, ortak çalışmalar yapılması, konu hakkında bütün daire başkanlıklarının ortak kararlar alması ve bilişim suçları hakkında bilgi bankası oluşturulması kaçınılmaz bir ihtiyaç haline gelmiştir.

Bilişim alanında işlenen suçlarla karakollarımızda ve diğer polis birimlerimizde yeterli bilgi birikimine sahip personel olmadığı için ideal manada mücadele edilememektedir. Yeterli teknik bilgiye sahip olmayan personelimizin bilişim sistemleri kullanılarak işlenen suçlarda konuyu yeterince anlayamadığı, iz ve delilleri incelemede yetersiz kaldığı, yanlış anlaşılmalarda neticesi olayların haricindeki insanların mağdur olduğu gözlenmiştir.

Bilişim suçları alanında çalışan, teşkilatımız içerisindeki tek büro olan, Bilgi İşlem Dairesi Başkanlığında bulunan Bilgisayar Suçları Bürosu sadece idari yapılanmaya ait çalışmalar yapmakta ve teşkilat içerisindeki koordinasyonu sağlamaktadır. Adli yönden şikayetleri takip etme ve olaylara müdahale etme görevi olmaması nedeniyle gelen taleplere ideal manada cevap verememektedir.

Yukarda belirtilen rahatsızlıkları gidermek, vatandaş memnuniyetini arttırmak polisin ileri teknoloji ürünü cihazlar kullanılarak işlenen suçlarla mücadeledeki başarısını arttırmak için bu konuda uzman personel yetiştirilmeli ve yeni birimler ihdas edilmelidir. Aşağıda belirtilen yapılanma tamamlanana kadar; Bilgi İşlem Dairesi Başkanlığında bulunan Bilgisayar Suçları Bürosu aktif hale geçirilip gerekli eğitimler verilerek bu alanda polis birimlerimize yardımcı olacak uzman birimler olarak çalıştırılmalıdır.

Bilişim suçları konusunda teşkilatımız içerisinde üç farklı yapılanmanın ihtiyaca cevap vereceği düşünülmektedir.

- 1) Bilgi İşlem Daire Başkanlığı altında kurulacak İnternet ve Bilişim Suçları Araştırma ve Koordinasyon Merkezi Şube Müdürlüğü
- 2) Merkez birimlerinde kurulacak Bilgi İşlem ve Bilişim Suçları Şube Müdürlükleri
- 3) Taşra teşkilatında ilgili birimlerde kurulacak Bilgi İşlem ve Bilişim Suçları Büro Amirlikleri

## **1) İnternet ve Bilişim Suçları Araştırma ve Koordinasyon Merkezi Şube Müdürlüğü**

Bilgi İşlem Daire Başkanlığı bünyesinde kurulması uygun olacak birim, bilişim suçları alanında ki koordinasyonu sağlamakla birlikte ilgili personelin eğitim ihtiyaçlarını da belirleyecektir.

Görevleri:

- Bilişim suçları konusunda teşkilat içerisindeki koordinasyonu sağlamak
- Teşkilat içerisinde konu hakkında uzmanlara yönelik eğitim ihtiyaçlarını belirlemek ve eğitim programları düzenlemek
- Bilişim suçları konusunda yurt içinde meydana gelen suç istatistiklerini toplamak ve yayınlamak
- Bilgisayar Sistemleri Güvenliği konusunda teşkilatı bilinçlendirici bülten hazırlamak
- Yurtiçi ve yurtdışı gelişmeleri takip etmek ve yönlendirmek amacıyla toplantı, konferans, seminer ve sempozyumlara katılmak ve düzenlemek
- Uluslararası kanaldan gelecek ve diğer ülkelere gidecek bilgilerde irtibat ve koordinasyon görevi yapmak
- Bilişim suçları konusunda çalışan personeli senede iki kere bir araya getirmek
- Bilgi İşlem ve Bilişim Suçları Bürolarına teknik destek vermek

## **2) Merkez Teşkilatındaki Yapılanma**

Merkez teşkilatımızda, Bilgi İşlem Daire Başkanlığımız bünyesinde kurulacak İnternet ve Bilişim Suçları Araştırma ve Koordinasyon Merkezi Şube Müdürlüğü haricinde daha önce hazırlanan Bilişim Suçları Raporunda yapılan görev dağılımı çerçevesinde ilgili daire başkanlıklarımızda Bilgi İşlem ve Bilişim Suçları Şube Müdürlükleri kurulması uygun olacaktır.

Bütün daire başkanlıklarımızda Bilgi İşlem Büroları bulunmaktadır. Bu bürolarda çalışan personelin bilgi birikiminden de istifade edilerek daire başkanlığının ilgi alanlarına giren konular üzerinde çalışacak bir şube müdürlüğünün kurulması hem taşra teşkilatındaki çalışmalarını takip etmek hem de gerekli koordinasyonu sağlamak adına son derece faydalı olacaktır.

Bu şube müdürlüklerinin Asayiş, Güvenlik, İnterpol, İstihbarat, Kaçakçılık ve Organize Suçlarla Mücadele, Kriminal Polis Laboratuvarları ve Terörle Mücadele ve Harekat Daire Başkanlıkları bünyesinde oluşturulması uygun olacaktır.

## **3) Taşra Teşkilatındaki Yapılanma**

Teşkilatımız içerisinde bilişim suçları konusunda gerek T.C.K-525 ve gerekse 5846 Sayılı F.S.E.K kanunları ve bunun yanında kanunlarımızda daha önceden tanımlanmış fakat bilgisayar sistemleri kullanılarak işlenen suçlar konusunda vatandaşlarımızın şikayetlerini iletebileceği bir birimimiz bulunmamaktadır. İl emniyet müdürlüklerimiz bu konuda Bilgi İşlem Şube müdürlüklerinden veya Bilgi İşlem Bürolarından yardım istemektedir. Bu tür uygulamalar ideal bir çözüm olmamakla birlikte Bilgi İşlem Şubelerine de asli görevleri olmayan konularda iş yükü getirmektedir. Bu eksikliği gidermek üzere illerde ilgili şube müdürlükleri altında Bilgi İşlem ve Bilişim Suçları Büroları kurulması uygun olacaktır. İhtiyaç duyuldukça açılacak Bilgi İşlem ve Bilişim Suçları Büroları vatandaş memnuniyeti

ve suç ve suçlu ile mücadele noktasında hayati bir önem arz edecektir. Konu hakkında uzman olmayan kişilerin olay yerlerinde yaptıkları yanlışlıklar hem teşkilatımızın imajını zedelemekte hem de mağdur vatandaşlarımızın ihtiyaçlarına cevap verememektedir. Hemen hemen bütün şubelerimizde bulunan bilgi işlem bürolarında çalışan teknik personelden de istifade edilerek oluşturulacak Bilgi İşlem ve Bilişim suçları büroları Daire başkanlıklarında kurulacak Bilgi İşlem ve Bilişim Suçları Şube Müdürlüklerinin bir alt birimi olarak görev yapacaklardır.

Öncelikli olarak bilişim teknolojileri kullanılarak işlenen suçların yoğun olduğu/olacağı illerde böyle bir yapılanmaya gidilmesi uygun olacaktır. İstanbul, Ankara, İzmir, Bursa, Adana, Samsun, Antalya, Erzurum ve Diyarbakır illerinde öncelikli olarak kurulması uygun olacaktır.

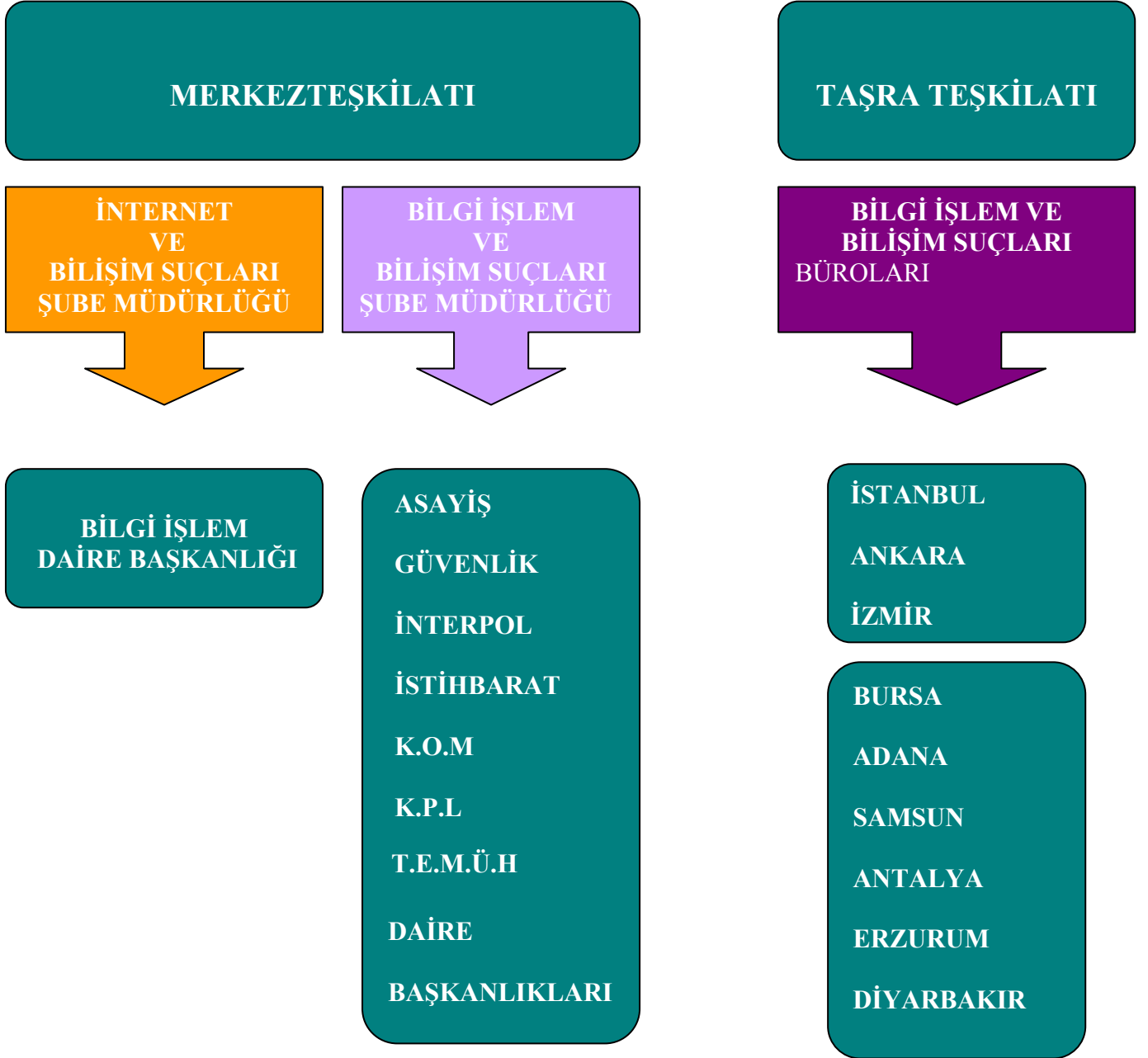
### **Karşılaşılan Problemler Ve İhtiyaçlar**

Bilişim suçları ile mücadele konusunda yapılacak idari yapılanma tek başına ihtiyaçlara cevap vermeyecektir. İdari yapılanmanın yanında teknik olarak ihtiyaçlara cevap veren birimler oluşturulmalı, bu birimlerde başta emniyet amiri ve müdürü olmak üzere orta seviye amir ve polis memurları bilgi birikimi ve liyakatlerine göre seçilerek bu birimlerde çalıştırılmalıdır. Şuan itibariyle ülkemizde böyle bir birimin eğitim ihtiyaçlarını karşılayacak her hangi bir kurum olmadığı için temel eğitimler ülkemizde verildikten sonra bu alanda çalışmaları olan başta A.B.D leri olmak üzere yapılacak ikili anlaşmalarla bu personele teorik ve pratik eğitimin yanında uygulamayı görmek ve öğrendiklerini tatbik edebilmek üzere staj yaptırılarak eğitim ihtiyacı karşılanmalıdır. Üst düzey yönetici ve teknik personel olarak iki farklı eğitim programı belirlenmeli üst düzey yönetici kursu üç aydan fazla olmayacak ve teknik personel eğitimi altı aydan az olmayacak şekilde belirlenmelidir.

Şuana kadar bilgisayar suçları konusunda yapılan uluslararası toplantı, konferans ve eğitimlere katılım için yapılan talepler özellikle eğitim programlarının ücretli olması sebebiyle tasarruf tedbirlerine aykırı bulunarak geri çevrilmiştir. Yaşanan bu tür aksaklıkları ortadan kaldırmak için bilişim suçları konusundaki teknik, idari ve eğitime ait ihtiyaçları gidermek üzere yeterli bir bütçe ayrılması uygun olacaktır.

2001 yılında çalışmalara başlanırsa önümüzdeki iki sene içerisinde idari yapılanma tamamlanarak bu birimlerde çalışacak personel seçilip eğitimleri verilip çalışmaya başlamış olacaktır. Yukarıda bahsi edilen yapılanma tamamlandıktan sonra teşkilatımızın bilişim alanında işlenen suçlarla mücadele konusundaki eksikliği giderilmiş ve A.B.D ve Avrupa ülkeleri düzeyinde bu tür suçlarla mücadele ediliyor olacaktır.

## EMNİYET GENEL MÜDÜRLÜĞÜ İÇERİSİNDEKİ BİLİŞİM SUÇLARI KONUSUNDA Kİ İDARİ YAPILANMA



**NOT: BİLİŞİM SUÇLARI BÜROLARI İL EMNİYET MÜDÜRLÜKLERİNDE İHTİYAÇ DUYULDUKÇA KURULACAK VE MEVCUT SAYI ARTTIRILACAKTIR**